CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

FUTURO DA CIÊNCIA CRIMINAL: ABORDAGEM JÚRIDICA E PRÁTICA ACERCA DA UTILIZAÇÃO DO CIBERESPAÇO POR CIBERCRIMINOSOS E CIBERTERRORISTAS

Bruno Bassetto Gumiero

Presidente Prudente/SP

2022

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

FUTURO DA CIÊNCIA CRIMINAL: ABORDAGEM JÚRIDICA E PRÁTICA ACERCA DA UTILIZAÇÃO DO CIBERESPAÇO POR CIBERCRIMINOSOS E CIBERTERRORISTAS

Bruno Bassetto Gumiero

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Professor Marcus Vinícius Feltrim Aquotti.

Presidente Prudente/SP

2022

FUTURO DA CIÊNCIA CRIMINAL: ABORDAGEM JÚRIDICA E PRÁTICA ACERCA DA UTILIZAÇÃO DO CIBERESPAÇO POR CIBERCRIMINOSOS E CIBERTERRORISTAS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito.

_____

Marcus Vinícius Feltrim Aquotti

Orientador

_____

Sérgio Tibiriçá do Amaral

1º Examinador

_____

Matheus da Silva Sanches

2º Examinador

Presidente Prudente, 25 de novembro de 2022.

Salmos 40:

1 Esperei com paciência no SENHOR, e ele se inclinou para mim, e ouviu o meu clamor.

2 Tirou-me dum lago horrível, dum charco de lodo, pôs os meus pés sobre uma rocha, firmou os meus passos.

3 E pôs um novo cântico na minha boca, um hino ao nosso Deus; muitos o verão, e temerão, e confiarão no Senhor.

4 Bem-aventurado o homem que põe no Senhor a sua confiança, e que não respeita os soberbos nem os que se desviam para a mentira.

5 Muitas são, Senhor meu Deus, as maravilhas que tens operado para conosco, e os teus pensamentos não se podem contar diante de ti; se eu os quisera anunciar, e deles falar, são mais do que se podem contar.

6 Sacrifício e oferta não quiseste; os meus ouvidos abriste; holocausto e expiação pelo pecado não reclamaste.

7 Então disse: Eis aqui venho; no rolo do livro de mim está escrito.

8 Deleito-me em fazer a tua vontade, ó Deus meu; sim, a tua lei está dentro do meu coração.

9 Preguei a justiça na grande congregação; eis que não retive os meus lábios, Senhor, tu o sabes.

10 Não escondi a tua justiça dentro do meu coração; apregoei a tua fidelidade e a tua salvação. Não escondi da grande congregação a tua benignidade e a tua verdade.

11 Não retires de mim, Senhor, as tuas misericórdias; guardem-me continuamente a tua benignidade e a tua verdade.

12 Porque males sem número me têm rodeado; as minhas iniquidades me prenderam de modo que não posso olhar para cima. São mais numerosas do que os cabelos da minha cabeça; assim desfalece o meu coração.

13 Digna-te, Senhor, livrar-me: Senhor, apressa-te em meu auxílio.

14 Sejam à uma confundidos e envergonhados os que buscam a minha vida para destruí-la; tornem atrás e confundam-se os que me querem mal.

15 Desolados sejam em pago da sua afronta os que me dizem: Ah! Ah!

16 Folguem e alegrem-se em ti os que te buscam; digam constantemente os que amam a tua salvação: Magnificado seja o Senhor.

17 Mas eu sou pobre e necessitado; contudo o Senhor cuida de mim. Tu és o meu auxílio e o meu libertador; não te detenhas, ó meu Deus.

(BÍBLIA. Português. Bíblia Sagrada).

AGRADECIMENTOS

Antes de tudo, enalteço a Deus, pois foi Ele quem me iluminou e capacitou para que eu pudesse desenvolver a presente monografia cujo tema, há muito tempo atrás, já era cogitado e querido por mim.

À Nossa Senhora, mãezinha do céu, cheia de graça, responsável por derramar bênçãos em minha vida, te ofereço meu eterno amor. E com toda admiração, comparo-a com minha mãe aqui na Terra, Fabiana, que nunca deixou de me proteger e amparar. Todas às vezes, minha mãe, que alguém me disse não, você disse sim para o meu coração!

Agradeço a minha família, ao meu pai Ricardo que sempre prezou pelo pão nosso de cada dia, à minha irmã Larissa que esteve e estará comigo nos piores e melhores dias da minha curta jornada por este mundo, ao meu tio e padrinho, aos meus amigos, que sempre deram todo o suporte, seja na vida acadêmica, seja na vida pessoal, oferecendo tudo de mais bonito e sincero para que eu pudesse amadurecer, aprender e zelar pela minha essência imutável, porém aperfeiçoável.

Estendo meus agradecimentos aos meus professores, em especial ao meu orientador e, também, ao coordenador do curso de Direito que me auxiliaram do início ao fim deste presente estudo, explicando e corroborando para o progresso do trabalho, bem como aprimorando todas as tratativas aqui realizadas.

De fato, não foi uma tarefa fácil escrever, organizar o conteúdo, bem como aprimorar específicas teses que desenvolvi ao longo do trabalho. No entanto, torna-se extremamente prazeroso quando a consciência sabe que o melhor foi ofertado.

"Deus é amor e o amor é o melhor dia da evolução".

(Bono)

"Love is bigger than anything in its way"

(O amor é maior do que qualquer coisa em seu caminho). Música: U2. Letra: Bono.

RESUMO

Esta dissertação científica abordou questões acerca do exponente crescimento de ataques cibernéticos, impulsionados pela pandemia da covid-19, que gerou mudança de paradigma global. Globalmente falando, as economias estão determinadas a salvar vidas, bem como à sustentabilidade, porém, janelas de oportunidades se abriram e se abrem para os sindicatos do crime cibernético. Com recursos financeiros, de informação e humanos insuficientes, a economia global pode se encontrar em uma situação precária para combater a pandemia e os crimes cibernéticos concomitantemente, a menos que outros institutos ou órgãos essenciais à Justiça interessados, desempenhem um papel significativo para ajudar entes federativos a repelir cibercriminosos. Este estudo contribui, ainda, para debates sobre questões de segurança preventiva cibernética, parâmetros legais para o controle jurisdicional e competência acerca da aplicação da lei penal e processual penal no espaço. Além disso, compartilha-se casos práticos e dados científicos com o objetivo de informar e alertar sobre o início de uma nova pandemia mundial com proliferação de crimes no espaço virtual ou ciberespaço.

Palavras-chave: Cibercrimes. Cibercrime. Ciberespaço. Futuro do Direito Penal. Convenção de Budapeste. Crimes praticados pela internet.

ABSTRACT

This scientific dissertation addressed questions about the exponential growth of cyber-attacks, boost by covid-19 pandemic that generated a global paradigm shift. Globally speaking, economies are determined to save lives as well as sustainability, however, windows of opportunity have opened and are opening for cybercrime syndicates. With insufficient financial, information and human resources, the global economy may find itself in a precarious situation to fight the pandemic and cybercrimes at the same time, unless other institutions or bodies essential to the Justice concerned play a significant role in helping federative entities. to repel cybercriminals. This study also contributes to debates on preventive cyber security issues, legal parameters for jurisdictional control and jurisdiction over the application of criminal law and criminal procedure in space. In addition, practical cases and scientific data are shared with the aim of informing and warning about the beginning of a new global pandemic with proliferation of crimes in virtual space or cyberspace.

Keywords: Cybercrimes. Cybercrime. Cyberspace. Future of criminal law. Budapest Convention. Crimes committed on the Internet.

SUMÁRIO

1 INTRODUÇÃO

Preliminarmente, retrocederemos a meados de março de 2020, quando se prolifera de maneira crescente o surto da Covid-19. A partir desse momento de origem, ao traçarmos a linha do tempo “cibernético”, é como se neste lapso temporal do “choque” pandêmico, os seres humanos obrigatoriamente fossem forçados a adentrar em um mundo alternativo no qual o contato visual, a forma de trabalho, até mesmo as compras, somente seriam possíveis por meio de um único caminho: internet.

O impacto da pandemia afetou não só o quadro de saúde de diversas pessoas mas também a relação de consumo, a fim de que houvesse uma tentativa de oxigenar a economia e lutar pela própria sobrevivência em um período escasso.

O cenário retratado acima, isto é, do distanciamento social e, por consequência, da forte adaptação digital, pode-se dizer que fora uma realidade totalmente utópica e distante de acontecer, conforme a pretérita otimista perspectiva global. A bem da verdade é que, tudo isso trouxeram-nos das mais diversas heranças, a maior delas pode se dizer, do ponto de vista dos criminalistas e da criminologia quanto ciência social, o aumento intenso da criminalidade no ciberespaço e a utilização da tecnologia para cometer crimes de diversas naturezas.

Da popularização, ou seja, da imersão do indivíduo no novo espaço, dá-se o que alguns autores chamam de “cibersocialização” do mesmo, ou seja, a subsunção desse novo espaço no indivíduo. Surge, então, o ciberespaço, e, com ele, uma cibercultura.

A cada dia mais, o meio digital tem sido um antro de criminosos que se escondem atrás das redes criptografadas se aproveitando para cometer crimes virtuais, talvez por acreditarem que o fato de estarem por detrás de uma tela de computador, suas identidades estariam resguardadas por estarem criptografadas por softwares de última geração, ou simplesmente pelo fato de determinado crime não ser físico, mas virtual, e que por isso não sofreriam consequências judiciais. No entanto, tais conclusões são, em regra, equivocadas.

Com o surgimento inesperado da pandemia Covid-19, alterou-se, drasticamente, todos os modelos de negócios, as abordagens dos comportamentos e

estilos de vida das pessoas, “trabalhar em casa”, mas conectando-se remotamente à infraestrutura de sistemas de informação corporativa da empresa. Os cibercriminosos tiraram proveito do abalo social causado pela Covid-19. Indivíduos e sociedades empresariais foram e continuam a ser vítimas de ataques e ameaças cibernéticas.

O dinamismo e a versatilidade, inerentes à internet, tornaram-se foco de preocupação para o poder legislativo (porém não o suficiente), que editou as Leis 12.735/12, 12.737/12 (Lei Carolina Dieckman – altera os art. 154, 266 e 298 do CP) e 12.965/14 (Marco Civil da Internet).

Dessarte, a abstração do pensamento de que, atualmente, o Brasil está “dando seus primeiros passos” para estruturar a sistemática criminal quando do investimento na segurança digital, tanto legislativa quanto judiciária, não é de todo errado. Até porque, se houvesse uma legislação evoluída e uma estrutura técnica exemplar para combater ataques cibernéticos, o Brasil possuiria dados menos significativos e preocupantes.

Nota-se que, diante dos dados acima mencionados, há urgência de um planejamento defensivo e seguro para com o combate aos ataques cibernéticos, que estão cada vez mais frequentes e perigosos, visto que suas consequências extrapolam quaisquer limite geográfico ou jurisdicional.

Ao fim, no desenvolvimento da sistemática do tema, especificamente, dos tópicos um ao sétimo, utilizou-se a metodologia ativa em pesquisas embasadas em livros temáticos e artigos científicos, monografias excepcionais, teses de mestrado e doutorado, que desenvolveram temas correlacionados ao mundo cibernético e cooperação judicial entre nações para o combate/prevenção dos crimes cibernéticos e do ciberterrorismo. No tópico imediatamente anterior à conclusão, desenvolveu-se uma tese a partir de um caso hipotético, envolvendo o uso de deep fake que é um assunto de tratamento relevante e polêmico, pois, cada dia mais, torna-se fidedigno e inexiste qualquer regulamentação quanto ao seu uso desarrozoado.

2 DIREITO PENAL NO CIBERESPAÇO

Historicamente, a origem da internet é atribuída à idealização, em 1969, por cientistas do Departamento de Defesa dos Estados Unidos (DOD) de um sistema de interligação entre bases de dados de diversos centros de pesquisa militares no país, visando a transmissão de informações e documentos – isto, é evidente, ao cabo de anos de paulatino aprimoramento dos sistemas de computação mecânica e eletrodinâmica[1].

Dois anos depois, o primeiro e-mail foi enviado por Ray Tomlinson. Naquele ano, também aparece o primeiro vírus Creeper. No início dos anos 70, nasceu a palavra Internet, que era aplicada ao sistema de redes interconectadas por meio dos protocolos TCP e IP (Transmission Control Protocol / Internet Protocol) nos quais eles baseavam serviços de Internet e e-mails.

Nos arredores das décadas de 60 e 70, começara, gradativamente, a dispersão da internet atrelada com às novas ferramentas que facilitam as práticas ilícitas no meio virtual. Inova-se a tecnologia, inova-se as formas de se cometer crime, tem-se um efeito reflexo constante e contínuo.

A sociedade digital, também denominada sociedade em rede, é uma evolução da sociedade em que vivemos para um modelo social digital, no qual há uma união completa do mundo real com o mundo digital, visto que o ocorrido no ambiente cibernético afeta até mais as pessoas do que no ambiente físico.

Da popularização, ou seja, da imersão do indivíduo no novo espaço, se dá o que alguns autores chamam de “cibersocialização” do mesmo, ou seja, a subsunção desse novo espaço no indivíduo. Surge, então, o ciberespaço, e, com ele, uma cibercultura.

A cada dia mais, o meio digital tem sido um antro de criminosos que se escondem atrás das redes criptografadas, aproveitando-se para cometerem crimes virtuais, talvez por acreditarem que o fato de estarem por detrás de uma tela de computador, suas identidades estariam resguardadas por estarem criptografadas por *softwares* de última geração, ou simplesmente pelo fato de determinado crime não ser físico, mas virtual, e que por isso não sofreriam consequências judiciais. No entanto, tais conclusões são, em regra, equivocadas.

---

[1] FONSECA FILHO, Cléuzio. **História da computação: teoria da computação: teoria e tecnologia**. São Paulo: LTr, 1999, p. 106.

A partir de uma notícia extraída do site "*securityreport"*, uma estatística preocupante é citada (revelada pela consultoria alemã Roland Berger), de que o Brasil foi o 5º país que mais sofreu crimes cibernéticos no ano passado, com 9,1 milhões de ocorrências, somente no primeiro trimestre – mais que o ano inteiro de 2020[2].

Além disso, segundo as informações de outro site renomado sobre tais assuntos, chamado "Olhar Digital", nos revela:

> "**O Brasil segue como um dos países que mais sofre com ataques hackers. Dados da Checkpoint Research mostram que a média de ataques cibernéticos no segundo trimestre de 2022 teve aumento de 46%, uma diferença de 14% da média global, de 32%. Os dados ainda reforçam que a pandemia da Covid-19 teve grande influência nesses ataques realizados** e empresas têm sofrido cada vez mais pelos ataques ransomware. **Os dados revelam que o Brasil tem em média 1.540 incidentes de cibersegurança. O número é superior à média global de 1.200 ataques por semana"**. (Grifou-se).[3]

O saudoso Damásio de Jesus e José Antônio Milagre, na obra Manual de Crimes Informáticos (2016), explanam a seguinte reflexão: "*se há crimes é porque também há riqueza, e o que não falta na internet é riqueza"*. De fato, a internet traz consigo um campo incomensurável a ser explorado. Sendo assim, é inegável que, da mesma forma que a internet evolui para o bem, evolui para o mal.

2.1 O que são "crimes cibernéticos"?

A prática de crimes na internet assume várias nomenclaturas como cibercrime, crime digital, crime informático, crime informático-digital, *high technology crimes*, *computer-related* crime. Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes.

Não obstante haver quem faça distinção entre crime cibernético e crime informático, mesmo sendo a raiz de tal discussão é meramente doutrinária, prefere-se por utilizar, nesta dissertação, de forma indistinta, os seguintes termos: "crimes cibernéticos ou cibercrimes".

---

[2] Redação. Brasil foi o 5º país com mais ataques cibernéticos em 2021. **Security Report.** Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.YvhTG3bMK70. Acesso em 13 de ago. 2022.

[3] WILLIAM, S. Ataques cibernéticos no Brasil cresceram 46% no segundo trimestre. **Olhar Digital**, 09 ago. 2022. Disponível em: https://olhardigital.com.br/2022/08/09/seguranca/ataques-ciberneticos-brasil-cresce-46/. Acesso em 13 ago. 2022.

O Advogado especialista em Cibercrimes, Luiz Augusto Filizzola D'Urso (2019), conceitua cibercrime como *"um delito cometido de maneira virtual, utilizando a Internet como meio, ou envolvendo arquivos ou sistemas digitais/tecnológicos."* [4]

Os juristas Emerson Wendt e Higor Vinícius Nogueira Jorge, ambos Delegados de Polícia, autores da obra "Crimes Cibernéticos: ameaça e procedimentos de investigação", conceituam como tais: "*delitos praticados por intermédio de dispositivos informáticos (computadores, notebooks, celulares etc.) conectados ou não à internet*". [5]

Ainda sobre a referida obra, os criminalistas subdividem "crimes cibernéticos" em "crimes cibernéticos abertos" e "crimes exclusivamente cibernéticos". Assim dispõem:

> "**Com relação aos crimes cibernéticos abertos são aqueles que podem ser praticados da forma tradicional ou por intermédio de dispositivos informáticos, ou seja, o dispositivo é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele**. Dentre os tipos penais abarcados nesta modalidade então, por exemplo, crimes contra a honra, ameaça, furto mediante fraude, estelionato, falsificação documental, falsa identidade, extorsão, tráfico de drogas etc. **Já os crimes "crimes exclusivamente cibernéticos" são diferentes, pois eles somente podem ser praticados com a utilização de dispositivos informáticos**. Um exemplo é o crime de aliciamento de crianças praticado por intermédio de salas de bate-papo na internet, previsto no art. 244-B, §1º, do Estatuto da Criança e Adolescente (Lei nº 8.069/1990). Também são exemplos os crimes de interceptação telemática ilegal (art. 10 da Lei nº 9.296/1996), interceptação ambiental de sinais ilegal (art. 10-A da Lei nº 9.296/1996, invasão de dispositivo informático (art. 154-A do Código Penal), divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (art. 218-C do Código Penal), imagens de abuso infantil por meio do sistema informática/telemática (arts. 241-A, 241-B e 241-C da Lei nº 8.0869/2019), registro não autorizado da intimidade sexual (art. 216-B do Código Penal), a alteração do art. 122 do Código Penal, dobrando a pena quando a instigação ou indução ao suicídio ou automutilação ocorrem por meio da internet (Lei nº 14.132/2021), e as alterações/inclusões nos arts. 155, §4º-B (furto mediante fraude por meio de dispositivo eletrônico ou informático) e 171, §2º-A (fraude eletrônica), promovidas pela Lei nº 14.155/2021". (Grifou-se)[6].

---

[4] Artigo Científico. **OAB-SP**. Disponível em: https://www.oabsp.org.br/comissoes2010/gestoes2/2016-2018/acao-social/artigos/Artigo%20Cibercrime%20-%20Luiz%20Augusto%20DUrso.pdf. Acesso em: 20 maio. 2022.

[5] WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação. 3ª ed. Editora Brasport. 2021, p.14.

[6] Ibid, p. 15-16.

A advogada especialista em Direito Digital, Patrícia Peck Pinheiro, explica que:

> "(...) É importante ressaltar que o ciberespaço e a sociedade digital são duas coisas distintas, porém são totalmente interligadas.
> O ciberespaço é um local onde há a troca de conhecimentos e de informações, não possuindo um espaço físico, mas existindo de forma virtual, embora real.
> A sociedade digital, também denominada sociedade em rede, é uma evolução do status a quo da sociedade em que vivemos para o status ad quem, criando um modelo social digital, no qual há uma união completa do mundo real com o mundo digital, visto que o ocorrido no ambiente cibernético afeta até mais as pessoas do que no ambiente real, como no caso quando alguém sofre uma difamação por meio de uma rede social".[7]

No mais, percebe-se que os termos: "crimes cibernéticos, cibercrimes e ciberespaço" são os mais usuais dentre os autores citados neste trabalho científico.

2.2 Identificação de usuário na internet

Para que um usuário possa ser "encontrado", o provedor lhe atribui um número de protocolo (IP) exclusivo, pelo período de conexão. Podemos imaginá-lo como um documento de identificação único, como o CPF, por exemplo.

Cada máquina tem um registro de IP, conceituado pelo Marco Civil da Internet em seu art. 5º, inciso III como endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais.

Cada provedor de conexão (empresas que fornecem pacotes de internet), é obrigado a guardar o registro de acesso dos usuários, desse modo caso acionado judicialmente, deverá fornecer os registros de conexão. A supracitada Lei estabelece no art. 5º, inciso VI que registro de conexão é 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 e 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.

---

[7] PINHEIRO, Patrícia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016. p. 67.

Desse modo, se houver necessidade, o advogado, a autoridade policial ou membro do Ministério Público poderão ingressar com requerimento ao juiz para que seja expedida notificação ao provedor de aplicação de internet, a fim de informar os registros de acesso, com a finalidade de identificar o usuário. Todavia é importante ressaltar que o juiz verificará o justo motivo para que os acessos do usuário sejam divulgados, visto que haverá quebra de sigilo obtendo os dados cadastrais e da privacidade desse indivíduo na internet.

2.3 Condutas dos cibercriminosos através da Engenharia Social

Os cibercriminosos utilizam-se da engenharia social para executar suas ações. De acordo com o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (|CERT.br), a engenharia social é:

> Técnica por meio da qual uma pessoa procura persuadir a outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma 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. O popularmente conhecido “conto do vigário” utiliza engenharia social (CERT.BR, 2012).[8]

É demasiadamente lamentável analisar e estudar os cenários atuais dentro da criminologia. Primeiro porque, a evolução da tecnologia nos revela o lado obscuro de uma sociedade em colapso iminente, qual seja: a intensidade e a velocidade explosivas de uma conduta criminosa ou terrorista a ser praticada a qualquer momento, em qualquer tempo e lugar.

Segundo porque, a tratativa desse fenômeno da ciência cibernética associado àqueles que a utilizam visando a prática de crimes, deveriam merecer um tratamento proporcional ao referido binômio (intensidade-velocidade) pelos três poderes, quais sejam: Legislativo, Executivo e Judiciário.

O Legislativo deve ter a responsabilidade para adequar o regramento legal à evolução tecnológica, mediante o exercício de sua iniciativa de projetos de Lei

[8] CERT.BR. **Cartilha de Segurança para Internet, versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012**.

ou edição de atos administrativos infralegais, quando possíveis, para definições de novos conceitos que se agreguem às normas penais em branco (vide item 9.1).

O Executivo para fornecer subsídios, estrutura e cooperatividade no plano internacional para ratificar eventuais Tratados ou Convenções.

O Judiciário para reciclar de conhecimento de seus membros, atualizar o entendimento jurisprudencial e se posicionar adequadamente frente à constância evolução cibernética.

Por fim, ainda que não façam parte dos três poderes da Federação, mas considerando a importância que tem para a persecução penal, também é necessário que os membros da Polícia Judiciária e membros do Mistério Público mantenham-se preparados e atualizados para a investigação criminal e formulação de denúncias em desfavor dos cibercriminosos.

3 DOS BENS JURÍDICOS

O bem jurídico é elementar para a constituição da ciência jurídica penal, pode-se dizer que é, antes de tudo, o único fator embrionário que justifica a estruturação e a modulação de normas penais e processuais penais, pois, abrange todos os aspectos principiológicos.

Nesse sentindo, pode-se extrair o seguinte conceito de bem jurídico: valor (material e imaterial) cuja importância é tanto alta para o ser humano, que é necessário a tutela penal para a sua proteção eficiente.

De forma sucinta, tais características englobam a aplicação do direito penal em *ultima ratio,* escalonando, proporcionalmente, a gravidade da consequência à importância do bem protegido.

Partindo desse breve pressuposto, compreende-se que cada conduta legalmente incriminada protege um bem jurídico de extrema relevância. Antecedentemente ao fenômeno da globalização e do império da internet, o legislador se submeteu à tarefa de proteger bens como a vida, saúde, patrimônio, honra, etc., com o viés de uma sociedade “não conectada”.

Qualquer ofensa a um bem jurídico penalmente tutelado justifica a intervenção do Estado no sentido de exercitar o jus puniendi. A importância de um bem jurídico e seu grau de afetação servem como critério para o estabelecimento de penalidades proporcionais e razoáveis.

Segundo uma concepção dogmática do bem jurídico, o legislador não o cria por meio da norma, apenas constata a sua existência no mundo jurídico e sua importância na sociedade. Assim, é possível constatar que o bem jurídico limita o poder do legislador, uma vez que ele não pode ser fruto da subjetividade de um único homem ou grupo (PRADO, 2011, p. 27-38).

A construção de um determinado tipo penal deve ser feita com muito cuidado, considerando a gravidade do dano, o caráter subsidiário da esfera penal, o princípio da intervenção mínima e o da fragmentariedade. Como bem elucida Claus Roxin:

> “É aceito de forma dominante que a ameaça de uma pena criminal, como a mais grave das sanções, apenas entra em cena quando regulações menos gravosas não se mostrem suficientes. O assim caracterizado princípio da

> subsidiariedade, como máxima de limitação do direito penal, está no mesmo plano de que o princípio da proteção de bens jurídicos e possui significado político-criminal no mínimo de mesma importância". (ROXIN, 2014, p. 84).

Diante de tais ponderações, a exemplo dos crimes contra a honra, uma pessoa que cometa esse crime por meio da internet tem sua pena aumentada em um terço, visto que a utilização de tal meio resulta na aplicação do artigo 141, III do Código Penal, que prevê o aumento da pena caso o crime seja ocorrido por um meio que facilite a divulgação da calúnia, da difamação ou da injúria, considerando a magnitude na divulgação dos dados trazida pela Internet. Justifica-se o tratamento penal diferenciado pelo fato de que as informações divulgadas pela internet são, na maioria das vezes, impassíveis de completa exclusão.

A velocidade do compartilhamento de informações pode promover um dano enorme à vítima, muito superior ao da realização de tais crimes por qualquer outro meio como o jornal, as revistas ou outros meios físicos de divulgação.

A liberdade informática, decorrência direta da liberdade de informação, tutelada pelo art. 220 da Constituição Federal, compreende, consoante Paesani (PAESANI, 2002, p. 21-22), o aspecto ativo de informar e o aspecto passivo de ser informado, decorrendo, do equilíbrio entre esses dois âmbitos, a comunicação em uma sociedade pluralista. Face à ocorrência de abusos desse direito constitucionalmente assegurado, é verificada a necessidade de imposição de limites ao mesmo, instaurando-se o controle estatal sobre a expressão intelectual.

Por sua vez, a privacidade, um direito intrínseco aos indivíduos, deve ser protegida. No entanto, da mesma forma que a privacidade serve para assegurar o ato honesto dos bons cidadãos, serve para esconder as atitudes abusivas dos criminosos, e isto configura-se, nas palavras de Assis Medeiros, um aparente paradoxo, qual seja: "A monitoração é defendida para que se possa identificar os criminosos cibernéticos, mas, ao mesmo tempo, é uma espécie de crime contra as liberdades individuais" (MEDEIROS, 2002, p. 153).

Ainda sobre o suposto paradoxo relativo ao direito à privacidade do indivíduo, a melhor solução filosófica foi construída por Robert Alexy, autor da obra "teoria dos direitos fundamentais".

Colisões de direitos fundamentais nascem sempre que o exercício ou a realização de determinado direito fundamental acarrete consequências negativas em relação a outro direito fundamental de outra pessoa. Ex.: publicação de biografias não

autorizadas caracteriza um conflito entre liberdade de expressão e direito de informação contra direitos da personalidade (privacidade, imagem e honra).

Alexy entende que uma das soluções para a colisão entre regras é declarar uma delas inválida. Ou seja, quando dois princípios entram em colisão, ganha aplicação aquele princípio que, pelas circunstâncias concretas do caso, mereça primazia sem que isso importe na invalidade do princípio oposto.

Destaca-se duas passagens da obra de Robert Alexy sobre a teoria dos direitos fundamentais:

> "Princípios são mandamentos de otimização em face das possibilidades jurídicas e fálicas. A máxima da proporcionalidade em sentido estrito, ou seja, exigência de sopesamento, decorre da relativização em face das possibilidades jurídicas. Quando uma norma de direito fundamental com caráter de princípio colide com um princípio antagônico, a possibilidade jurídica para a realização dessa norma depende do princípio antagônico. Para se chegar a uma decisão é necessário um sopesamento nos termos da lei de colisão[9]

E nos termos da lei de colisão, idealizada por Alexy, a solução acontece da seguinte forma:

> "As colisões entre princípios devem ser solucionadas de forma completamente diversa. Se dois princípios colidem - o que ocorre, por exemplo, quando algo é proibido de acordo com um princípio e, de acordo com o outro, permitido-, um dos princípios terá que ceder. Isso não significa, contudo, nem que o princípio cedente deva ser declarado inválido, nem que nele deverá ser introduzida uma cláusula de exceção. Na verdade, o que ocorre é que um dos princípios tem precedência em face do outro sob determinadas condições. Sob outras condições a questão da precedência pode ser resolvida de forma oposta. Isso é o que se quer dizer quando se afirma que, nos casos concreto, os princípios têm pesos diferentes e que os princípios com o maior peso têm precedência. Conflitos entre regras ocorrem na dimensão da validade, enquanto as colisões entre princípios - visto que só princípios válidos podem colidir - ocorrem, para além dessa dimensão, na dimensão do peso"[10].

Nesse sentido, com vistas a promover uma repressão eficaz aos delitos cibernéticos, é fundamental uma ponderação entre os interesses acima descritos, sob a perspectiva da razoabilidade e proporcionalidade, tanto no âmbito legislativo quanto no jurisdicional. De forma que, além de se considerar essas questões controversas, é

---

[9] ALEXY, Robert. Teoria dos Direitos Fundamentais. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Editora Malheiros, 2008, p. 117.
[10] ALEXY, Robert. Teoria dos Direitos Fundamentais. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Editora Malheiros, 2008, p. 93-94.

preciso que se atente às peculiaridades do ambiente virtual, em virtude de seus traços característicos de “anarquia”, individualidade e autonomia.

3.1 Dos bens jurídicos nos crimes cibernéticos

A definição de um bem jurídico a ser tutelado nos crimes cibernéticos ou informáticos é de extrema relevância para o sistema penal brasileiro, sendo isso o que legitima a classificação de uma conduta como alguns autores chamam de “crime informático próprio” (aqueles em que o computador, normalmente por meio da Internet, é utilizado como mero meio para a realização do crime fim), permitindo que este seja tipificado, sem que condutas dignas de tutela penal não sejam criminalizadas.

Conforme entendimento de Jorge de Figueiredo Dias, uma das funções do bem jurídico é servir como padrão crítico para constituição de normas. Nesse sentido:

> “Ele deve servir, em segundo lugar, como padrão crítico de normas constituídas ou a constituir, porque só assim pode ter a pretensão de se arvorar em critério legitimador do processo de criminalização e de descriminalização (DIAS, 1999, p.65)”.[11]

Um exemplo disso é interferência em sistemas computacionais, aduzida por Vianna e Machado (VIANNA; MACHADO, 2013, p. 32- 33). Essa conduta é caracterizada pela ação do agente no sentido de impossibilitar o acesso dos dados armazenados no sistema, prática conhecida como Ataque de Negação de Serviço (DoS Attack – acrônimo em inglês para Denial of Service). Cotidianamente falando, essa conduta se define como a “retirada de um site do ar”. Essa ação causa sérios danos de ordem econômica aos sites de comércio eletrônico, que ficam impedidos de realizarem vendas e obterem lucro durante o período em que o site se encontra indisponível.

Diante da diferenciação doutrinária entre crimes informáticos próprios e impróprios, os autores supramencionados consideram que o bem jurídico dos crimes informáticos próprios é a inviolabilidade dos dados informáticos. Nesse sentido, eles

---

[11] DIAS, Jorge de Figueiredo. **Questões fundamentais do direito penal revisitadas**. São Paulo: Editora Revista dos Tribunais, 1999, p. 65.

defendem que essa ação deve ser tipificada, pois houve uma lesão indireta ao bem jurídico. Tais juristas explicam:

> “A inviolabilidade dos dados, neste caso, é protegida indiretamente, uma vez que perder a capacidade de processar os dados pode equivaler a perder os próprios dados. Não há, nessa hipótese um acesso ao dados armazenados no sistema. (VIANNA; MACHADO, 2013, p. 32-33)”.

Para a construção do bem jurídico proposto neste tópico, utiliza-se como base o conceito construído por Túlio Vianna e Felipe Machado, além da concepção construída pela Convenção de Budapeste. O primeiro conceito, diz respeito ao fato de que o bem jurídico é a informação armazenada nos dispositivos informáticos e não da inviolabilidade dos programas (VIANNA; MACHADO, 2013, p. 21). Ele foi construído sob a égide do artigo 5º, inciso X da Constituição Federal, que dispõe: “*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*”.

Já a segunda conceituação refere-se ao bem jurídico coletivo e tem sua base ancorada nos preceitos construídos pela Convenção de Budapeste. No âmbito internacional, tal Convenção é o único instrumento plurilateral que trata de legislação penal relativa aos crimes informáticos.

O instrumento fora criado com o objetivo de uniformizar a legislação penal internacional que trata de crimes informáticos, devido ao fato de que a internet é um meio global, salientando que sua eficiência dependerá de uma cooperação internacional. Em seu preâmbulo, sugere a criação de “uma política criminal comum direcionada à proteção da sociedade contra o cibercrime”, e em seu texto, propõe a criação de um bem jurídico denominado “segurança informática”, que possui três elementos: confidencialidade, integridade e disponibilidade dos dados informáticos.

Comprova-se a necessidade de uma reformulação da matéria penal no que tange as condutas ilícitas no campo da informática.

De forma geral, verifica-se que o simples fato de a conduta ser tipificada, não garante que o bem jurídico seja devidamente protegido, tendo em vista os problemas citados sobre a legislação brasileira, o que reforça a importância do estudo do bem jurídico para criação de uma política criminal eficiente.

4 CONVENÇÃO DE BUDAPESTE

4.1 Noções jurídicas preliminares

De acordo com o conceito dado pela Convenção de Viena Sobre o Direito dos Tratados, “tratado significa um acordo internacional concluído por escrito entre Estados e regido pelo Direito Internacional, quer conste de um instrumento único, quer de dois ou mais instrumentos conexos, qualquer que seja sua denominação específica”.

A expressão “tratado” é mais genérica, que abrange dentro de si diversas nomenclaturas. Em uma acepção mais específica, portanto, o termo Convenção nada mais é do que um acordo formalizado e concluído entre sujeitos de direito internacional público e destinado a produzir efeitos jurídicos. Convenção é um tratado que cria normas gerais.

No ano de 2001, em Budapeste, na Hungria, surge a Convenção sobre Cibercrimes, também conhecida como Convenção de Budapeste, a qual está em vigor desde 2004 e passou a vigorar em 2006 com o Protocolo Adicional à Convenção de Budapeste, que tipifica infrações de direitos autorais, fraudes informáticas, pornografia infantil e violações da segurança de rede, tudo em um só documento. A Convenção é composta por quatro capítulos e quarenta e oito artigos, considerada de fácil compreensão por não trazer expressões técnicas.

Tal Convenção de Cibercrimes tem como objetivo principal promover a proteção da sociedade contra a criminalidade no ciberespaço, através da designação de legislações adequadas e a cooperação internacional entres os entre os estados signatários e a indústria privada.

Trata-se de uma Convenção extremamente importante no que concerne a cooperatividade internacional em investigações e repressões de crimes cometidos pela internet, sendo o primeiro acordo internacional que visou a abordar a cibercriminalidade e a harmonizar as legislações, para que houvesse uma regulamentação geral entre as nações.

Atualmente 66 (sessenta e seis) países ratificaram o referido documento, outros 158 utilizam como orientação para suas legislações nacionais de combate aos crimes cibernéticos. A adesão do Brasil à Convenção de Budapeste foi aprovada pelo Senado no dia 15 de dezembro de 2021. O Projeto de Decreto Legislativo (PDL)

255/2021 foi relatado pelo senador Nelsinho Trad (PSD/MS) e, em atual momento, aguarda promulgação pelo Congresso Nacional[12].

4.2 Convenção de Budapeste e seu caráter internacional para o combate e a prevenção aos crimes cibernéticos

O artigo 23º da Convenção de Budapeste prevê princípios gerais relativos à cooperação internacional, dispondo da seguinte forma:

> "As partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas, e do seu direito nacional, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos a infrações penais relacionadas com sistemas e dados, ou para recolher provas sob a forma eletrônica de uma infração penal".

Entre as questões tratadas na Convenção de Budapeste estão a criminalização de condutas, normas para investigação e produção de provas eletrônicas e meios de cooperação internacional. Em novembro do ano de 2021, em seminário realizado pela Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados, o Ministério Público Federal (MPF) defendeu a urgência na aprovação do PDL para oficializar a adesão do Brasil ao tratado.

O pedido foi feito pelo procurador da República George Lodder, que integra o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF (2CCR/MPF). Nesta ocasião, ele ainda defendeu a inclusão, na legislação brasileira, da obrigação de sites e plataformas comunicarem os órgãos de persecução penal sobre casos de crimes praticados por seus usuários.

George Lodder esclareceu que, atualmente, muitas das informações sobre crimes de pedofilia e outros praticados no Brasil por meio da internet chegam ao conhecimento das autoridades nacionais por meio do *National Center for Missing & Exploited Children* (NCMEC), entidade privada sem fins lucrativos que atua nos Estados Unidos, onde a legislação estabelece que essa comunicação é obrigatória.

[12] Última atualização do processo legislativo ocorrida em 02 de novembro de 2022.

Para o membro do MPF, prever obrigação semelhante na legislação nacional representaria enorme avanço. Segundo extrai-se da matéria do site do Ministério Público Federal:

> "Hoje, não existe na legislação brasileira essa obrigação correspondente, de modo que, quando é uma empresa americana, temos sucesso em obter esses dados, mas quando se trata de plataforma de origem de outro país, como o TikTok, por exemplo, que é chinês, ou plataforma brasileira, isso nem sempre acontece", Segundo o procurador, muitas vezes as plataformas até têm interesse em compartilhar as informações, mas, como a prática não está prevista no marco legal brasileiro, têm receio de serem responsabilizadas pela captura e transferência dos dados aos órgãos de persecução".[13]

Frisa-se que a adesão ocorreu em um momento no qual o país emerge de uma pandemia sanitária de escala global, durante a qual o mundo se deparou com uma significativa escalada dos crimes cibernéticos, que vitimaram grandes empresas e até mesmo instituições públicas, por meio de condutas de sequestro de dados e extorsão.

Competência e Cooperação Internacional são vistas no Artigo 22º, o qual aponta quando e como uma infração é cometida, além de deixar a critério das Partes a "jurisdição mais apropriada para o procedimento legal".

O Comitê da Convenção de Crimes Cibernéticos (T-CY), formado por Estados Partes, observadores de países convidados a aderir à Convenção de Budapeste e participantes *ad hoc*, é a entidade responsável, entre outras, por realizar avaliações da implementação das disposições da Convenção de Budapeste, bem como por adotar pareceres e por expedir recomendações quanto à interpretação e implementação das suas principais disposições.[14]

Durante a Conferência Octopus de Cooperação contra o Cibercrime de novembro de 2021, que marcou o 20º aniversário da Convenção de Budapeste, os organizadores anunciaram que o Comitê de Ministros do Conselho da Europa aprovou a adoção do Segundo Protocolo Adicional à Convenção de Budapeste sobre

---

[13] BRASIL. Ministério Público Federal. **Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime** Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime.

[14] BRASIL. **Comitê da Convenção sobre Crimes Cibernéticos, "Regras de Procedimento T-CY. Conforme revisto por T-CY em 16 de outubro de 2020"**, Estrasburgo, 16 de outubro de 2020, disponível em: https://rm.coe.int/t-cy-rules-of-procedure/1680a00f34.

cooperação reforçada e divulgação de evidências eletrônicas, como originalmente adotadas pela 24ª Sessão Plenária do Comitê T-CY, em maio de 2021.

O texto do Segundo Protocolo Adicional será oficialmente aberto para assinatura entre os Estados Partes da Convenção de Budapeste dentro do ano de 2022.

O Segundo Protocolo Adicional à Convenção de Budapeste sobre cooperação reforçada e divulgação de provas eletrônicas regula, nomeadamente, a maneira como as informações e provas eletrônicas, incluindo informações de assinantes, dados de tráfego e dados de conteúdo, podem ser ordenadas e preservadas em investigações criminais entre Estados Partes no Convenção de Budapeste.

Desse modo, fornece uma base legal para a divulgação de informações relativas ao registo de nomes de domínio e outros aspectos essenciais relativos a investigações transfronteiriças, incluindo procedimentos de assistência jurídica mútua, cooperação direta com prestadores de serviços, divulgação de dados em emergências, proteção de salvaguardas para o acesso transfronteiriço aos dados e equipes conjuntas de investigação.[15]

[15] Veja o texto do Relatório Explicativo do Segundo Protocolo Adicional à Convenção de Budapeste elaborado pelo Comitê da Convenção sobre Crimes Cibernéticos (T-CY) em: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b.

5 JURISDIÇÃO E COMPETÊNCIA

Antes de aprofundar no tema de jurisdição e competência em crimes cibernéticos, é imprescindível fazer algumas prévias considerações sobre a aplicação da Direito Processual Penal no espaço.

Vigora no nosso ordenamento jurídico o princípio da territorialidade, que significa a aplicação da lei processual penal brasileira a todo delito ocorrido em território nacional (art. 1º, CPP), da mesma forma que se utiliza em direito penal (art. 5º, CP). É regra que assegura a soberania nacional, tendo em vista não haver sentido aplicar normas procedimentais estrangeiras para apurar e punir um delito ocorrido dentro do território brasileiro. O direito alienígena é composto pela vontade de outro povo, razão pela qual os magistrados, em nosso país, não cumprem e não devem, de fato, seguir legislação que não seja fruto do exclusivo desejo da nação brasileira.

Um dos fatores de afastamento da aplicação da lei processual penal é a ressalva feita aos tratados, convenções e regras de direito internacional (art. 1º, I, CPP).

Nesse contexto, como já visto anteriormente, a tendência é que a Convenção de Budapeste seja inserida no nosso ordenamento, até porque, uma vez ratificada, aderimos a ela. Desse modo, deverão ser respeitados os procedimentos de cooperação internacional sobre as apurações e prevenções de crimes cibernéticos entre os países membros.

Caso, então, o Brasil vier a firmar um tratado, uma convenção ou participe de uma organização mundial qualquer, cujas regras internacionais a norteiem, deve a lei processual penal pátria ser afastada para que outra, proveniente de tais fontes, em seu lugar, seja aplicada.

O Desembargador e doutrinador Guilherme de Souza Nucci nos ensina sobre o tema da territorialidade:

> “Os tratados e convenções subscritos pelo Brasil podem excepcionar a aplicação da lei brasileira a crime cometido no território nacional, como ocorre com a Convenção de Viena em relação às imunidades diplomáticas. Diplomatas estrangeiros, que praticam infrações penais no Brasil, estão imunes à jurisdição nacional”.[16]

[16] NUCCI, Guilherme de Souza. **Curso de Direito Processual**. 18. ed. – Rio de Janeiro: Forense, 2021, p. 163.

Jurisdição é o poder-dever atribuído, constitucionalmente, ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos. (CAVALLO, La Sentenza penale, p.38, tradução livre).

O Supremo Tribunal Federal tem competência para exercer sua jurisdição em todo o Brasil, embora, quanto à matéria, termine circunscrito a determinados assuntos. Não pode, por exemplo, o Ministro homologar um acordo de partes de qualquer lugar do país, embora possa, conforme o caso, apreciar um habeas corpus de pessoa presa em qualquer ponto do território brasileiro. Enfim, jurisdição todo magistrado possui, não obstante a competência, devidamente fixada em normas constitucionais e através de leis, seja diferenciada.

Jurisdição é força, é virtude, é poder. Competência é simples possibilidade, qualidade daquilo que não contradiz, que não ultrapassa os limites impostos por lei.

Em síntese, todo juiz, investido na sua função, possui jurisdição, o que é a atribuição de compor os conflitos emergentes na sociedade, valendo-se da força estatal para fazer cumprir a decisão compulsoriamente.

Há princípios que regem a jurisdição criminal, são eles:

a) Indeclinabilidade: o juiz não pode abster-se de julgar os casos que lhe forem apresentados;
b) Improrrogabilidade: as partes, mesmo que entrem em acordo, não podem subtrair ao juiz natural o conhecimento de determinada causa, na esfera criminal;
c) Indelegabilidade: não pode o juiz transmitir o poder jurisdicional a quem não o possui;
d) Unidade: a jurisdição é única, pertencente ao Poder Judiciário, diferenciando-se apenas no tocante à sua aplicação e ao grau de especialização, podendo ser civil – federal ou estadual; militar – federal ou estadual; eleitoral ou trabalhista.

Competência

Competência trata-se de uma limitação da jurisdição, ou seja, o espaço dentro do qual pode determinada autoridade judiciária aplicar o direito aos litígios que lhe forem apresentados, compondo-os. A título de exemplo didático-ilustrativo, jurisdição é como se fosse um “bolo inteiro” e a competência seria cada pedaço que, posteriormente, viesse a ser cortado.

Quando houver previsão típica em tratado ou convenção internacional cumulada com a transnacionalidade de crimes cibernéticos, a competência será da justiça federal. Assim dispõe a Carta Magna:

> “Art. 109. Aos juízes federais compete processar e julgar:
> V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente”.

A Justiça Estadual zelaria, então, pelos demais casos de crimes cibernéticos, cometidos dentro do país.

Entende a maioria dos doutrinadores que somente são passíveis de delegação as regras de competência, isto é, o limite para o exercício do poder jurisdicional. Assim, para que um juiz ouça uma testemunha residente em outra Comarca, fora de sua competência, expede uma carta precatória, delegando a possibilidade de colher a prova a outro magistrado.

Nos dizeres de Nucci:

> “Lembremos que *delegar* é transmitir poderes, atribuições ou meramente incumbir alguém de fazer algo, exatamente o que faz o deprecante: transmite o poder de convocar e ouvir uma testemunham que diz respeito a processo seu, a outro juízo. Estende-se a competência do juiz em face de delegação autorizada em lei. Por outro lado, se um desembargador pode ir à Comarca do interior onde se encontra determinada testemunha para inquiri-la, mas prefere não o fazer, deprecando o ato (carta de ordem), está autorizando, por delegação de competência, que o juiz local o faça.
> Não é uma questão de transmitir poder jurisdicional, mas de conferir competência a magistrado que não a possui. Essa parece-nos ser a questão central, que autoriza a concluir ser delegável apenas a competência, de acordo com os ditames legais”. (Curso de Direito Processual. Guilherme de Souza Nucci. – 18. ed. – Rio de Janeiro: Forense, 2021. Pg. 312)”.

Há entendimento doutrinário, no entanto, que considera não haver hipótese alguma para delegação, seja de jurisdição, seja de competência.

Por exemplo, quando um juiz expede precatória a outro, nada mais faz do que transmitir uma solicitação para que o deprecado proceda a uma inquirição ou colha uma prova que está dentro da sua esfera de competência, visto que o deprecante não poderia fazê-lo. Nessa linha: Greco Filho, Tornaghi, Assaf Maluf dentre outros.

Por sua vez, o artigo 70 do Código de Processo Penal disciplina a competência pelo lugar da infração penal:

> "Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
> § 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção".

A competência em regra é determinada em razão do lugar onde a conduta criminosa se consumou ou no caso de crime tentado, no local da prática do último ato de execução. Contudo, levando-se em conta que o crime cibernético não apresentará apenas um alcance local, mas em muitos casos de ordem internacional, surge a necessidade de que tais crimes sejam estudados observando-se se os efeitos por eles produzidos incidem apenas em território nacional, mesmo que em diferentes localidades, ou se ultrapassam os limites territoriais brasileiros.

A competência se subdivide em:

a) Absoluta: hipótese de fixação de competência que não admite prorrogação, isto é, deve o processo ser remetido ao juiz natural determinado por normas constitucionais ou processuais penais, sob pena de nulidade do feito. Encaixam-se nesse perfil a competência em razão da matéria (ex. federal ou estadual; criminal ou cível; matéria criminal geral ou especializada como o júri etc.) e a competência em razão da prerrogativa de função (ex. julgamento de juiz de direito deve ser feito pelo Tribunal de Justiça etc.).

b) Relativa: hipótese de fixação de competência que admite prorrogação, ou seja, se não invocada a tempo a incompetência, tem-se como competente o juízo que conduz o feito, não se admitindo qualquer alegação posterior de nulidade.

É bem verdade que não há um consenso consagrado em nossa jurisprudência acerca da aplicação das regras de jurisdição e competência quando envolve crimes cometidos no ciberespaço. No entanto, há o critério norteador consagrado na Constituição Brasileira (art. 109, inc. V).

Não obstante tal “deficiência”, existente em nosso ordenamento, adveio, como já exposto, do processo de inclusão da importante Convenção de Budapeste para servir de parâmetro para facilitar e promover a cooperação jurídica internacional entre as Nações.

5.1 Contato com os Provedores Estrangeiros – Cooperação Internacional Jurídica e Policial

A dificuldade investigativa surge quando estamos frente a um provedor estrangeiro, que não possui escritório de representação aqui no Brasil. Assim, no caso de e-mail, site ou conexão de internet de responsabilidade do provedor estrangeiro, deve-se contatar o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), da Secretaria Nacional de Justiça (SNJ), vinculada ao Ministério da Justiça e da Segurança Pública.

Em razão de o Brasil ser signatário de um tratado para cooperação judicial (Mutual Legal Assistence Treaty – MLAT), órgãos investigativos do país podem representar pela concessão desse tipo de medida investigativa.

Para o requerimento de informações a serem requeridas a Estados estrangeiros, alguns elementos devem constar do pedido de cooperação internacional a ser formulado pelas autoridades brasileiras competentes e algumas providências prévias e específicas podem ser tomadas antes ou concomitantemente ao envio de uma solicitação de assistência relacionada a crimes cibernéticos.

Nos casos em que é necessária uma cooperação que envolva medida judicial, como uma quebra de sigilo ou medida que, necessariamente, comporte uma decisão judicial, os pedidos passam, no Brasil, pelo Ministério da Justiça, por intermédio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), departamento este que está incluso à Secretaria Nacional de Justiça e Segurança Pública.

Os pedidos de cooperação internacional possuem base nos tratados e acordos bilaterais firmados pelo Brasil (vide a Convenção de Budapeste) e, via de

regra, consistem na obtenção de dados cadastrais, de tráfego (de conexão) ou de conteúdo.

Lembrando que a cooperação jurídica internacional só será necessária fora das hipóteses previstas no Marco Civil da Internet, ou seja, quando se tratar de provedor de serviço localizado no exterior e que não preste serviço no Brasil.

O Brasil ainda faz parte da rede para assuntos de crime e informática (*network for computer crime matters*) e, de acordo com o documento firmado entre os países signatários, o contato no Brasil é o Setor de Crimes de Informática da Polícia Federal.

A Direção-Geral da Polícia Federal está sediada em Brasília e lá se encontram as ramificações da Direção-Geral, dentre as quais existe a Divisão de Repressão a Crimes Cibernéticos (DRCC), que, por sua vez, é subdividida em Núcleos, quais sejam, o Núcleo de Repressão a Crimes de Alta Tecnologia, o Núcleo de Repressão a Fraudes Bancárias e o Núcleo de Repressão a Crimes de Ódio e Pornografia Infantil.

Referidos órgãos centrais não têm função de execução, ou seja, não fazem a condução dos inquéritos policiais, mas sim coordenam e unificam os procedimentos, os treinamentos, o desenvolvimento de novas tecnologias para a investigação e para a cooperação com outros órgãos, tanto no Brasil e no exterior.

Em questão de crimes cibernéticos, como já alertado, a cooperação com outros órgãos estrangeiros é de suma importância, já que tais infrações penais não conhecem fronteiras.

Diante do rápido avanço da tecnologia, a Polícia Federal, visando a acompanhar tal característica inerente também aos crimes cibernéticos, vem desenvolvendo projetos, tais como o “**Projeto Tentáculos**”, para o combate a fraudes bancárias eletrônicas, o “**Projeto Prometheus**”, que visa a aumentar o resultado operacional da Polícia Federal para a racionalização de instauração de inquéritos policiais, o “**Sistema ePol**”, que é um sistema totalmente online de tratamento das investigações, abolindo o uso de papel, a ferramenta “**LED**”, que é um localizador de evidências digitais e foi desenvolvida pela perícia da própria Polícia Federal, cujo objetivo é auxiliar Policiais Federais à localização de evidências digitais que comprovem o armazenamento e/ou compartilhamento de arquivos relacionados aos crimes de abuso e de exploração sexual infantil, sem necessidade de acesso a cada

arquivo individual pelo investigador, ou seja, a pesquisa é feita de forma global por meio de algoritmo, acelerando e facilitando a busca e preservando a prova.

Ainda sobre crimes sexuais contra crianças e adolescentes, a Polícia Federal desenvolveu o “**Sistema Rapina**”, que é alimentado com dados do NCMEC (National Center for Missing and Exploited Children), que por sua vez, é uma organização não governamental, sem fins lucrativos, que recebeu apoio do Governo norte-americano para estabelecer um mecanismo centralizado de recebimento de “denúncias” sobre crimes relacionados a abuso sexual infantil e desaparecimento de crianças.

O diálogo da Polícia Federal com órgãos internacionais é corriqueira, cabendo citar a integração constante com os principais órgãos como FBI, Interpol, Americapol e Europol. Quanto a Interpol cabe registrar que há representante dentro da Polícia Federal em solo brasileiro, portanto, pedidos de cooperação policial internacional é feito diretamente para o responsável pela Interpol dentro da Polícia Federal, que encaminha o pedido para os órgãos de investigação de cada estado-membro demandado.

Destarte, é notória a mudança social abarcada pela globalização da internet, que trouxe nova forma de comunicação e modificou as relações sociais em todo o mundo. Contudo, junto com tais benefícios, surgiram também novos riscos, impondo a necessidade de um controle jurídico mais eficaz, bem como de fortificar a cooperatividade jurídica e policial internacionais, facilitando assim a persecução penal.

6 DOS CIBERCRIMES

6.1 Furto eletrônico

No ano de 2020, em razão da pandemia do coronavírus, milhões de pessoas tiveram de permanecer a maior parte do tempo em suas casas e passaram a utilizar com maior frequência serviços eletrônicos das mais diversas espécies, o que multiplicou de forma preocupante os casos de fraude eletrônica.

Por tal razão, o legislador penal resolveu acrescentar uma figura qualificada ao artigo 155 do Código Penal, visando a punir de forma mais severa o crime de furto quando praticado por meio eletrônico ou dispositivo informático:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
> Furto qualificado
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
> I - com destruição ou rompimento de obstáculo à subtração da coisa;
> II - com abuso de confiança, ou mediante fraude, escalada ou destreza;
> III - com emprego de chave falsa;
> IV - mediante concurso de duas ou mais pessoas.
> § 4º-A A pena é de reclusão de 4 (quatro) a 10 (dez) anos e multa, se houver emprego de explosivo ou de artefato análogo que cause perigo comum. (Incluído pela Lei nº 13.654, de 2018)
> **§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)**. (Grifou-se).

A fraude de qualquer espécie é qualificadora tradicional do furto nos termos do artigo 155, § 4º., II, CP. Ocorre que, com o advento da Lei 14.155/21, o legislador criou uma qualificadora específico (artigo 155, § 4º. – B, CP), também baseada no elemento da fraude.

Então, o chamado “Furto Eletrônico ou Informático” será caracterizado pela fraude, mas com o detalhe de ter sido praticada com emprego de “dispositivo eletrônico ou informático”, não exigindo a tipificação que tal dispositivo seja

necessariamente conectado à internet, ou que haja necessariamente violação de mecanismo de segurança ou utilização de programas maliciosos.

O § 4º - B, em estudo, termina sua descrição com a fórmula genérica de "qualquer outro meio fraudulento análogo", o que aparentemente causa um conflito desta com a norma genérica do "Furto mediante Fraude" do § 4º., II.

No entanto, esse conflito não se justifica.

Esses meios fraudulentos genéricos devem ser interpretados por analogia a qualquer situação que, necessariamente, envolva o uso da tecnologia eletrônica e/ou informática. Outras fraudes, praticadas por meios diversos, serão tipificadas no antigo artigo 155, § 4º., II, CP.

Eduardo Luiz Santos, Delegado de Polícia Civil, faz a seguinte observação:

> "Importa ainda ter em mente que o emprego de dispositivo informático há que ser "meio" ou "instrumento" para a prática do crime, não apenas integrante da conduta ou forma de o agente obter a subtração. Por exemplo, se um indivíduo consegue convencer alguém a convidá-lo para uma festa, por meio de conversa telefônica ou por troca de mensagens de WhatsApp, a fim de furtar objetos na casa dessa pessoa, comete o furto mediante fraude previsto no artigo 155, § 4º., II, CP e não o furto eletrônico em estudo. O dispositivo informático não foi instrumento do crime, mas apenas a forma pela qual o infrator se comunicou com a vítima".[17]

Vejamos a seguir uma jurisprudência paradigmática anterior à vigência da supracitada Lei 14.155/21.

Uma breve pesquisa realizada na página eletrônica do Superior Tribunal de Justiça nos revela reiteradas decisões em conflitos de competência relativos a subtrações fraudulentas cometidas pela rede mundial de computadores, nas quais a conduta é executada em um lugar e o patrimônio atacado se encontra em outro.

O caso abaixo trata-se, atualmente, de furto eletrônico, em que houve subtração de valores mediante transferência eletrônica fraudulenta.

A Terceira Seção do STJ firmou entendimento, à época, no sentido de que a subtração de valores de conta-corrente mediante transferência eletrônica

---

[17] CABETTE, Eduardo Luiz Santos. **Invasão de dispositivo informático, furto eletrônico, estelionato eletrônico e competência – Lei 14.155/21**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 26, n. 6613, 9 ago. 2021. Disponível em: https://jus.com.br/artigos/92210/invasao-de-dispositivo-informatico-furto-eletronico-estelionato-eletronico-e-competencia-lei-14-155-21. Acesso em: 28 maio 2022.

fraudulenta configura crime de furto, previsto no artigo 155, parágrafo 4º, inciso II, do Código Penal.

Segue a ementa:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSUAL PENAL. FURTO MEDIANTE FRAUDE. TRANSFERÊNCIA BANCÁRIA VIA INTERNET SEM O CONSENTIMENTO DA VÍTIMA. CONSUMAÇÃO NO LOCAL DA AGÊNCIA ONDE O CORRENTISTA POSSUI A CONTA FRAUDADA. COMPETÊNCIA DO JUÍZO SUSCITADO.
> 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP.
> 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal - CPP; no caso, na Comarca de Barueri/SP.
> Conflito de competência conhecido para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, o suscitado.

A Terceira Seção do Superior Tribunal de Justiça firmou, então, o entendimento de que o juízo competente para julgar o caso acima descrito é o de Barueri, uma vez que o delito em questão fora consumado no local da agência bancária onde a vítima possuía conta.

Antes da alteração legislativa, essas subtrações se subsumiam à qualificadora do art. 155, § 4º, inc. II, com pena de dois a oito anos.

No entanto, em razão dos prejuízos provocados e da maior dificuldade de apuração revelada nesses casos, é que decidiu o legislador inserir no art. 155 o Código Penal uma qualificadora específica, para as situações em que o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático. Logo, o novo enquadramento legal, agora, é aquele previsto no art. 155, §4º - B.

O advogado criminalista, Procurador de Justiça aposentado e doutor em Direito Penal, Cezar Roberto Bitencourt, critica essas alterações legislativas, pois segundo ele, criaram-se três subespécies da prática da qualificadora (§4 – B), utilizando-se sempre, como meio, dispositivo informático ou eletrônico. Em suas palavras:

> "**Trata-se, inegavelmente, de uma tipificação esdrúxula, prolixa e mal constituída**, como tem ocorrido frequentemente com as alterações criadas

> pelo atual legislador. **Exige, a rigor, um grande esforço do intérprete para dissecar seus elementos constitutivos, inclusive os *meios* e *modos* utilizados pelo infrator na prática criminosa. O legislador, pelo que se depreende, motivado pelo acréscimo desse *modus operandi* adotado na *subtração da coisa alheia móvel*, qual seja, a utilização da *eletrônica* no crime de furto**, decidiu *"qualificar"* essa conduta, considerada fraudulenta pelo legislador, na *"subtração da coisa alheia móvel"*, elevando excessivamente a pena cominada, fixando-a entre quatro e oito anos de reclusão e multa". (Grifou-se).[18]

O criminalista continua a criticar o texto legal do §4 - B, que segundo seu ponto de vista, fora mal redigido, *in verbis*:

> "**É irrelevante, para a definição legal, que referido dispositivo esteja ou não conectado à *rede de computadores* e que haja ou não violação de mecanismo de segurança porventura existente. No entanto, a não conexão da rede de computadores diminui ou até elimina a sua periculosidade, posto que sem rede e sem conexão virtual reduz-se consideravelmente o dano que a gravidade dessa ação delituosa poderia produzir**. Convém destacar que a gravidade da conduta estando conectado à *internet* (ou similar) é uma e, na sua ausência, será outra consideravelmente inferior. Pois, para o legislador a maior gravidade dessa *conduta fraudulenta de subtrair* coisa alheia móvel, ciberneticamente, reside exatamente na utilização da rede mundial de computadores ou similar, na comunicação virtual e instantânea, na maior facilidade de execução, quando o infrator se utiliza de *meio eletrônico ou informático*.
> **Em outros termos, a maior punição dessa forma qualificada de subtração da coisa alheia móvel fundamenta-se, principalmente, *na utilização dessa tecnologia avançada* para *fraudar* ou *ludibriar* a atenção da vítima, dificultando e, por vezes, até inviabilizando a autoproteção pessoal e patrimonial. Com efeito, nessas circunstâncias, qualquer vítima, fica totalmente *vulnerável*, à mercê da picardia, da habilidade e da maldade dos denominados *"ladrões cibernéticos"*, justificando-se, na ótica do legislador, a punição desse tipo de crime, com uma pena de reclusão tão grave.**
> **A rigor, o texto legal não identifica com segurança a configuração de *fraude* no simples uso de dispositivo eletrônico informático, especialmente quando desconectada da rede mundial de computadores (ou similares), pois constituiria a *mera utilização da tecnologia moderna*, aliás, usada no quotidiano. Seria *somente a utilização de um meio informático*, já penalizada pela própria qualificadora. Essa definição demanda uma boa interpretação de nossos Tribunais, especialmente pela gravidade da punição, especialmente quando não conectado na rede mundial de computadores ou outras redes similares"**. (Grifou-se).[19]

---

[18] BITENCOURT, Cezar Roberto. Furto mediante uso de dispositivo eletrônico ou informático. **Revista Consultor Jurídico**. Disponível em: https://www.conjur.com.br/2021-jun-14/bitencourt-furto-mediante-uso-dispositivo-eletronico-ou-informatico. Acesso em 29 maio 2022.
[19] Ibid.

O renomado jurista, portanto, critica a falta de técnica redacional dos legisladores. E continua seu posicionamento lançando críticas quanto ao exagero das penas previstas na qualificadora, assim como a ilogicidade da própria descrição legal, pois a presença da conjunção alternativa “ou” (“conectado ou não à rede de computadores”) pressupõe um patamar de mesma gravidade, mas que, na realidade, não é. Até porque, segundo Bitencourt, a ausência de conexão à rede de computadores diminui substancialmente ou até elimina a sua periculosidade, pois, sem rede e sem conexão virtual reduz-se consideravelmente a gravidade do dano que essa ação delituosa poderia produzir em escala nacional e internacional.

6.1.1 Da causa de aumento de pena quando o crime é cometido mediante a utilização do servidor fora do território nacional

Dispõe o Código Penal:

> “§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021) **I** – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; (Incluído pela Lei nº 14.155, de 2021)”.

O fundamento da majoração está na constatação de um maior “poder de fogo” do agente, que dispõe de conhecimentos e/ou recursos para fazer uso dessa estratégia mais sofisticada de valer de servidores localizados em países estrangeiros.

Outro ponto a se considerar é a maior dificuldade de investigação que decorre dessa transnacionalidade contida na majorante em estudo.

6.2 Do crime de Estelionato Virtual

O termo estelionato provém da expressão grega *stelio* que dá nome a uma espécie de lagarto que muda de cor para iludir suas presas. A origem da palavra atenta para a tipificação do delito cometido pelo estelionatário, que usa artifícios para enganar alguém.

O autor do crime de estelionato emprega artifício ardil ou qualquer meio fraudulento para induzir ou manter a vítima em erro, com o objetivo de obter para si ou para terceiros vantagem indevida. Pune-se aquele que, por meio da “malícia”,

“engodo”, “mentira”, procura a despojar a vítima de seu patrimônio fazendo com que ela entregue voluntariamente a coisa visada, evitando, assim, retirá-la por meios violentos.

O estelionato é um crime doloso que se consuma com a efetiva obtenção da vantagem ilícita pelo autor, em prejuízo da vítima. Tutela-se a inviolabilidade patrimonial, aviltada pela prática de atos ilusórios pelo agente.

O crime de estelionato é tipificado no artigo 171 do Código Penal e possui a seguinte descrição:

> 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.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> § 2º - Nas mesmas penas incorre quem:
> Disposição de coisa alheia como própria
> I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> Alienação ou oneração fraudulenta de coisa própria
> II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> Defraudação de penhor
> III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
> Fraude na entrega de coisa
> IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> Fraude para recebimento de indenização ou valor de seguro
> V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
> Fraude no pagamento por meio de cheque
> VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.

Este era o arcabouço legal em vigência antes da alteração promovida no ano de 2021.

A recente modificação prevista no crime do artigo 171, acrescentou uma nova modalidade de estelionato, por meio eletrônico, mas, por infelicidade legislativa ou não, esta alteração atraiu críticas que serão abaixo melhor detalhadas.

6.2.2 Da alteração legislativa e o “estelionato virtual”

Adiante, destaca-se a alteração recente no Código Penal, pela Lei nº 14.155, de 2021, que trouxe a modalidade de estelionato por meio de fraude eletrônica. O dispositivo legal possui o seguinte texto:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. (Grifou-se).

O crime de estelionato também passou a contar com uma qualificadora semelhante àquela tratada no furto. Neste caso, contudo, a lei não faz menção específica ao dispositivo eletrônico ou informático, que, no furto, pode ser invadido por meio de manobras fraudulentas. A invasão é justamente o que possibilita a subtração sem que a vítima se dê conta.

No caso do estelionato, é mais grave a conduta de quem obtém vantagem utilizando informações fornecidas pela vítima ou por terceiro induzido em erro (divisões elencadas pelo Rogério Sanches Cunha, Promotor de Justiça)[20]:

> “a) por meio de redes sociais: atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados;
> b) por contatos telefônicos: são também muito comuns as fraudes cometidas por meio telefônico. Uma situação que se vê com certa frequência é o envio de mensagem (por WhatsApp, por exemplo) na qual o estelionatário se identifica como amigo ou familiar da vítima e lhe pede um depósito bancário devido a uma emergência. Sem dar-se conta, a vítima efetua o depósito na conta do criminoso;
> c) pelo envio de correio eletrônico fraudulento: neste caso, a vítima recebe um e-mail fraudulento, muitas das vezes imitando os caracteres de empresas ou de organizações conhecidas e, a partir do acesso por meio do link disponibilizado, insere dados de cartão de crédito ou efetua pagamentos de compras simuladas, o que proporciona a vantagem ao estelionatário;

[20] BRASIL. **Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP**. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/. Acesso em: 29 maio 2022.

> d) <u>por qualquer outro meio fraudulento análogo</u>: nesta fórmula analógica se inserem quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, como páginas na internet, por exemplo, em que a vítima não é diretamente abordada pelo estelionatário, como nas modalidades anteriores, mas é induzida em erro por fatores diversos (simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada etc.)".

De fato, os autores do crime de estelionato virtual, na maioria dos casos, possuem notório saber técnico-informático, pois precisam de um conhecimento mais apurado para manejar redes sociais, sites, correio eletrônico, ou algoritmos cibernéticos em geral.

E quanto maior o conhecimento tiver um estelionatário virtual, maior será a probabilidade de dano à vítima, sem contar a maior dificuldade de identificação da autoria.

Não é à toa que a quantidade de "golpes" continua a crescer, mas agora, este motivo se dá pelo aumento da qualidade ardilosa empregada pelos cibercriminosos para ludibriar a vítima e prejudicá-la.

Assevera o ilustríssimo doutrinador e Promotor de Justiça, Rogério Sanches Cunha:

> "**Ao contrário do que acontece no furto, a vítima, ao fornecer informações que possibilitam a prática do crime, integra diretamente o ardil preparado pelo estelionatário para obter a vantagem indevida**. Ilustremos com exemplos ambas as figuras para bem diferenciá-las:
> a) Aproveitando a vulnerabilidade de pessoas que utilizam uma rede pública de internet, um hacker intercepta a conexão e obtém dados de acesso a contas bancárias. Com esses dados à disposição, acessa as contas e transfere quantias em dinheiro para outra conta da qual efetua saques. É um caso típico de furto mediante fraude, no qual a manobra ardilosa (interceptar os dados transmitidos entre o usuário e o ponto de conexão) é utilizada para que as vítimas sejam despojadas de seus bens sem que nada percebam.
> b) Pretendendo adquirir um televisor, um indivíduo faz uma pesquisa na internet e encontra a página de uma conhecida rede varejista na qual o produto está sendo anunciado por um preço muito abaixo das concorrentes. Insere seus dados pessoais e bancários sem saber que, na verdade, se trata de uma página clonada, que apenas copia os caracteres da famosa rede varejista, para induzir as pessoas em erro. Efetuado o pagamento, o dinheiro é creditado ao autor da fraude, que evidentemente não pretende entregar o produto anunciado. Nesse exemplo, ao contrário do anterior, a vítima tem participação direta, pois, induzida por um anúncio enganoso, fornece os dados para que o autor da fraude possa obter a vantagem. Trata-se, portanto, de estelionato."(Grifou-se).[21]

[21] Ibid.

Sobre questões de competência nos crimes de estelionato comum e virtual, há tratamento diverso conferido pela legislação, notadamente quando a fraude se der mediante atos de natureza bancária, conforme o que dispõe o §4º do artigo 70 do Código de Processo Penal.

A regra geral, prevista no artigo 70 do Código de Processo Penal, conforme leciona Vicente Greco Filho, fixa a competência a partir do local da consumação do crime, ou seja, onde a vítima experimento o efetivo prejuízo:

> "Algumas situações, ainda, merecem explicação. Em se tratando de estelionato, em sua figura fundamental, é competente o foro do lugar em que ocorreu o prejuízo e não o do lugar das manobras fraudulentas". (Manual de processo penal / Vicente Greco Filho. – 9. ed. rev. e atual. – São Paulo: Saraiva, 2012, página 163).

Já a regra específica, oriunda da recente inserção do §4º ao artigo 70 daquele mesmo Código, preceitua que a competência será do juízo do local da residência da vítima, nos seguintes termos:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (Incluído pela Lei nº 14.155, de 2021).

Portanto, o estelionato poderá ser ou não ser processado perante o juízo do local de residência da vítima a depender de ter sido ou não utilizado a rede bancária para a obtenção de vantagem indevida. Trata-se de norma processual penal podendo ser aplicada de imediato, inclusive, em inquéritos e processos já em cursos.

6.3 Pornografia infantil na internet

Com o precoce acesso infantil à internet e em redes sociais torna-se, consequentemente, mais fácil o contato entre crianças e pedófilos, que usam desse meio para aproveitar da fragilidade e inocência daquelas, ludibriando-as com métodos atrativos. Esses crimes são uma realidade no Brasil e no mundo, pois a rede facilita os mercados pornográficos nacionais e internacionais, possibilitando a realização de crimes virtuais.

O artigo 241, da Lei nº 8.069/90, pune qualquer ato com venda ou exposição de pornografia infantil. Esta pena, estabelecida no Estatuto da Criança e do Adolescente, pretende preservar a integridade moral, psíquica ou física das vítimas. Assim dispõe:

> "Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. 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".

Por sua vez, a proteção integral foi regulamentada pelo artigo 3º do mesmo diploma legal (Lei nº 8.069/90):

> "Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade. 38 Parágrafo único. Os direitos enunciados nesta Lei aplicam-se a todas as crianças e adolescentes, sem discriminação de nascimento, situação familiar, idade, sexo, raça, etnia ou cor, religião ou crença, deficiência, condição pessoal de desenvolvimento e aprendizagem, condição econômica, ambiente social, região e local de moradia ou outra condição que diferencie as pessoas, as famílias ou a comunidade em que vivem".

No ano de 2018, época em que já era perceptível o aumento da cibercriminalidade, um novo delito foi inserido no artigo 218 do Código Penal. Trata-se do artigo 218-C, que descreve:

> "Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou,

> sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave".

É inquestionável a prioridade da tutela da liberdade sexual e, consequente, dignidade sexual da criança e do adolescente no tocante ao cometimento de crimes de tais natureza.

Outrossim, é preciso um olhar mais clínico e rigoroso quando se trata de vítima mais vulnerável, seja pela menoridade, seja pelo ambiente em que está inserida.

Existe grande dificuldade para punições de crimes contra a liberdade/dignidade sexual, seja eles cometidos virtualmente ou não, pois, possuem peculiaridades no sistema processual penal.

Isso porque os meios de obtenção do corpo probatório, por vezes, chocam direitos fundamentais, principalmente: privacidade e intimidade.

6.3.1 Meios de produção probatória em crimes cibernéticos envolvendo a liberdade sexual

A utilização da internet e de dispositivos eletrônicos como meios para a prática de crimes de conteúdo sexual, se, por um lado, tem grande potencial lesivo em razão da grande velocidade e da larga abrangência em sua divulgação, por outro, deixa registros ou rastros digitais que, em determinadas situações, podem favorecer a apuração policial e a persecução penal.

A partir de tais registros ou rastros é possível, por exemplo, a identificação do IP utilizado pelo autor ou, eventualmente, a obtenção de dados de georreferenciamento que permitam, após a devida apuração de todos os demais elementos de prova, conduzir à identificação da autoria.

O simples armazenamento de imagens contendo pornografia infantil, por exemplo, já configura, por si só, crime autônomo, ainda que o detentor de tais imagens não tenha sido aquele que, em um primeiro momento, registrou-as.

Aliás, a conduta "armazenar" aponta para a prática de um crime de natureza permanente e, portanto, enquanto o autor mantiver consigo, armazenados em seu dispositivo eletrônico ou informático, arquivos contendo fotos ou cenas pornográficas de crianças ou adolescentes, poderá ser preso em flagrante delito.

Questão interessante diz respeito à contraposição entre o direito à privacidade e à intimidade do conteúdo de um aparelho eletrônico (ex. telefone celular) e à possibilidade de acesso a este mesmo conteúdo, independentemente de prévia autorização judicial.

Isso porque, tratando-se o aparelho de telefone celular (que armazena imagens de pornografia infantil) da própria materialidade de crime em flagrante, é imprescindível que o acesso a tal conteúdo seja, necessariamente, objeto de prévia autorização pelo Poder Judiciário?

O Superior Tribunal de Justiça, em caso paradigmático, já teve oportunidade de se debruçar sobre o tema e respondeu negativamente à referida pergunta. Ou seja, tratando-se o aparelho eletrônico do flagrante delito em si, o acesso ao seu conteúdo não dependente de autorização judicial para que a obtenção da respectiva prova seja lícita e legítima.

Neste sentido, transcreve-se a ementa do julgamento do STJ no AgRg no HC 656873/SC:

> AGRAVO REGIMENTAL NO HABEAS CORPUS. CRIME DE PRODUÇÃO DE PORNOGRAFIA INFANTIL. ART. 240, §2º, INCISO II DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE - ECA. NULIDADE. AUTORIZAÇÃO JUDICIAL PARA O ACESSO A DADOS. INEXISTÊNCIA. PRESCINDIBILIDADE NA HIPÓTESE. AGRAVO REGIMENTAL DESPROVIDO.
> 1. Os dados constantes em dispositivos eletrônicos particulares se submetem a proteção constitucional à intimidade, sendo que o acesso a seu conteúdo depende, em regra, de prévia e expressa autorização judicial.
> 2. No entanto, deve ser realizado um discrímen nos casos em que a materialidade delitiva está incorporada na própria coisa. É dizer, quando se tratar do próprio corpo de delito, ou seja, quando a própria materialidade do crime se encontrar plasmada em fotografias que são armazenadas naquele aparelho, como na espécie, a autorização judicial não será imprescindível. (RHC 108.262/MS, Rel. Ministro ANTONIO SALDANHA PALHEIRO, SEXTA TURMA, julgado em 5/9/2019, DJe 9/12/2019).
> 3. Agravo Regimental no habeas corpus desprovido. (AgRg no HC n. 656.873/SC, relator Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 23/11/2021, DJe de 26/11/2021).

Em sede de crimes cibernéticos, notadamente contra a liberdade sexual, portanto, as ferramentas digitais que facilitam a prática e a difusão dessas condutas ilícitas, podem, também, tornar mais eficiente a investigação e a persecução penais.

Dentre as medidas cautelares comuns, passíveis de aplicação em situações tais, podem ser citadas a busca e apreensão de dispositivos eletrônicos ou informáticos (computadores, HD´s, pen drives, celulares, tablets, smart watches, etc),

bem como o afastamento do sigilo de dados cadastrais, telefônicos e/ou telemáticos, com destaque, nesta última hipótese, da possibilidade de acesso, mediante autorização judicial, a serviços de armazenamento remotos, tais como o Google Drive e o *ICloud*, dentre outros.

Tais serviços de nuvem, inclusive, quando as imagens com conteúdo criminoso tiveram sido feitas pelo próprio dispositivo do autor, a cuja conta de usuário (ID) esteja àquele vinculado, poderão até mesmo fornecer, com detalhamento, a data, a hora e as coordenadas geográficas onde as cenas foram capturadas.

Atualmente, existem plataformas programáticas altamente avançadas que possibilitam o acesso ao conteúdo de aparelhos celulares ou de computadores, enfim, de qualquer dispositivo de armazenamento, mesmo que tais dispositivos eletrônicos e seus conteúdos estejam protegidos por qualquer espécie de barreira ou senha.

Dentre esses programas ou softwares, podemos citar o *Cellebrite*, que é uma plataforma de inteligência digital que fornece tecnologia e serviços de segurança pública, a fim de ajudar a proteger as vítimas, garantindo o acesso efetivo à justiça.

Através desse software, os órgãos de persecução penal podem quebrar o sigilo de dados telefônicos, mesmo sem que se tenha acesso à senha.

Segundo notícia veiculada no site TecMundo:

> "A ferramenta é voltada exclusivamente para o uso de autoridades policiais e tem capacidade de desbloquear celulares e acessar mensagens e outros dados apagados do dispositivo. O serviço, disponibilizado pela empresa especialista em dispositivos para extração de dados, Cellebrite, foi pensado para ajudar autoridades em investigações. Segundo a organização, o software consegue desbloquear celulares com Android e iOS, contando com um laboratório com "especialistas certificados em inteligência digital".
> O funcionamento do serviço é um segredo comercial. Sabe-se, no entanto, que a empresa utiliza uma combinação de softwares e hardwares para encontrar brechas de segurança e extrair dados do celular. Considerando que os investigadores que utilizam o programa devem preservar a validade jurídica da prova, a ferramenta evita qualquer manipulação ou alteração de dados do aparelho.
> Em relação à extração de dados que já foram apagados pelo usuário, especialistas afirmam que nenhuma informação é realmente excluída de um aparelho. Em vez disso, o sistema marca o espaço do arquivo como livre, mas guarda endereços da memória no dispositivo, tornando possível o "resgate" da informação".[22]

[22] BRASIL. Cellebrite: conheça o software usado na investigação do caso Henry. **TecMundo**. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em 02 nov.2022.

Portanto, além da elaboração de leis eficientes e atualizadas, de esclarecimento e de orientação da população, é crucial que as forças públicas envolvidas na persecução penal de crimes cibernéticos sejam constantemente treinadas, capacitadas e providas de ferramentas de alta tecnologia que permitam fazer frente aos desafios de se apurar, processar e punir tais crimes.

6.3.2 Operação DirtyNet

No final do ano de 2011 e no decorrer de 2012, a Polícia Federal protagonizou uma operação intitulada como “DirtyNet” (internet suja), em que um grupo de cibercriminosos compartilhava material de pornografia infantil na internet. Além da troca de arquivos, foram identificados, ainda, relatos de outros crimes praticados pelos envolvidos contra crianças, inclusive com menção a estupro cometido contra os próprios filhos, sequestros, assassinatos e atos de canibalismo.

A operação ocorreu em 11 estados e no Distrito Federal.

Os brasileiros, além de atuarem em solo brasileiro, também compartilhavam material de pornografia infantil com outros usuários da internet residentes em, aproximadamente, 34 (trinta e quatro) países.

Veiculada a matéria da operação pelo G1 do Rio Grande do Sul, um dos estados onde estavam os principais envolvidos, divulgaram-se detalhes:

> “Em apenas um dos mandados de busca cumpridos em Porto Alegre, foi apreendida uma coleção de cerca de 5,7 mil fotos de pornografia infantil, além de diversos vídeos. O material passará pela perícia para comprovar o indício de produção de imagens, ou seja, de abuso e estupro de vulnerável.
> De acordo com a delegada Diana Kalazans Mann, responsável pela operação no Rio Grande do Sul, os suspeitos trocavam milhares de arquivos contendo cenas degradantes de adolescentes, crianças e até bebês em contexto de abuso sexual.
> “São lesões corporais cometidas contra crianças no meio de fantasias sexuais macabras, inclusive com extração de pedaços, e relatos abomináveis. Do que já chegou para mim, é o que eu vi de pior”, declarou a delegada.
> A PF começou a monitorar o grupo há seis meses. A partir da investigação de uma pessoa descobriu-se uma rede de 160 usuários de conteúdos pornográficos envolvendo crianças e adolescentes: 63 no Brasil e 97 no Exterior. Trata-se de uma rede privada, criptografada, onde só é possível entrar com convite e aprovação dos outros membros, destacou a PF”.[23]

[23] BRASIL. Operação da PF contra pedofilia prende 32 pessoas em 9 estados. **G1.** Disponível em: http://g1.globo.com/rs/rio-grande-do-sul/noticia/2012/06/operacao-da-pf-contra-pedofilia-prende-32-pessoas-em-9-estados.html. Acesso em 13 ago. 2022.

O Tribunal Regional Federal da 4ª Região, no Rio Grande do Sul, proferiu o seguinte acórdão a respeito da operação DirtyNet, *in verbis*:

> **DIREITO PENAL E PROCESSUAL. ARTIGO 241-A DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. OPERAÇÃO DIRTYNET. COMPARTILHAMENTO DE FOTOS E VÍDEOS PORNOGRÁFICOS ENVOLVENDO CRIANÇAS E ADOLESCENTES PELO PROGRAMA GIGATRIBE. EMULE E ARES COM RESULTADO DENTRO E FORA DO TERRITÓRIO BRASILEIRO. TRANSNACIONALIDADE. COMPETÊNCIA DA JUSTIÇA FEDERAL NO CASO CONCRETO**. OITIVA JUDICIAL DE PERITO, FLAGRANTE PREPARADO E INDEFERIMENTO DE PEDIDO DE INSTAURAÇÃO DE INCIDENTE DE INSANIDADE MENTAL. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. TESES PRELIMINARES AFASTADAS. MÉRITO. MATERIALIDADE, AUTORIA E DOLO COMPROVADOS. CONDENAÇÃO ARMAZENAMENTO DOSIMETRIA. CIRCUNSTÂNCIAS JUDICIAIS. PENA-BASE READEQUAÇÃO. CONTINUIDADE DELITIVA. REDUÇÃO DO MONTANTE DE AUMENTO. MEDIDAS CAUTELARES. TRATAMENTO MÉDICO PSIQUIÁTRICO. VIOLAÇÃO AO ART. 319 DO CPP. NÃO OCORRÊNCIA. MEDIDA ADEQUADA E FAVORÁVEL AO RÉU. EXECUÇÃO PROVISÓRIA DA PENA. ESGOTAMENTO DA JURISDIÇÃO ORDINÁRIA DA CORTE DE APELAÇÃO. POSSIBILIDADE. PRECEDENTE STF COM REPERCUSSÃO GERAL. SÚMULA 122 TRF4. COMUNICAÇÃO AO JUÍZO DE ORIGEM.
> **1. Trata-se de crimes cuja previsão resulta das orientações traçadas em acordos e tratados internacionais - dos quais o Brasil é signatário - visando a combater a pedofilia via internet. A incorporação da Convenção da ONU sobre pornografia infantil no Direito Pátrio deu-se mediante o Decreto legislativo 28/90 com promulgação pelo Decreto Presidencial nº 99.710/90. 2. No caso, a ação penal que originou-se da operação policial em território pátrio que decorreu das investigações realizadas na chamada Operação DirtyNet, desenvolvida no final do ano de 2011 e no decorrer de 2012. Segundo apurado, as ações criminosas de compartilhamento entre usuários estrangeiros e brasileiros de material envolvendo cenas de pornografia infantil e de conteúdo pedófilo na rede mundial de computadores, por meio do software Gigatribe (programa fechado de rede social) Emule e Ares, cuja comunicação eletrônica é disponibilizada para qualquer indivíduo, dentro e fora do Brasil, restando, por conseguinte, evidenciada a prova da internacionalidade, a atrair a competência da Justiça Federal. 3. Tema pacificado pelo STF em Repercussão Geral. no RE 628.624/MG**.
> (...)
> Concluído o julgamento dos recursos pelo segundo grau de jurisdição, com manutenção das condenações impostas em sentença ou mesmo impondo-se condenação, é cabível a imediata execução da pena, independentemente da eventual interposição de recursos especial ou extraordinário ou mesmo da sua admissibilidade. Posição do STF em repercussão geral. ARE 964246/SP. 19. A 4ª Seção desta Corte editou a 'Súmula nº 122: Encerrada a jurisdição criminal de segundo grau, deve ter início a execução da pena imposta ao réu, independentemente da eventual interposição de recurso especial ou extraordinário'. 20. Conforme entendimento do STF e desta Corte, apesar de a pena restritiva de direitos não ter como pressuposto a segregação do condenado em estabelecimento prisional, é inquestionável a sua natureza de sanção penal, mormente se considerada a possibilidade de conversão em pena privativa de liberdade. Por esse motivo, não há razão para diferenciar as duas modalidades de sanção quanto à possibilidade de execução provisória da pena. 21. A execução provisória da pena será iniciada após o

> encaminhamento de comunicado ao juízo de origem, dando-lhe ciência do esgotamento da jurisdição ordinária desta Corte e do preenchimento das condições necessárias ao início da execução provisória, nos moldes dos embargos infringentes e de nulidade nº 5008572-31.2012.404.7002 (letras 'a' a 'c'). Improvimento dos embargos infringentes. (TRF 4, 7ª Turma, Classe: ACR – APELAÇÃO CRIMINAL. Relatora: SALISE MONTEIRO SANCHOTENE. Processo: 5005920-33.2015.4.04.7100. UF: RS. Data da Decisão: 20/02/2018). Grifou-se.

Conforme destacado acima, apesar de as condutas terem permeado o mundo todo, a ação penal se originou em território brasileiro, momento em que a competência foi atraída à Justiça Federal, sem prejuízo, claro, do auxílio da Interpol para a investigação.

Esse contato da Polícia Federal para com a polícia criminal internacional, como a Interpol, facilita o andamento das investigações, até porque crimes cibernéticos envolvendo a dignidade sexual, exige uma celeridade e eficiência muito maior, pois, uma vez lançado o conteúdo pornográfico dentro do ciberespaço, a propagação pode ser incontrolável e/ou irreparável.

7 CIBERTERRORISMO

7.1 Ligação entre terrorismo tradicional e o ciberterrorismo

Em nosso ordenamento jurídico, sobretudo, na Constituição Federal, é instituído o máximo repúdio ao terrorismo.

A Lei Federal nº 13.260/2016 regulamentou o artigo 5º, inciso XLIII da Constituição Federal, disciplinado o terrorismo e tratando de disposições investigatórias e processuais, bem como reformulando o conceito de organização terrorista.

> Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.
> § 1º São atos de terrorismo:
> I - usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa;
> II – (VETADO);
> III - (VETADO);
> IV - sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou **servindo-se de mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento;
> V - atentar contra a vida ou a integridade física de pessoa:
> Pena - reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.(grifou-se)

Não obstante toda a cautela legislativa para tentar prevenir ou erradicar o terrorismo, pouco se tem, em texto de lei, sobre o terrorismo cibernético, uma nova vertente do terrorismo que está se tornando mais frequente conforme a tecnologia avança e, em muitos casos, tem sido confundido com os crimes cibernéticos.

O termo “ciberterrorismo” foi empregado pela primeira vez no ano de 1980 em um artigo redigido por Barry Collin (ALCÂNTARA, 2015), significando a junção do ciberespaço e do terrorismo convencional, para ataques conduzidos à longa distância, tornando a população refém do medo e ameaçando um Estado Democrático de Direito.

Esse tipo de terror cibernético se opera em espaço virtual e, por consequência, a periculosidade desta prática tende a ser mais graduada em comparação ao terrorismo propagado em plano material.

Esse embate motivou a realização, no dia 16 de outubro de 2017, da audiência promovida pela Comissão de Relações Exteriores e Defesa Nacional (CRE) chamada de “Terrorismo e ameaças cibernéticas no século XXI: os inimigos sem rosto” e, com a análise da lei, foi possível determinar que o terrorismo não está previsto somente na Constituição Federal, mas também na Lei de Crimes Hediondos (Lei 8.072/90) e na própria Lei Antiterrorismo (Lei 13.260/2016), que estabelece o único conceito de terrorismo cibernético exposto de modo lacônico, atraindo crítica de alguns doutrinadores e especialistas do tema.

7.2 Ciberataques e a carência de segurança cibernética

Os ataques de ciberterroristas acontecem por várias maneiras, como, por exemplo: vírus, cavalo de troia, worms, spywares e SPAM. Essas formas são meios iniciais de ciberataque e são utilizadas porque possuem uma grande capacidade de difusão no campo virtual.

No ano de 2017, ciberataques ocorreram em larga escala, afetando, inclusive, o Brasil.

Conforme veiculado no site do G1:

> “Empresas de ao menos 74 países, incluindo o Brasil, foram alvos de um ciberataque em "larga escala" nesta sexta-feira (12). Os ataques atingiram hospitais públicos na Inglaterra, causaram a interrupção do atendimento do INSS e afetaram empresas e órgãos públicos de 14 estados brasileiros mais o Distrito Federal. A extensão do ataque leva especialistas em segurança a acreditar que se trate de uma ação coordenada, mas não se sabe ainda a autoria.
> Veja abaixo os principais pontos do caso e em seguida as informações completas:
> O ataque atingiu empresas ao redor do mundo na manhã desta sexta. Estimativa divulgada à tarde pelo grupo russo de segurança Kaspersky Lab fala em 74 países. A empresa Avast diz que foram 99 países atingidos.
> Representantes de hospitais afetados na Inglaterra relataram que cancelaram atendimentos e redirecionaram ambulâncias para outras unidades.
> No Brasil, ataques atingiram empresas e órgãos públicos. O atendimento do INSS está suspenso.
> Ataques usam vírus de resgate ("ransomware"), que inutilizam o sistema ou seus dados, até que seja paga uma quantia em dinheiro. Segundo a Kaspersky, o vírus se espalha por meio de uma brecha no Windows.

> “The New York Times" diz que ação pode ter usado ferramenta roubada da NSA, a agência de segurança nacional dos EUA.
> (...)
> No Brasil: TJ e outros
> O Judiciário estadual de SP admitiu que computadores da instituição foram infectados, o que motivou o desligamento de todas as máquinas do órgão em todo o estado. Os outros TJs estaduais citam "medidas de precaução", mas não dizem que foram atingidos diretamente pelo vírus.
> O juiz Alécio Martins Gonçalves, assessor da presidência do TJ-SP, disse que poucas máquinas foram infectadas. “Se não conseguirmos recuperar, serão dados que existem nessas máquinas, mas não houve infecção do datacenter, dos nossos servidores, então a população pode ficar tranquila."
> A Petrobras divulgou comunicado dizendo que, "ao tomar conhecimento de um vírus global, a empresa adotou medidas preventivas para garantir a integridade da rede e seus dados."
> Após ciberataque à Telefônica na Espanha, a Vivo no Brasil orientou funcionários a não acessarem a rede corporativa da empresa no Brasil - a medida foi direcionada para os escritórios da empresa, sem afetar os usuários dos serviços da Vivo.
> O Itamaraty disse que desligou suas máquinas preventivamente, mas disse que não foi alvo direto dos ataques. O site do Ministério das Relações Exteriores saiu do ar”.[24]

O ordenamento jurídico brasileiro precisa se renovar, uma vez que, com o avanço do mundo cibernético, os atos do terror cibernético se tornarão cada vez mais frequentes, intensos e serão mais dificilmente identificados e punidos, sendo que a desterritorialização ainda é um dos principais obstáculos para sua devida punição.

Conclui-se que, embora haja a tipificação do terrorismo no segundo parágrafo da Lei nº 13.260/2016, o conceito de terrorismo cibernético ainda é vago e é necessário implementar novas ferramentas que ajudem a aplicar, de forma mais eficaz, essa norma ao caso concreto.

Para isso surgiram o PL nº 272 de 2016 e o PL nº 2.418 de 2019, visando a auxiliar a aplicação da Lei Antiterrorismo e a incrementar o Marco Civil da Internet, para que haja, também neste, melhores respostas ao terrorismo cibernético.

A legislação, por si só não poderá lidar com esse problema e, por isso, as propostas para a melhor adequação são oferecer treinamento contínuo aos profissionais da área jurídica e militar, para que consigam buscar uma solução viável a cada caso concreto, sendo de muita importância o monitoramento mais atencioso das redes sociais, uma vez que, por meio delas, apoiadores ou novos membros conseguem contato com grupos terroristas.

---

[24] BRASIL. **Ciberataques em larga escala atingem empresas no mundo e afetam Brasil**. **G1.** Disponível em: https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml. Acesso em 14 out. 2022.

Os apoios ideológico ou monetário a práticas terroristas devem ser punidos de forma ainda mais gravosa, uma vez que, sem esse tipo de suporte, seria mais dificultosa a execução de crimes por terroristas. Enquanto não surgem as inovações, é preciso que a justiça brasileira utilize aquilo que a legislação oferece, a medida em que busca métodos evolutivos equivalentes ao avanço das práticas criminosas, visando ao controle e à punição eficazes.

8 DO DEEPFAKE

8.1 Conceito de inteligência artificial

Antes de se discorrer sobre deepfake, é importante tratar brevemente sobre a inteligência artificial.

O conceito surgiu na década de 1960. O cientista John McCarthy definiu, à época, inteligência artificial da seguinte maneira: “Inteligência artificial é a ciência de desenvolver máquinas inteligentes, especialmente softwares inteligentes”.

Desde então, o conceito foi se aprimorando e se tornando mais plural, de modo que não exista uma definição para inteligência artificial, mas sim muitas.

O consenso atual, no entanto, é que a inteligência artificial significa uma série de algoritmos matemáticos ou estatísticos que permitem que máquinas desenvolvam raciocínios aproximados ao raciocínio humano para determinadas atividades.

Além disso, há o desenvolvimento de processamento e de cognição semântica, que permite, por exemplo, que uma máquina consiga interpretar mensagens de um texto, reaja a imagens e até mesmo transforme textos e mensagens em imagens.

Logo, tornou-se viável a inserção dessa tecnologia nas ciências humanas, uma vez que é possível, por meio da inteligência artificial, que um programa compreenda o real sentido das palavras. Ou seja, com IA, as máquinas não são mais restritas a reagir a códigos numéricos, mas também a palavras.

Também existem algoritmos que permitem que os robôs aprendam com suas decisões anteriores, seja com a supervisão de humanos ou por análise estatística.

Não se pode olvidar que a inteligência artificial se tornou um tema muito significativo nos dias atuais, pois dela herdou-se uma verdadeira revolução constante tecnológica, rendendo amplos debates, questionamentos ou até mesmo insegurança social de que, em um futuro próximo, a sociedade civil poderá vir a ser dominada pela inteligência artificial.

8.2 Conceito de Deepfake

Deepfake é a junção das palavras deep *learning* e fake. Em tradução livre do inglês, tais termos significam, respectivamente, “aprendizagem profunda” e “falso”.

O termo deepfake foi utilizado pela primeira vez por um usuário do Reddit (plataforma de compartilhamento de informações e fonte “não profissional” de notícias na internet).

Na prática, é uma técnica que sintetiza imagens e sons reais para criar, com base em inteligência artificial (especificamente o *machine learning*, que usa algoritmos para coletar dados e aprender com eles), vídeos falsos com as personagens reais, mas com falas, gestos e ações que de fato, não existiram.

Os algoritmos são aplicados para fazer o reconhecimento da imagem que será copiada, levando em consideração a altura dos olhos, posicionamento do nariz e movimento da boca durante a fala, aprendendo a copiar as expressões e as características da pessoa que terá sua imagem utilizada no vídeo falso.

Daí o porquê do termo *deep learning*, pois a montagem se dá por meio do uso de redes neurais artificiais, ou seja, algoritmos programados para classificar imagens, reconhecer fala, detectar objetos e descrever conteúdo, com capacidade de continuamente melhorar e se adaptar a mudanças no padrão de informações recebidas, aprendendo o formato de um determinado rosto, como ele se mexe e reage a luz e sombras, criando, assim, uma série de imagens que parecem muito reais.

O uso de tecnologias deepfake para fins maliciosos está se expandindo rápido e, atualmente, está sendo explorado por cibercriminosos em escala global. Por exemplo, em 2019, cibercriminosos usaram um software de geração de voz de IA para se passar pela voz de um executivo-chefe de uma empresa de energia sediada no Reino Unido e conseguiram obter, ilicitamente, US$ 243.000 e distribuir as transferências dos fundos para contas bancárias localizadas no México e em outros países.[25]

[25] Wall Street Journal, **“Fraudsters Use AI to Mimic CEO's Voice in Unusual Cybercrime Case”, 30 de agosto de 2019.** Disponível em: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 .

8.3 Deepfake em período eleitoral e disseminação de “Fake News”

Em época de eleições, os cibercriminosos fomentam a disseminação da discórdia e das chamadas Fake News (notícias falsas), induzindo os eleitores leigos ao consumo e ao compartilhamento de conteúdos falsos.

O fato de a maioria das pessoas estar predisposta a acreditar em um vídeo ou em um áudio criado digitalmente, por não saberem que é possível fazer tal montagem, facilita o êxito de campanhas de desinformação ou de golpes *online* que utilizem tais técnicas.

Segundo a advogada Evelyn Melo Silva, especialista em Direito Digital e membro da Comissão de Direito Eleitoral e de Direito Constitucional da OAB/RJ, é necessário que Tribunal Superior Eleitoral discipline medidas preventivas e combativas no tocante ao deepfake e às fake news. Extrai-se um trecho de uma matéria do site CNN Brasil, em que a advogada participou:

> “Para manter o público e o eleitorado em alerta, Evelyn defende que o Tribunal Superior Eleitoral (TSE) retome a estratégia de educação digital usada durante as últimas eleições, de 2020, quando veiculou em TV aberta campanhas sobre deepfakes e fake news.
> “Partimos da premissa de que os celulares e os planos de dados são acessíveis [para fazer a checagem de informações], mas essa não é a realidade nacional”, alerta a advogada. Ela lembra que o recebimento de informações acontece de maneira gratuita em mensageiros instantâneos, mas a checagem ainda exige o consumo do plano de dados de boa parte dos brasileiros.
> “Não adianta falar em educação [midiática] sem conceder instrumentos de acesso à informação”, pontua.
> **Falta de regulamentação**
> Em termos legais, os deepfakes flutuam em uma zona cinzenta de falta de regulamentação. Segundo a interpretação de Evelyn Melo Silva, que atua em direito eleitoral, nem mesmo deepfakes criados com autorização dos candidatos — por exemplo, para agilizar a confecção de materiais de campanha — seriam considerados legais.
> Eles esbarraram no conceito de “trucagem” estabelecido na lei 9.504, que proíbe o uso de “montagens” em campanhas políticas, seja para ridicularizar ou beneficiar um candidato.
> “Considerando uma interpretação fria da lei, a legislação não permitiria. No entanto, essa tecnologia não existia na época em que essa definição foi feita, então não existia esse debate, e a interpretação da lei pode variar conforme o tempo, pondera a advogada”.[26]

Uma das formas para que as consequências da difusão de conteúdos inverídicos possam ser atenuadas é ensinar aos respectivos consumidores o exercício

[26] BRASIL. **Deepfake preocupa especialistas, que veem tecnologia incipiente no jogo eleitoral do Brasil. CNN Brasil.** Disponível em: https://www.cnnbrasil.com.br/tecnologia/deepfake-preocupa-especialistas-que-veem-tecnologia-incipiente-no-jogo-eleitoral-do-brasil/. Acesso em 09 set. 2022.

da plena cautela, ou seja, ensinar a desenvolverem o hábito de procurarem outras fontes e de analisarem minuciosamente o material veiculado, confrontando-o com outros vídeos que saibam ser reais.

8.3.1 Caso emblemático de Donald Trump vs. Barack Obama

Em 2018, durante as eleições americanas, um vídeo com aparência realista fora circulado em todas as mídias sociais e telejornais.

O material consistia, basicamente, em xingamentos proferidos pelo Barack Obama direcionado ao candidato à época que ganhou a eleição, Donald Trump.

Mais ou menos na metade do vídeo, originalmente publicado pelo BuzzFeed, é revelado que Obama na verdade não havia pronunciado essas palavras e que elas foram ditas pelo diretor e escritor de "Corra!", Jordan Peele, cuja voz e boca foram inseridas digitalmente em um texto original.

Nos próximos anos, a presença de deepfakes também foi significativa durante as eleições dos EUA em 2020, quando o País votou para Presidente e elegeu Joe Biden. O panorama daquele momento levou a Microsoft, gigante de tecnologia, a criar um software especializado na identificação de deepfakes.

É nítido o desastre que esse mecanismo artificial pode causar.

8.3.2 Primeiro caso de deepfake no Brasil durante a campanha eleitoral de 2022

Na época das eleições do ano de 2022, nas redes sociais, circulou um vídeo em que continha deepfake, maculando a campanha eleitoral.

O primeiro caso de deepfake do período oficial de campanha eleitoral de 2022 já foi identificado, explana colunista Cristina Tardáguila, do Portal UOL[27].

Trata-se de um vídeo falso, veiculado no mês de agosto do ano de 2022 e que circulou nas redes sociais com imagens do Jornal Nacional, mostrando o Presidente Jair Bolsonaro (PL) à frente do ex-presidente Lula (PT) nas intenções de voto para a eleição presidencial da pesquisa Ipec divulgada em 15 de agosto de 2022.

---

[27] TARDÁGUILA, C. **Eleições: 1ª deepfake mostra pesquisa falsa na voz de Renata Vasconcelos**. **UOL.** Disponível em: https://noticias.uol.com.br/colunas/cristina-tardaguila/2022/08/18/eleicoes-1-deep-fake-mostra-pesquisa-falsa-na-voz-de-renata-vasconcellos.htm. Acesso em: 10 de set. 2022.

Conforme a colunista supra, o vídeo usa um áudio manipulado da apresentadora Renata Vasconcellos, na bancada do Jornal Nacional.

Os dados realmente apresentados pelo Jornal Nacional, mostram que Lula liderava a disputa com 44% das intenções de voto, seguido pelo presidente Jair Bolsonaro, com 32%.

A TV Globo se pronunciou afirmando que o vídeo circulado era falso e que o Ipec está "denunciando a peça de desinformação no Sistema de Alerta de Desinformação Contra as Eleições do Tribunal Superior Eleitoral (TSE) e no Ministério Público Eleitoral (MPE) para que adotem as medidas cabíveis".

8.4 Vídeos falsos de pornografia envolvendo famosos

O uso da inteligência artificial parece não ter limites. Não obstante todas as consequências devastadoras quando se trata de política, disseminação de fake news e, consequente, ódio à oposição, a cultura criminosa dos deepfakes também é encontrada em materiais de cunho pornográficos.

Enquanto a ciência tem dedicado esforços a buscar formas de combater a propagação das chamadas fake news, a indústria do sexo passou a se direcionar a combater um problema semelhante, mas talvez ainda mais grave.

Artistas musicais e cinematográficos estão sendo alvos de deepfakes envolvendo pornografia. Tal técnica é utilizada para colocar a imagem de celebridades praticando todos os tipos de atrocidades sexuais possíveis, o que satisfaz os desejos de fãs que costumam consumir esse material.

De acordo com o noticiado, conteúdos pornográficos respondem por 96% de todos os vídeos com deepfake que circulam na Internet. Essa é uma das descobertas feitas pelo estudo The State of Deepfakes, desenvolvido pela firma de segurança Deep Trace, especializada em rastrear materiais do tipo criados com inteligência artificial para proteger a reputação das vítimas.

Extrai-se a conclusão de uma matéria publicada, ano de 2019, do site especialista em assuntos de tecnologia, TechTudo, por Paulo Alves:

> Segundo o levantamento publicado na última semana, há atualmente 14.678 vídeos que falsificam a identidade dos personagens de alguma maneira, número que quase dobrou em menos de um ano. A técnica já foi usada para vídeos em que o ex-presidente dos Estados Unidos, Barack Obama, aparece

> xingando o atual Donald Trump, além de montagens pornográficas com as atrizes Gal Gadot e Emma Watson, por exemplo.[28]

Outrossim, percebe-se que, os dados acima revelados são anteriores à Covid-19, período este que alavancou e aperfeiçoou as técnicas de uso do deep fake.

8.4.1 Caso da atriz americana Scarlett Johansson

Uma das maiores atrizes da atualidade, Scarlett Johansson, famosa por interpretar a viúva negra, heroína da Marvel, com participações na franquia “Os Vingadores”, processou, em 2011, um hacker que vazou fotos íntimas e as inseriu em um falso vídeo pornográfico.

Tal caso tornou-a o símbolo de uma nova era chocante de violações de privacidade. O hacker foi posteriormente condenado a 10 anos de prisão.

Esses tipos de conteúdo afetam mais ainda celebridades pela facilidade de encontrar material multimídia sobre elas na rede.

Extrai-se de uma matéria do site americano “The Washington Post” um trecho da entrevista em que a atriz alertou sobre o futuro da deepfake se nada for feito para conter o fenômeno:

> “Claramente, isso não me afeta tanto porque as pessoas assumem que não sou realmente eu em um pornô, por mais humilhante que seja. Eu acho que é uma busca inútil, legalmente, principalmente porque a internet é um vasto buraco de minhoca de escuridão que se devora. Há coisas muito mais perturbadoras na dark web do que isso, infelizmente. Acho que cabe a um indivíduo lutar pelo seu próprio direito à sua imagem, reivindicar danos, etc. [...] Além disso, cada país tem seu próprio “juridiquês” em relação ao direito à sua própria imagem, portanto, embora você possa derrubar sites nos EUA que estão usando seu rosto, as mesmas regras podem não se aplicar na Alemanha. Mesmo que você tenha direitos autorais de fotos com sua imagem que pertencem a você, as mesmas leis de direitos autorais não se aplicam no exterior. Infelizmente, já passei por esse caminho muitas e muitas vezes. O fato é que tentar se proteger da internet e sua depravação é basicamente uma causa perdida, na maior parte. Pessoas vulneráveis como mulheres, crianças e idosos devem tomar cuidado extra para proteger suas identidades e conteúdo pessoal. Isso nunca será alterado, não importa o quanto o Google faça suas políticas. Eu acho que é uma busca inútil, legalmente, principalmente porque a internet é um vasto buraco de escuridão que se consome. Há muito mais coisas perturbadoras na teia escura do que isso, infelizmente [...]. Nada pode impedir alguém de cortar e colar minha imagem ou de qualquer outra pessoa em um corpo diferente e fazê-la parecer tão sinistramente realista quanto desejado. Basicamente, não há regras na

[28] ALVES, P. 96% dos vídeos deepfake têm conteúdo pornográfico; veja sete fatos. **TechTudo**. Disponível em: https://www.techtudo.com.br/listas/2019/10/96percent-dos-videos-de-deepfake-tem-conteudo-pornografico-veja-sete-fatos.ghtml. Acesso em: 10 de set. de 2022.

> internet, porque é um abismo que permanece praticamente sem lei, suportando as políticas dos EUA que, novamente, só se aplicam aqui". (Tradução nossa). [29]

De acordo com The Washington Post, um dos vídeos falsos produzidos com a imagem da atriz foi visualizado mais de 1.000.000 (um milhão) de vezes. Conforme acima alertado por Johansson, é questão de tempo até que outro alvo seja escolhido para conteúdo deste tipo. Para as vítimas desta ação criminosa, a sensação é de que a internet é um abismo sem lei.

O jornal ainda trouxe o caso de uma mulher de 40 anos, que descobriu um vídeo adulto deepfake com o rosto dela circulando pela web logicamente sem seu consentimento. A pessoa que produziu o vídeo utilizou mais de 400 fotos do rosto dela, sendo que boa parte das imagens foi obtida por meio do Facebook.

[29] HARWELL, DREW. "Scarlett Johansson on fake AI-generated sex videos: 'Nothing can stop someone from cutting and pasting my image". December 31, 2018 (31 de dezembro de 2018). Disponível em: https://www.washingtonpost.com/technology/2018/12/31/scarlett-johansson-fake-ai-generated-sex-videos-nothing-can-stop-someone-cutting-pasting-my-image/. Acesso em: 16 out. 2022.

9 POSSIBILIDADE DE SE CARACTERIZAR O CRIME DE FRAUDE PROCESSUAL POR MEIO DE DEEP FAKE

A tecnologia deepfake é uma espécie de inteligência artificial que visa a transformar, a mascarar, a modificar, a criar ou a introduzir falas e vídeos falsos dentro de um contexto autêntico e aparentemente real. O que mais preocupa é que tais inteligências artificiais, como os deepfakes, vêm sendo aperfeiçoadas cada dia mais, consequentemente, torna-se mais difícil a correspondente detecção de conteúdos inverídicos ou, até mesmo, de comprovar a disparidade entre o conteúdo real e o falso.

Portanto, o grande cerne deste problema é: verossimilhança fática criada pela tecnologia deepfake, é dizer, a probabilidade de consumir uma mídia totalmente maculada por cibercriminosos, sem o mínimo espaço para a percepção de que o conteúdo não é verdadeiro, mas sim criado.

Dentro da referida perspectiva, analisaremos o possível cometimento de fraude processual no âmbito penal por emprego de deepfake.

A fraude processual é um dos crimes contra a administração da justiça e está tipificado no artigo 347 do Código Penal, que assim dispõe:

> **Fraude processual**
>
> Art. 347 - Inovar artificiosamente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito:
> Pena - detenção, de três meses a dois anos, e multa.
> Parágrafo único - Se a inovação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro.

O presente dispositivo visa a coibir o artifício malicioso destinado a ludibriar o magistrado e a obter injusto proveito. Em outras palavras, consiste em inovar artificiosamente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito.

Trata-se de crime comum, podendo ser praticado por qualquer pessoa (vítima, acusado ou mesmo advogado), tendo ou não interesse no processo. A pena prevista é de detenção, de três meses a dois anos, e multa. Se a inovação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro.

A partir das noções jurídicas acima, podemos aventar a seguinte hipótese de deepfake para fins de fraude processual.

O sujeito A é vizinho do sujeito B, que é profissional em tecnologias e em computação. Ambos se conhecem e frequentam a casa um do outro. Certo dia, o sujeito B nota que um objeto de alto valor sumiu de sua casa, na mesma ocasião em que A o visitara. O furto é noticiado à Polícia e é instaurado um Inquérito Policial para a apuração da autoria. Como o sujeito B não tinha como provar a autoria do crime, mas por acreditar em seu íntimo que o sujeito A seria o responsável, decide modificar/inovar artificiosamente (deepfake) um vídeo aleatório que possuía de A, de forma a aparentar a confissão do crime e um pedido desculpas por seu colega vizinho. Para tornar a montagem o mais verossímil possível, o sujeito B edita o vídeo colocando sua casa como ambiente de fundo, local do furto. Posteriormente, o sujeito B vai à Delegacia de polícia com o intuito de inserir a mídia contendo a confissão falsa no inquérito policial. Diante disso, pergunta-se: qual crime o sujeito B cometeu?

O caso hipotético descrito acima, em tese, enquadra-se no que dispõe o art. 347, crime de fraude processual.

O legislador taxou os objetos materiais que levam o sujeito ativo a inovar artificiosamente o processo penal, mesmo que não iniciado, são eles: estado de lugar, de coisa ou de pessoa.

Há de se observar que o exemplo supracitado não constitui crime de falso testemunho, pois as condutas deste crime consistem no ato de mentir ou deixar de falar a verdade quando as referidas pessoas estiverem em juízo, processo administrativo, inquérito policial ou em juízo arbitral.

Frisa-se também que o sujeito B não cometeu crime de denunciação caluniosa (art. 339 do Código Penal), os motivos são claros:

a) B não deu causa à instauração de inquérito policial especificamente contra o sujeito A;

b) O crime em questão demanda que o autor, imbuído de má-fé, atribua a alguém fato criminoso sabendo ser inocente. O que não aconteceu. O inquérito policial já havia sido iniciado e, posteriormente, o sujeito B, com plena convicção de que A era o autor do furto, ausente prova robusta que comprovasse a autoria, forja uma “prova” contra aquele e a faz introduzir em inquérito policial já em andamento.

Sendo assim, o ato de transformar ou de alterar vídeos “pessoais” do sujeito A introduzindo falas e gesticulações que remetem à confissão do crime

supratranscrito, para forjar prova de autoria por meio do emprego de deepfake, teoricamente configura o crime de fraude processual.

Outro questionamento pertinente é: como proceder juridicamente diante de um caso como esse?

Há quem possa defender que tal crime não é possível ser cometido mediante meio eletrônico (inteligência artificial), reforçando a ideia de que o caput é taxativo, sem abertura para que meios eletrônicos sejam *modus operandi* deste crime.

Ou seja, o agente, mediante fraude, modifica ou altera somente por força de uma ação natural própria do homem, aspecto físico, exemplo: retirar manchas de sangue impregnadas na roupa da vítima (alteração de coisa), mudar o aspecto físico exterior mediante cirurgia estética (alteração de pessoa).

Mas e sobre o vocábulo “coisa” existente no caput? É mais abrangente, até porque não existe um significado específico para esta palavra. Muito menos existe um sinônimo. Digamos que é uma palavra aberta e paradoxalmente vaga. Dessarte, ironicamente, qualquer “coisa” pode, em tese, se encaixar nesse contexto. Inclusive o uso de deepfake.

Extrai-se a palavra “coisa” do tipo legal do crime de fraude processual para ser, aqui, analisada.

Qual significado o legislador da época de 1940 quis atribuir ao sentido da palavra “coisa”? E mais, será que há um vernáculo existente na face da Terra que defina o que é “coisa”?

Talvez seja tal vocábulo um “curinga” para ser utilizado quando alguém não lembra a definição de algo ou quer atribuir um sentido figurado a qualquer “coisa”.

Segundo o Dicionário Michaelis, a palavra “coisa” pode assumir inúmeros significados, são eles:

> “1 Tudo o que existe ou pode existir: “[…] a quitandeira, quando precisava de dinheiro para qualquer coisa, dava um pulo até à venda”.
> 2 Um objeto inanimado em oposição a um ser vivo.
> 3 Aquilo em que se pensa: Coisas vagas lhe ocupavam a mente.
> 4 Algo ao qual nos referimos; acontecimento, caso, circunstância: Aquilo foi uma coisa difícil de suportar.
> 5 Aquilo que tem existência concreta; fato, realidade: Tais coisas se impõem mais que brilhantes discursos.
> 6 O conjunto do que existe: As coisas humanas são transitórias.
> 7 Assunto, matéria ou objeto de que se trata.
> 8 Essência ou substância, em oposição à forma e à aparência.
> 9 Aquilo que liga, une; relação, vínculo: Não tenho coisa alguma com ele.
> 10 Transação na qual a pessoa está envolvida; negócio: A coisa não lhe correu bem e acabou indo à falência.

> 11 Razão para realizar algo; causa, motivo: Por coisa alguma, farei isso.
> 12 Aquilo que é realizado; ato, feito: O prefeito orgulha-se muito de suas coisas.
> 13 Aquilo de que não se tem conhecimento; mistério, segredo: Aqui tem coisa!
> 14 Mal-estar súbito, inexplicável: De repente, senti uma coisa que me apertava o peito e caí em prantos.
> 15 VULG Órgão sexual feminino ou masculino.
> 16 JUR Tudo aquilo que, com existência corpórea ou concebível pela inteligência, pode ser utilizado pelo homem e constituir objeto de direito."[30]

A reflexão que ainda perpetua é: como interpretar a descrição legal do artigo 347 com a palavra que absorve diversos sentidos literários ali inserida?

Até porque, exige-se como elemento do crime a tipicidade, que é a consunção da conduta à descrição legal. Mas o que viria a ser considerado crime de fraude processual quando uma pessoa inovar artificiosamente um estado de "coisa", cuja palavra comporta infinitas interpretações? Estaria o próprio legislador penal descrevendo um crime cuja tipicidade formal e material caberá à interpretação em um caso concreto?

Portanto, entende-se que, cibercriminosos, através do deepfake, poderiam cometer crime de fraude processual, de acordo com o exemplo descrito no começo deste tópico, vez que estariam inovando artificiosamente, ao menos, um estado de "coisa".

Noutra perspectiva, o caput traz: com o intuito de induzir a erro o juiz ou perito.

Muito é discutido sobre a possibilidade de no futuro a inteligência artificial substituir a qualidade do juiz, isto é, robôs julgando lides.

Essa projeção utópica pode refletir no crime ora em estudo, pois, se a finalidade do crime de fraude processual é impedir que o juiz caia em manobras processuais, como que um robô com inteligência artificial não identificará eventuais fraudes cibernéticas?

De fato o vácuo legal cria uma sensação de impunidade. Vale lembrar que o direito penal brasileiro não recepciona analogia *in malam partem* e nem cria delitos por meio de decreto. Isto faz com que o processo se torne muito mais complicado, pois torna a vacância legal de crimes próprios infinitamente mais perigosa que a de crimes impróprios. Pois, nesses, por mais que o Código Penal seja de 1940,

---

[30] BRASIL. **Dicionário Michaelis online.** Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/coisa. Acesso em 09 set. 2022.

crimes como fraude, roubo, furto, estelionato, falsificação, falsa identidade dentre outros estão previstos em lei. Já nos crimes próprios a conduta praticada não pode ser objeto de uma ação penal quando não há previsão legal em legislação esparsa alguma.

Acontece que, o exemplo concreto hipotético trazido aqui à tona, não fora tratado por nenhuma doutrina moderna, atual, tampouco há na jurisprudência pátria precedente ou sentença monocrática tratando acerca deste caso imaginário, mesmo que análogo.

Outrossim, não se pode olvidar que, atualmente, o Direito Penal está imerso em uma realidade extremamente diversa e tecnológica quando comparada àquela em que, outrora, foram redigidos os tipos penais em vigor, tal como é o caso do crime de fraude processual.

É papel que cabe aos doutrinadores da área, aos estudiosos do tema e aos operadores do Direito refletir e questionar sobre a constante evolução da sociedade, dos programas e das máquinas, de modo a equalizar e a estimular a aplicação da lei material ou processual sempre compatível com a visão atual e até mesmo de um futuro “projetado”, que hoje ainda pode ser taxado de utópico.

9.1 Direito Penal Cibernético e norma penal em branco

Determinados crimes praticados por meio na internet, já tipificados, quando identificado os infratores, possibilitam a aplicação da sanção penal.

Pode-se ter a falsa impressão de que a ausência, dentre as elementares dos tipos, da palavra “internet” possibilitaria a impunidade das condutas praticadas pela rede mundial de computadores. Tal situação, contudo, não impede a punição naqueles casos em que a internet é meio para a prática de crimes (*modus operandi*).

Pessoas têm medo de ser punidas, mesmo assim muitas apostam na inoperância dos aparelhos de controle do Estado e, diante desta crença, pode-se inferir que, quanto maior a sensação de impunidade, maior será o índice de criminalidade, pois “*nada torna mais frágil o instrumento das leis que a esperança de impunidade*” (FOUCAULT, 2013, p. 92).

Mesmo que o Código Penal não tenha sido criado com o objetivo de punir crimes cibernéticos, ainda assim acaba sendo utilizado para o enquadramento de determinadas condutas executadas por intermédio da rede mundial de

computadores, o que, na visão de alguns, trata-se da aplicação indevida do princípio da analogia, na medida em que o judiciário estaria se utilizando desse princípio “In malam partem”, para punir os crimes cibernéticos nos termos do Código Penal e não de uma lei específica sobre o tema.

Damásio de Jesus e José Antônio Milagre, a respeito das leis específicas que versam sobre o tema de crimes virtuais, são bem diretos em seus entendimentos, pois na visão deles:

> “[...] o Brasil está bem atrasado em termos de legislação penal informática. De fato, não pairam dúvidas de que a revolução tecnológica trouxe grandes desafios ao Direito Penal, com a ocorrência de inúmeras situações em que forçosa era a subsunção dos casos trazidos à lei”. (JESUS, MILAGRE, p70, 2016).

É necessário termos em mente que a estrutura penal evolui dia após dia, é um fenômeno essencialmente mutável. O Direito, como uma percepção científica, é assim, sofre modulações e metamorfoses. Não existe, definitivamente, uma ramificação do Direito que traz características de uma matéria invariável.

Pode-se afirmar que o Direito é incompatível com o fenômeno da estabilização. E, assim, funciona o metaverso/ciberespaço e a tecnologia, estes dois mundos, automaticamente, seguem o caminho da evolução. Talvez com maior rapidez na constante.

Logo, a sociedade está, querendo ou não, sob a mercê do que a tecnologia cria, modifica ou transforma. Houve uma aceitação tácita pela sociedade civil de que o metaverso criou a chamada inteligência artificial, que faz, na maioria das vezes, o mesmo papel de um humano.

Nessa perspectiva de rápida evolução, no âmbito do Direito Penal, a classificação doutrinária dada à norma penal em branco se faz interessante.

Segundo o doutrinador Renato Brasileiro de Lima, Promotor da Justiça Militar da União, as normas penais em branco são aquelas:

> (...) cuja compreensão do preceito primário demanda complementação. Em outras palavras, por mais que exista a descrição de uma conduta proibida, esta descrição demanda um complemento extraído de um outro diploma, como, por exemplo, leis, decretos, regulamentos, etc., para que se possa

> compreender os limites da proibição feita pela lei penal (LIMA, 2016, p. 693, grifo do autor)[31].

Por ora, a criação de um conjunto de normas-regra ou principiológicas penais em branco, ao nosso ver, é uma medida racional e guarda compatibilidade com a rápida evolução da tecnologia.

E, com isso, conforme a tecnologia vai sofrendo modificações, poderá vir o legislador penal a editar normais penais em branco, cujos regulamentos possam ser, mais pronta e facilmente, alterados, sem os entraves procedimentais e temporais de um processo de edição de leis ordinárias ou complementares.

Quem garante que os “dispositivos, aparelhos eletrônicos e/ou informáticos” serão os mesmos daqui a vinte, trinta ou quarenta anos? Às vezes, aquilo que hoje se entende por celular, poderá, num futuro incerto, adotar diversa nomenclatura ou forma.

Todo esse raciocínio é útil para que o jurista ou estudioso jamais enxergue o Direito (engloba-se todo o conjunto normativo, sem exceções) com os mesmos olhos do passado.

A filosofia de Foucault, construída e interpretada ao longo dos tempos, voltada à impunidade e ao remodelamento Estatal para atuar como instrumento de repressão criminal e controle social, serve de guia histórico para a chegada da nova era cibernética, que antes era considerada “utópica”.

[31] LIMA, Renato Brasileiro de. Legislação Especial Criminal Comentada. 5. ed. Salvador: Juspodivm, 2016.

10 CONCLUSÃO

Ao analisarmos historicamente a metamorfose legislativa, houve grande quantidade de normas que foram editadas, criadas ou revogadas em face do exponente crescimento virtual, gerando uma sociedade civil totalmente conectada.

No entanto, o Brasil está muito longe de ser um país de referência em assuntos cibernéticos.

Primeiro porque, não temos suporte especializado próprio ou convencionado para detectar no “ninho” ataques de cibercriminosos, ressalvada a Convenção de Budapeste, que instiga apenas a cooperação internacional no que tange a persecução penal, jurisdição e competência.

Segundo porque não há, no plano legislativo, medidas repressivas ou até mesmo intervenção qualificada do Poder Judiciário para pacificar entendimento sobre as manobras criminosos desenfreadas do uso de “deepfakes”, consubstanciando-se, em muitos casos, nas consequentes ondas de fakes news.

Uma ferramenta não tão aplicada ao combate de ataques cibernéticos, a chamada “engenharia social”, pode ser utilizada no âmbito da investigação criminal, que é uma técnica por meio da qual uma pessoa procura persuadir a outra a executar determinadas ações. Um exemplo emblemático se dá em situações em que um policial se infiltra em uma organização criminosa para coletar indícios sobre a prática de crimes. Nesses casos, são utilizadas técnicas de engenharia social para que seja coletado o maior número de informações. É engenharia social contra o crime.

O uso de sistemas de inteligência artificial em diferentes setores é uma tendência contínua e isso inclui autoridades do sistema de justiça criminal que perceberam os benefícios e vantagens do uso dessa tecnologia.

As autoridades nacionais responsáveis pela aplicação da lei penal, envolvidas na investigação de crimes cibernéticos, ainda não estão totalmente preparadas para lidar com as dimensões técnicas e legais da IA quando usada para fins disruptivos ou maliciosos.

Além disso, ainda não há evidências suficientes para justificar se as autoridades policiais em todo o mundo estão bem equipadas e treinadas para coletar evidências transfronteiriças, para conduzirem investigações nacionais onde um sistema de IA esteve envolvido na perpetração de uma conduta ilícita.

A coordenação e cooperação com provedores de serviços e empresas que gerenciam e operam sistemas e serviços do mundo cibernético são cruciais para ajudar a determinar o uso abusivo ou criminoso por parte dos perpetradores.

No entanto, essas tarefas trazem uma série de desafios técnicos e legais, já que a maioria dos sistemas de IA depende de uma conexão com a Internet para funcionar, sede em que, muitas vezes, são necessários dados de assinantes e tráfego para realizar uma investigação.

Portanto, os provedores de serviços globais também terão um papel importante a desempenhar na possível identificação e localização de criminosos cibernéticos, uma situação que requer esforços, medidas e respostas bem coordenadas com base em tratados internacionais e leis nacionais entre autoridades policiais e entidades do setor privado. A necessidade de mais parcerias estratégicas para combater o cibercrime é mais atual e importante do que nunca.

O trabalho futuro entre Estados Federados, como se deu na Convenção de Budapeste, será muito relevante para os formuladores de políticas e as autoridades policiais, orientando a implementação de futuras políticas nacionais de IA.

Outrossim, uma das maiores “doenças cibernéticas” que permeiam o mundo, com certeza, é a pornografia infantil e, concomitantemente, a divulgação de materiais pornográficos por meio da internet. Por isso tem-se a urgente necessidade de aperfeiçoar o sistema legislativo, sobretudo, enrijecendo laços internacionais para o combate de tais crimes gravíssimos e, claro, preparar tecnicamente os órgãos de persecução criminal.

Normas penais em branco, com regulamentos passíveis de evolução mais rápida e flexível, compõem o conjunto de instrumentos voltados ao combate eficaz e eficiente de cibercrimes.

A criação de forças-tarefa nacionais sobre crimes cibernéticos (compostas por autoridades policiais, representantes do judiciário, desenvolvedores de tecnologia e provedores de serviços globais) pode servir como um veículo relevante para coordenar e combater condutas ilícitas relacionadas ao uso indevido do ciberespaço e da inteligência artificial. Tais forças-tarefa podem ser articuladas no contexto das estratégias nacionais de IA e devem estar vinculadas às tarefas das autoridades de justiça criminal para combater o cibercrime.

“A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original”.

(Albert Einstein)

“Acredito que o desenvolvimento pleno da inteligência artificial poderia significar o fim da raça humana”.

(Stephen Hawking)

REFERÊNCIAS

ALCÂNTARA, Bruna Toso de. Brasil e Ciberterrorismo: desafios para o Rio 2016. Ninth International Conference on Forensic Computer Science 89, 2015. Disponível em: http://icofcs.org/2015/papers ago. 2019.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Editora Malheiros, 2008.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal. Introdução à sociologia do direito penal**. 3. ed. Rio de Janeiro: Revan, 2002.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. Revista Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/.

BRASIL. **Brasil foi o 5º país com mais ataques cibernéticos em 2021. Security Report, 2022**. Disponível em: https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/#.YvhTG3bMK70. Acesso em: 13 ago. 2022.

BRASIL. Ministério Público Federal. **Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime**. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em 14 mar. 2022.

BRASIL. Portal Unificado da Justiça Federal da 4ª região. Disponível em: https://www.trf4.jus.br. Acesso em: 22 de out. de 2022.

CABETTE, Eduardo Luiz Santos. **Invasão de dispositivo informático, furto eletrônico, estelionato eletrônico e competência – Lei 14.155/21**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 26, n. 6613, 9 ago. 2021

CAVALLO, Vincenzo. La Sentenza Penale. Imprenta: Napoli, E. Jovene, 1936.

CUNHA, Rogério Sanches. **Manual de Direito Penal: parte especial (arts. 121 ao 361)**. 13.ed. rev., atual e ampl. – Salvador: Juspodivm, 2021.

DIAS, Jorge de Figueiredo. Questões fundamentais do direito penal revisitadas. São Paulo: Editora Revista dos Tribunais, 1999.

ERDELYI, Maria Fernanda. **Itamaraty ainda estua adesão à Convenção de Budapeste**. Disponível em: https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste. Acesso em: 08 abr. 2022.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 2013.

FONSECA FILHO, Cléuzio. História da computação: teoria da computação: teoria e tecnologia. São Paulo: LTr, 1999.

JESUS, Damásio de; MILAGRES, José Antônio. **Manual de Crimes Informáticos**. 1ª Edição. ed. São Paulo: Saraiva, 2016. 231 p. ISBN 978850262724-6. Disponível em> https://docero.com.br/doc/ecv5ns. Acesso em: 08 abr. 2022.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2002.

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

PRADO, Luiz Regis. **Bem Jurídico-Penal e Constituição**. 5 ed. São Paulo: Revista dos Tribunais, 2011.

MPMG, Ministério Público do Estado de Minas Gerais. Combate aos Crimes Cibernéticos. Disponível em: https://www.mpmg.mp.br/areas-de-atuacao/atuacao-criminal/crimes-ciberneticos/ . Acesso em: 14 mar. 2022.

MEDEIROS, A. **Hackers: entre a ética e a criminalização**. Florianópolis: Visual Books, 2002.

LIMA, Renato Brasileiro de. **Legislação Especial Criminal Comentada**. 5. ed. Salvador: Juspodivm, 2016.

RIBEIRO, Eliete da Silva. **Crime de Estelionato – Uma análise da evolução sob a égide da impunidade na cidade de Manaus**. 2019. Disponível em: https://semanaacademica.org.br/system/files/artigos/crime_de_estelionato_-_uma_analise_da_evolucao_sob_a_egide_da_impunidade_na_cidade_de_manaus_eliete_ da_silva_ribeiro_0.pdf>. Acesso em: 17 abr. 2022.

VIANNA, Tulio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013.

GRECO FILHO, Vicente. **Manual de processo penal**. 9. ed. rev. e atual. – São Paulo: Saraiva, 2012.

WILLIAM SCHENDES. Olhar Digital, 2022. Ataques cibernéticos no brasil cresceram 46% no segundo trimestre. Disponível em: https://olhardigital.com.br/2022/08/09/seguranca/ataques-ciberneticos-brasil-cresce-46/. Acesso em: 13 ago. 2022.

Wall Street Journal, “Fraudsters Use AI to Mimic CEO's Voice in Unusual Cybercrime Case”, 30 de ago. de 2019”. Disponível em: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos- voice-in-unusual-cybercrime-case-11567157402. Acesso em 3 de set. 2022.