DESAFIOS DO DIREITO PENAL NA REPRESSÃO DA ENGENHARIA SOCIAL EM AMBIENTES VIRTUAIS NO BRASIL

CHALLENGES OF PENAL LAW IN REPRESSING SOCIAL ENGINEERING IN VIRTUAL ENVIRONMENTS IN BRAZIL

DOI: 10.19135/revista.consinter.00019.18
Recebido/Received 29/06/2023 – Aprovado/Approved 17/01/2024

Matheus de Quadros[1] – *https://orcid.org/0000-0001-7971-3799*
Fabrício Bittencourt da Cruz[2] – *https://orcid.org/0000-0003-0538-9193*

Resumo

Este artigo objetiva, através do método hipotético-dedutivo, analisar a eficácia do Direito Penal na prevenção às práticas de engenharia social em ambientes virtuais no Brasil. Foi conduzida uma pesquisa qualitativa e exploratória, utilizando-se de recursos documentais e bibliográficos. O artigo também explora estudos e experiências internacionais para identificar potenciais abordagens complementares ao combate da engenharia social online. A conclusão aponta que, apesar dos esforços legislativos em fazer com que o Direito Penal abranja as práticas de engenharia social em ambientes virtuais, obstáculos estruturais dificultam a efetividade dessa abordagem. Ademais, o artigo destaca a necessidade de uma estratégia preventiva por parte do Estado, a ser implementada por meio de políticas públicas complementares.

Palavras-chave: Engenharia Social; Prevenção; Direito Penal.

Abstract

This article aims, through the hypothetical-deductive method, to analyze the effectiveness of Criminal Law in preventing social engineering practices in virtual environments in Brazil. A qualitative and exploratory research was conducted, using documentary and bibliographic resources. The article also explores international studies and experiences to identify potential complementary approaches to combating online social engineering. The conclusion points out that, despite legislative efforts to make Criminal Law encompass social engineering practices in virtual environments, structural obstacles hinder the effectiveness of this approach. Furthermore, the article highlights the need for a preventive strategy by the State, to be implemented through complementary public policies.

Keywords: Social engineering; Prevention; criminal law.

[1] Mestrando em Ciências Sociais Aplicadas pela UEPG, pós-graduado em Direito Processual Penal e Prática Forense Penal pela UEPG e em Direito Constitucional pelo Instituto Damásio de Direito. Professor do Curso de Direito do Centro Universitário de Telêmaco Borba. Universidade Estadual de Ponta Grossa: CEP: 84010-330. Ponta Grossa, Paraná, Brasil, *E-mail*: mdqmatheus@gmail.com. https://orcid.org/0000-0001-7971-3799

[2] Doutor em Direito pela Faculdade de Direito da USP. Professor Adjunto na UEPG (Graduação, Mestrado e Doutorado). Líder do Projeto MindTheGap: inovação em Direito (https://mdgap.org). Juiz Federal. Universidade Estadual de Ponta Grossa: CEP: 84010-330. Ponta Grossa, Paraná, Brasil, *E-mail*: fabriciobittcruz@gmail.com. https://orcid.org/0000-0003-0538-9193

Além do Direito Penal: o Direito Administrativo Sancionador como forma complementar de combate às práticas de engenharia social; 5. Considerações finais; 6. Referências.

1 INTRODUÇÃO

Apesar de desafios sociais, a popularização da internet no Brasil tem ocorrido a passos largos. Segundo dados do Instituto Brasileiro de Geografia e Estatística, 90% dos lares brasileiros já tinham acesso à internet em 2021[3]. Esse amplo acesso tem alcançado níveis de democratização muito mais rápidos e abrangentes do que muitos outros direitos fundamentais, como o saneamento básico, ainda inacessível para quase metade da população brasileira[4].

O mundo virtual impôs uma nova realidade, modificando profundamente a dinâmica da sociedade. Como observa Ulrich Beck, a modernidade promoveu uma globalização dos riscos que ultrapassa as barreiras de classe e fronteiras nacionais[5]. Além disso, com a ampla democratização da internet, novos bens jurídicos surgiram e outros foram atualizados para enfrentar as novas situações[6].

Bens jurídicos tradicionalmente protegidos pelo Direito Penal, como a honra e a propriedade, são afetados pelos novos riscos trazidos pela internet. Há também um intenso debate sobre a necessidade de proteger novos bens jurídicos, como a integridade e a confidencialidade dos dados pessoais digitais[7].

Com a expansão da internet surgem novas situações prejudiciais, em relação às quais o sistema legal e a estrutura estatal brasileiros podem não estar preparados para atuar, dada a escala e a rapidez com que essas mudanças estruturais ocorrem. Segundo levantamento realizado pela empresa *Kapersky*, a população brasileira foi o maior alvo de ataques de *phishing* no aplicativo *WhatsApp* no mundo[8], evidenciando a especial vulnerabilidade dos brasileiros neste cenário.

Esta situação está relacionada a um conceito mais amplo de práticas de manipulação, persuasão e influência sobre o comportamento humano para obtenção de informações sigilosas e/ou de grande valor, denominadas engenharia social, o principal foco deste estudo.

A engenharia social é um conceito anterior à popularização da internet, tendo atingido outro patamar de danos com a expansão das interações online, devido à facilidade em obter informações e enganar vítimas. Em resposta a esse problema,

---

3 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, *Internet já é acessível em 90,0% dos domicílios do país em 2021*, disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021, acesso em: 28 abr. 2023.

4 RODRIGUES, Alex, *Quase 50% dos brasileiros não têm acesso a redes de esgoto, diz MDR*, disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-12/quase-50-dos-brasileiros-nao-tem-acesso-redes-de-esgoto-diz-mdr, acesso em: 28 abr. 2023.

5 BECK, Ulrich, *Sociedade de risco: rumo a uma outra modernidade*, 2. ed., São Paulo, Editora 34, 2011, Tradução de Sebastião Nascimento, p. 43.

6 *Ibid.*, p. 43.

7 FULLER, Greice Patricia, TATEOKI, Victor Augusto, "Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação", *Revista em Tempo*, vol. 22, n°. 1, fev. 2023, pp. 110-124.

8 KULIKOVA, Tatyana *et al*, *El spam y el phishing en 2022*, disponível em: <https://securelist.lat/spam-phishing-scam-report-2022/97582/>, acesso em: 28 abr. 2023.

legisladores e a população geral usualmente recorrem ao Direito Penal, buscando prevenir e responsabilizar os autores dessas práticas.

Mas o Direito Penal é adequado para lidar com golpes virtuais que utilizam a engenharia social?

Em busca de resposta, analisamos a problemática do ponto de vista formal, para verificar se o Direito Penal abrange tipos que se enquadram nas situações de engenharia social. Em seguida, avaliamos a questão na perspectiva prática/material, com o objetivo de observar se as estruturas policial e judiciária brasileiras têm sido eficazes no combate às situações de engenharia social por meio do Direito Penal.

Finalmente, exploramos se outros ramos do Direito poderiam ser mais adequados para lidar com o combate à engenharia social no *ciberespaço*. Neste caso, sugerimos o uso do Direito Administrativo Sancionador como uma alternativa mais eficaz.

Esta pesquisa é classificada, de acordo com Gil, como qualitativa e exploratória[9], visando a obter uma perspectiva mais ampla sobre a resposta do Direito Penal brasileiro aos golpes relacionados à engenharia social na internet. Utilizamos a abordagem hipotética-dedutiva para aferir a hipótese, formulada a partir de observações empíricas em situações cotidianas, de o Direito Penal ser insuficiente para prevenir de maneira adequada as práticas criminosas relacionadas à engenharia social em ambiente virtual no Brasil.

Para a construção do referencial teórico, utilizamos técnicas de pesquisa bibliográfica e documental, seguindo as orientações de Marconi e Lakatos[10]. No âmbito da pesquisa bibliográfica, consultamos livros especializados em temas relacionados ao objeto de pesquisa, além de artigos, com ênfase nas consultas às bases de dados: Scientific Eletronic Library Online (SciELO) Brasil, Google Acadêmico e Portal de Periódicos da CAPES, selecionando os artigos devido à sua relevância para o objeto de pesquisa.

A revisão da literatura foi realizada nas bases de pesquisa mencionadas, buscando os termos: "regulação", "engenharia social", "phishing", "prevenção", "Direito Penal", "crimes virtuais", "políticas públicas" em várias combinações em português, espanhol e inglês.

Apesar da existência de diversos estudos sobre crimes informáticos, há poucos trabalhos sobre a efetividade do Direito Penal para lidar com algumas das novas situações trazidas pela popularização da internet. Além disso, devido à rápida evolução do mundo digital e às recentes inovações legislativas, a exemplo da Lei Geral de Proteção de Dados de 2018, nem todos os materiais disponíveis estão atualizados.

A pesquisa documental foi realizada principalmente a partir da análise da legislação pertinente e de estudos realizados por agências de pesquisa sobre a prática da engenharia social no Brasil e suas consequências.

---

9 GIL, Antonio Carlos, *Como elaborar projetos de pesquisa*, 4. ed., São Paulo, Atlas, 2017, pp. 41-42.

10 MARCONI, Marina de Andrade, LAKATOS, Eva Maria, *Fundamentos de metodologia científica*, 5. ed., São Paulo, Atlas, 2003.

2 TIPICIDADE PENAL DAS TÉCNICAS DE ENGENHARIA SOCIAL

A engenharia social envolve um vasto conjunto de práticas que empregam a manipulação, a persuasão e a influência sobre as vítimas como estratégias para capturar informações. Joseph M. Hatfield, ao analisar 134 definições do termo em estudos acadêmicos escritos entre 1990 e 2017, concluiu que o termo engenharia social fundamenta-se em três pilares: assimetria epistemológica, dominância tecnocrática e substituição teleológica[11].

Segundo o autor, a prática de engenharia social ocorre quando uma pessoa (ou um grupo de pessoas) tem certa vantagem em conhecimentos técnicos sobre outra, utilizando essa vantagem para modificar o comportamento da vítima e conduzindo-a a realizar alguma atitude desejada por essa pessoa ou grupo de pessoas[12].

Considerando as formas de engenharia social que se valem da internet, destacam-se algumas técnicas frequentemente utilizadas nesse contexto: *Phishing*, *Sextortion/catphishing*, *Smishing*, *Vishing* e *Watering holes*[13].

A técnica de *Phishing* envolve se passar por uma entidade ou pessoa que tenha a confiança da vítima, com o objetivo de obter dados pessoais. Geralmente o engenheiro social encaminha por *e-mail* ou mensagem via redes sociais um *website* que transmita sensação de confiança e/ou familiaridade à vítima, induzindo-a a revelar dados sensíveis ou instalar *softwares* mal-intencionados[14/15].

Com a técnica *Sextortion/catphishing*, o engenheiro social consegue obter imagens íntimas da vítima e as usa para constrangê-la, coagindo a pessoa a ceder valores, informações ou a realizar uma ação específica, sob ameaça de divulgar o conteúdo[16].

Smishing é uma variação da técnica de *phishing* que usa mensagens de texto (SMS), objetivando induzir a vítima a clicar em um *link* suspeito enviado pelo remetente na mensagem. Através desse *link*, o engenheiro social buscará obter dados sensíveis da vítima por meio de formulários ou da instalação de *softwares* mal-intencionados[17/18].

---

11 HATFIELD, Joseph M., "*Social engineering in cybersecurity: The evolution of a concept", Computers & Security*, vol. 73, mar. 2018, pp. 1-28.

12 HATFIELD, Joseph M., "*Social engineering in cybersecurity: The evolution of a concept", Computers & Security*, v. 73, mar. 2018, pp. 1-28.

13 Além das técnicas descritas neste trabalho, há também diversas outras que são comumente citadas, como *dumpster diving*, *baiting* e *shoulder surfing*. Contudo, devido ao modo de execução dessas formas de engenharia social, elas fogem ao escopo deste estudo.

14 PINTO, Luiz Tiago Souza, BERENGUEL, Orlando Leonardo, "Engenharia social: a porta de entrada para informações confidenciais", *Revista Científica E-Locução*, vol. 1, n°. 17, out. – dez. 2020, p. 489.

15 SILVA, Francisco José Albino Faria Castro e, *Classificação taxonómica dos ataques de Engenharia Social: caracterização da problemática da segurança de informação em Portugal relativamente à Engenharia Social*, 131 p., Dissertação (Mestrado em Segurança dos Sistemas de Informação), Faculdade Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, disponível em: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, acesso em: 28 abr. 2023, p. 27.

16 PETHERS, Brent, BELLO, Abubakar, "*Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks*", *Future Internet*, vol. 15, n°. 1, jan. 2023, pp. 1-5.

17 PINTO, BERENGUEL, *op. cit.*, p. 491.

18 SILVA, *op. cit.*, p. 28.

Vishing também é semelhante à técnica de *phishing*. Consiste em ludibriar a vítima com táticas que a fazem crer estar falando com alguma instituição de sua confiança, como seu banco pessoal. O engenheiro social, já em posse de alguns dados da vítima que serão usados para ganhar sua confiança, telefona para ela, passando-se por alguma instituição que precisa da "confirmação" dos dados sensíveis da pessoa[19/20].

Através da técnica de *Watering holes*, o engenheiro social infecta *websites* mirando um usuário ou um grupo específico de usuários. O objetivo é que esse(s) usuário(s) não desconfie(m) do meio utilizado e confie(m) no website infectado para fornecer informações sensíveis ou fazer download de softwares mal-intencionados[21].

Muitas das práticas mencionadas se enquadram em tipos penais já previstos. *Phishing*, *smishing*, *vishing* e *watering holes* encaixam-se no art. 171 do Código Penal, segundo o qual constitui crime de estelionato "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".

A reforçar esta afirmação, a Lei 14.155/2021 ampliou o tipo penal de estelionato ao adicionar a chamada fraude eletrônica, prevista nos artigos 171, §2°-A, e 171, §2°-B, do Código Penal.

Com a inovação legislativa, a pena para o crime de estelionato foi aumentada se a fraude for cometida utilizando-se de informações fornecidas por meio de redes sociais, e-mails (*phishing*), chamadas telefônicas (*vishing*) ou qualquer outro meio fraudulento semelhante.

O legislador, consciente das tendências prejudiciais da globalização, estipulou que, se o crime de estelionato por meio de fraude eletrônica for cometido utilizando um servidor mantido fora do território brasileiro, a pena prevista no art. 171, §2°-A, do Código Penal será aumentada de um a dois terços.

Vale ressaltar que, dependendo do caso concreto, podem ser caracterizados os crimes de furto (art. 155 do Código Penal), dano (art. 163 do Código Penal) e falsa identidade (art. 307 do Código Penal). Além disso, quando as práticas envolvem o acesso não autorizado do engenheiro social a um dispositivo informático da vítima, seja para obtenção de dados ou instalação de softwares mal-intencionados, poderá haver a caracterização do crime de invasão de dispositivo informático (art. 154-A do Código Penal).

Em relação à prática de *sextortion*, existe uma variedade de tipos penais possíveis, dependendo da maneira como o conteúdo íntimo foi obtido e da finalidade de sua utilização. A *sextortion*, por vezes traduzida para o português como sextorsão,

---

19 PINTO, Luiz Tiago Souza, BERENGUEL, Orlando Leonardo, "Engenharia social: a porta de entrada para informações confidenciais", *Revista Científica E-Locução*, vol. 1, n°. 17, out. – dez. 2020, p. 490.

20 SILVA, Francisco José Albino Faria Castro e, *Classificação taxonómica dos ataques de Engenharia Social: caracterização da problemática da segurança de informação em Portugal relativamente à Engenharia Social*, 131 p., Dissertação (Mestrado em Segurança dos Sistemas de Informação), Faculdade Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, disponível em: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, acesso em: 28 abr. 2023, p. 28.

21 PINTO, BERENGUEL, *loc. cit.*

envolve a obtenção de conteúdo íntimo da vítima como parte da prática de engenharia social.

O primeiro ato dessa técnica pode constituir os delitos de violação de dispositivo informático (art. 154-A do Código Penal) ou de violação sexual mediante fraude (art. 215 do Código Penal).

Com relação ao segundo ato, em que o conteúdo íntimo é utilizado para a obtenção de vantagens, é possível um desdobramento em condutas típicas.

Na perspectiva de Rogério Sanches Cunha, caso o agente constranja a não fazer o que a lei permite, ou a fazer o que ela não manda, ocorrerá crime de constrangimento ilegal (art. 146 do Código Penal). Se o constrangimento da vítima for realizado com o intuito de obter indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa, entende o autor pela configuração do crime de extorsão (art. 158 do Código Penal). Por outro lado, se a vítima constrangida à prática de atividade sexual, há o crime de estupro (art. 213, do Código Penal)[22].

Dessa forma, observa-se que as práticas de engenharia social podem se adequar a diversos tipos penais existentes[23].

Embora existam situações específicas que podem não se enquadrar nos tipos penais atualmente existentes, é plausível afirmar que, ao menos no aspecto formal, o Direito Penal está preparado para combater a cibercriminalidade proveniente de práticas de engenharia social.

No entanto, uma pergunta se impõe: o atual panorama legislativo penal tem se mostrado eficaz no combate à engenharia social?

3 DESAFIOS DO DIREITO PENAL NA REPRESSÃO DA ENGENHARIA SOCIAL EM AMBIENTES VIRTUAIS

Relatórios divulgados por empresas de segurança e por instituições públicas mostram que os crimes de engenharia social realizados no ambiente virtual têm alcançado proporções antes inimagináveis, dificultando a reação estatal.

Segundo o levantamento realizado pelo laboratório de segurança digital *dfndr lab*, mais de cinco milhões de pessoas foram vítimas de clonagem do aplicativo *Whatsapp* em 2020[24], conduta compatível com a técnica de *phishing*.

Em sentido semelhante, o Anuário Brasileiro de Segurança Pública de 2022, produzido pelo Fórum Brasileiro de Segurança Pública, aponta um aumento de 179,9% nas taxas de estelionato no país entre 2018 e 2021, impulsionado pelos crimes de estelionato cometidos no ambiente digital[25/26.]

---

22 CUNHA, Rogério Sanches, *Manual de Direito Penal: parte especial (arts. 121 ao 361)*, 11. ed., Salvador, Editora Juspodivm, 2019, pp. 208-209.

23 JESUS, Damásio de, MILAGRE, José Antônio, *Manual de crimes informáticos*, São Paulo, Editora Saraiva, 2016, *e-book*, p. 21.

24 BIANCAMANO, Paula, *Mais de 5 milhões de brasileiros foram vítimas do golpe de Clonagem de WhatsApp em 2020*, disponível em: <https://www.psafe.com/blog/mais-de-5-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-clonagem-de-whatsapp-em-2020/>, acesso em: 28 abr. 2023.

25 Ainda, aponta o Anuário Brasileiro de Segurança Pública de 2022 que esse número foi confeccionado sem os dados de nove estados da federação brasileira, o que torna o número de crimes cometidos por engenharia social no meio eletrônico ainda mais relevante no cenário atual, pois o número real, considerando todos os estados da Federação, provavelmente é muito maior.

Adicionalmente, de acordo com os dados do mesmo Fórum de Segurança Pública, em 2021 foram registrados pelo menos 60.590 casos de estelionato através de fraude eletrônica[27].

É evidente, portanto, que grande parte dos crimes atuais no Brasil ocorre no ambiente virtual. Essa nova forma de criminalidade acrescenta uma variável ao aumento geral do número de crimes. Além de fatores comuns, como o aumento da população e a desigualdade social, o Poder Público agora precisa se ajustar ao aumento da criminalidade resultante dos novos cenários da contemporaneidade.

Isso nos leva à questão da escassez de recursos. Há um limite orçamentário para lidar com um número crescente de delitos.

Como poderá a Autoridade Policial lidar com a mesma eficiência em suas investigações, por exemplo, diante de um aumento alarmante de crimes realizados no ambiente digital? Haverá disposição orçamentária condizente com o aumento de recursos para a Segurança Pública na mesma proporção que aumentam os números referentes aos crimes cometidos em ambiente virtual? Essas perguntas parecem ter respostas negativas.

Como registrado no relatório final da Comissão Parlamentar de Inquérito (CPI) dos Crimes Cibernéticos em 2016, um dos principais problemas verificados no combate aos crimes cibernéticos no Brasil é a escassez de efetivo na Polícia Federal face ao aumento da demanda de casos e às estruturas deficitárias da Polícia Civil e da Polícia Federal[28].

Ademais, a forma de investigação passou por uma transformação significativa. A natureza das evidências em crimes cometidos no mundo analógico é muito diferente daquelas em crimes digitais. Para os crimes chamados de crimes de rua, a autoria e a materialidade dos delitos são geralmente aferidas a partir de prova testemunhal, buscas e apreensões, imagens de câmeras de segurança, entre outros meios obtidos em diligências predominantemente físicas. Por outro lado, em crimes digitais, a evidência é principalmente pericial, o que dificulta e encarece as investigações.

Segundo Emerson Wendt e Higor Vinicius Nogueiro Jorge, os desafios na investigação dos crimes cibernéticos no Brasil incluem a falta de capacitação adequada dos policiais e outros atores da persecução penal, e a falta de órgãos especializados para lidar com crimes cibernéticos[29].

A globalização e a popularização da internet eliminaram as distâncias físicas entre o local do crime e o autor dos fatos, muitas vezes inviabilizando a atividade

---

[26] FORUM BRASILEIRO DE SEGURANÇA PÚBLICA, *Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas*, Anuário Brasileiro de Segurança Pública 2022, disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf>, acesso em: 28 abr. 2023, p. 8.

[27] *Ibid., p. 8.*

[28] BRASIL, Câmara dos Deputados. *Relatório Final da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país*, Brasília, 2016, disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%253D%253E+RCP+10/2015>, acesso em 28 abr. 2023, pp. 85-87.

[29] WENDT, Emerson, JORGE, Higor Vinicius Nogueira, *Crimes cibernéticos: ameaças e procedimentos de investigação*, 3. ed., Rio de Janeiro, Brasport, 2021, *e-book*, pp. 304-306.

investigativa. O criminoso não mora necessariamente na mesma cidade, estado ou região da consumação do crime, pois o engenheiro social pode estar sediado no outro lado do Brasil ou mesmo em outro país. Essa característica faz que seja necessário expedir cartas precatórias ou rogatórias visando ouvir um possível investigado ou testemunhas, demandando muito tempo e recursos.

Além disso, os engenheiros sociais costumam usar protocolos ou sistemas que dificultam a coleta de indícios de autoria. Alesandro Gonçalves Barreto e Beatriz Silveira Brasil apontam que os primeiros nomes que surgem como autores em investigações de crimes de engenharia social são falsos ou "laranjas"[30]. Redes como o TOR (*The Onion Router*) dificultam ainda mais a tarefa dos investigadores, ao mascarar o IP (*Internet Protocol*) e a localização originais do engenheiro social por meio de várias camadas de outros computadores conectados ao sistema[31].

Somada a isso, a corrida contra o tempo, pois os tipos penais relatados neste estudo não têm prazos prescricionais particularmente longos, segundo o art. 109 do Código Penal. Assim, os problemas ora mencionados podem levar à extinção da punibilidade antes de uma efetiva responsabilização dos agentes.

Em síntese, existem vários obstáculos a impedir que os tipos penais inerentes à engenharia social *online* sejam efetivamente aplicados contra essa prática no Brasil, evidenciando a insuficiência do Direito Penal.

4 ALÉM DO DIREITO PENAL: O DIREITO ADMINISTRATIVO SANCIONADOR COMO FORMA COMPLEMENTAR DE COMBATE ÀS PRÁTICAS DE ENGENHARIA SOCIAL

O cenário é propício para o emprego de outras técnicas de combate a práticas de engenharia social no ambiente virtual brasileiro, em conjunto com as estratégias de Direito Penal.

Adotamos a perspectiva de Jennifer Lynch, onde as estratégias para combater os delitos de engenharia social são divididas em três níveis: autoajuda (estratégias de nível primário), arquitetura e controle por entidades privadas (estratégias de nível secundário), e aplicação da lei (estratégias de nível terciário)[32].

De acordo com Lynch, seria necessário adotar outras estratégias antes do envolvimento legal, principalmente devido à dificuldade e ao custo das investigações[33]. Nessa linha, o estudo se volta para a análise de outras maneiras pelas quais o Estado pode colaborar na luta contra as atividades relacionadas à engenharia social no ambiente virtual.

Nessa linha argumentativa, sugerimos que a solução pode residir em alterar o foco da ação estatal, transitando de uma abordagem primariamente repressiva para uma abordagem preventiva.

---

30 BARRETO, Alessandro Gonçalves, BRASIL, Beatriz Silveira, *Manual de investigação cibernética à luz do Marco Civil da Internet*, Rio de Janeiro, Brasport, 2016, *e-book*, p. 226.

31 ARAUJO, Fábio Lucena de, "Aspectos jurídicos no combate e prevenção ao *ransomware*" *in* BRASIL, Ministério Público Federal, 2ª Câmara de Coordenação e Revisão, org., *Crimes Cibernéticos: coletânea de artigos*, vol. 3, Brasília, MPF, 2018, p. 101.

32 LYNCH, Jennifer "*Identity theft in cryberspace: crime control methods and their effectiveness in combating phishing attacks*", *Berkeley Techonology Law Journal*, vol. 20, 2005, pp. 274-299.

33 *Ibid*., p. 292.

Como mencionado anteriormente, o principal obstáculo à eficácia do Direito Penal reside na produção de provas de materialidade e indícios de autoria, dadas as limitações materiais encontradas pelo Estado. Além disso, o Direito Penal envolve pretensa responsabilização após o dano já ter sido concretizado, muitas vezes sem a possibilidade de uma reparação efetiva.

Portanto, uma solução possível poderia estar não na punição dos engenheiros sociais após os fatos, mas sim na criação de uma regulamentação preventiva capaz de dificultar a prática da engenharia social online.

Um ponto primordial na perspectiva preventiva é a educação dos usuários. É essencial, por exemplo, o usuário entender que, ao estar *online*, deve tomar precauções extras, dada a dificuldade de verificar a legitimidade das pessoas em ambientes virtuais.

A conscientização sobre os riscos inerentes ao ambiente virtual está amparada no Marco Civil da Internet (Lei 12.965/2014), ao dispor que um dos objetivos do uso da internet no Brasil é promover o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos (art. 4°, inciso II).

Além disso, como destacam Mateus de Oliveira Fornasier, Norberto Milton Paiva Knebel e Fernanda Viero da Silva, a educação está diretamente ligada ao conceito de cidadania digital, que pressupõe o empoderamento técnico dos usuários diante das assimetrias tecnológicas da estrutura social[34].

Estudo conduzido por Adam Kavon Ghazi-Tehrani e Henry N. Pontell sugere que os principais pilares em campanhas de conscientização devem se concentrar no entendimento de como funcionam os golpes de engenharia social (conscientização) e em como reconhecer uma tentativa de golpe (prevenção)[35/36].

Como exemplos de políticas públicas para conscientização sobre os riscos dos crimes cibernéticos, é relevante mencionar duas iniciativas adotadas pelo Reino Unido: "*10 Steps to Cyber Security*" e "*Cyber Essentials*". Ambas as políticas concentram-se em educar empresas, indo além da mera conscientização, para persuadir as companhias a tomar ações proativas para mitigar os riscos no ambiente virtual[37].

Em outra vertente, o combate preventivo às *botnets*[38], que são frequentemente usadas em ataques de *phishing*, representa uma estratégia efetiva de larga escala contra as práticas de engenharia social.

Experiências internacionais, como as observadas na Austrália, Coréia do Sul, Japão, Alemanha e Holanda demonstram a eficácia de uma regulamentação multilateral, realizada em conjunto com provedores de internet e empresas de antivírus[39].

---

34 FORNASIER, Mateus de Oliveira, KNEBEL, Norberto Milton Paiva, SILVA, Fernanda Viero da, "*Phishing* e engenharia social: entre a criminalização e a utilização de meios sociais de proteção", *Meritum*, vol. 15, n°. 1, jan.-abr. 2020, p. 123.

35 GHAZI-TEHRANI, Adam Kavon, PONTELL, Henry N., "*Phishing evolves: analyzing the enduring cybercrime*", *Victims & Offenders*, vol. 16, n°. 3, 2021, pp. 333-334.

36 No caso, o estudo produzido pelos autores foca na técnica de *phishing*. Contudo suas conclusões servem a todos os tipos de técnica de engenharia social produzida no ambiente virtual.

37 REINO UNIDO, *National cyber security strategy 2016-2021*, disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf >, acesso em: 30 abr. 2023.

38 O termo *botnet* se refere a uma rede de grande número de computadores infectados por *trojan horses* com o intuito de serem gerenciadas remotamente para campanhas de *spam* ou ataques *DDoS*.

39 DUPONT, Benoit, "*Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime*", *Crime Law Soc Change*, vol. 67, 2017, pp. 107-111.

Isso possibilita uma ação preventiva, bloqueando o efeito dos *botnets* identificados antes que eles sejam usados para enviar *spams* ou outros conteúdos nocivos.

Outras formas de prevenção incluem: a adoção de selos de verificação em redes sociais, a utilização de *blacklists* para *websites* suspeitos e de *whitelists* para *websites* oficiais, a criação de um período de espera para a oposição de registros de domínios com nomes enganosos, a adoção de autenticação em múltiplos fatores e o aprimoramento de filtros de *spam*[40/41].

Políticas públicas em colaboração com o setor privado podem constituir maneiras eficazes de abordar os desafios apresentados pela engenharia social online e crimes cibernéticos em geral.

Este tipo de abordagem reconhece a necessidade de uma cooperação robusta entre o governo e o setor privado para lidar com questões de segurança cibernética. Visando à efetiva adoção dessas técnicas, sugere-se sua incorporação legislativa.

A regulamentação brasileira em relação ao espaço digital anda a passos largos. Leis como o Marco Civil da Internet e a Lei Geral de Proteção de Dados representam avanços significativos na criação de um ambiente *online* mais seguro. No entanto, ainda há espaço para avançar nesta direção e explorar a possibilidade de legislações mais eficazes para prevenir práticas de engenharia social.

Este estudo aponta para criação de leis de boas práticas contra a engenharia social, visando a adotar procedimentos como os acima referidos, em cumulação a estrutura legal e administrativa já existente no Brasil. Uma abordagem híbrida que combine a ação preventiva do Direito Administrativo Sancionador com a resposta repressiva do Direito Penal parece consistir em uma estratégia promissora.

A partir da estrutura já criada com a Lei Geral de Proteção de Dados, podem ser incorporadas novas missões à estrutura da Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 55-J da Lei Geral de Proteção de Dados e recentemente instituída pela Lei 13.853/2019.

No que diz respeito à Autoridade Nacional de Proteção de Dados (ANPD), sua recente elevação ao *status* de autarquia e a expansão de suas responsabilidades poderiam desempenhar um papel crucial na proteção dos dados dos cidadãos e na prevenção da engenharia social. A ANPD já tem como missão garantir a proteção dos dados pessoais e pode servir como uma entidade importante para coordenar esforços no combate à engenharia social na perspectiva do Direito Administrativo Sancionador.

Isto porque, nos termos da Lei Geral de Proteção de Dados, cabe à ANPD dispor sobre padrões e técnicas utilizados em processos de anonimização de dados e realizar verificações sobre sua segurança, estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais e sugerir a

---

40 SUMAN, Shreya, SRIVASTAVA, Neha, PANDIT, Renu, "*Cyber crimes and phishing attacks*", *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, n°. 2, fev. 2014, p. 326.

41 VILELA, Erica, UEDA, Eduardo Takeo, GAVA, Vagner Luiz, "Phishing e engenharia social: conceitos, modalidades, técnicas de detecção e prevenção de fraudes. Uma revisão sistemática da literatura" *in* 19th CONTECSI – International Conferece on Information Systems and Technology Management, São Paulo, *Anais Eletrônicos* [...], São Paulo 2022, disponível em: <https://www.tecsi.org/contecsi/index.php/contecsi/19CONTECSI/paper/view/7138>, acesso em 29 abr. 2023, pp. 9-11.

adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Também estão entre as atribuições da ANPD: dispor sobre padrões técnicos mínimos sobre medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; e estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

A ANPD dispõe de poder para criar medidas de proteção de dados, o que implica em medidas de prevenção às práticas de engenharia social que visem obter dados sensíveis.

Afinal, espera-se que a ANPD seja uma autarquia moderna e dinâmica, de modo a atuar de forma pragmática, objetivando uma mudança efetiva de cultura quanto à proteção de dados[42].

Em síntese, há uma vasta gama de possibilidades a ser adotadas para garantir a proteção contra ataques de engenharia social no ambiente virtual no contexto brasileiro, com especial protagonismo a uma recente entidade pública, a ANPD.

5 CONSIDERAÇÕES FINAIS

Este artigo buscou conceituar o termo engenharia social, analisar sua interação na sociedade da informação e investigar como as técnicas de engenharia social mais comuns são empregadas no ambiente virtual, incluindo *phishing*, *smishing*, *vishing*, *sextortion* e *watering holes*.

As técnicas de engenharia social mais comuns empregadas em ambiente virtual envolvem *phishing*, *smishing*, *vishing*, *sextortion* e *watering holes*. As condutas a elas inerentes se adequam a diversos tipos penais, mostrando-se relevante a recente atuação legislativa no sentido de ampliar a abrangência do Direito Penal de modo a abranger a engenharia social online. Portanto, é possível notar que o Direito Penal, ao menos formalmente, está preparado para enfrentar essa nova realidade impulsionada pela internet.

No entanto, existem obstáculos a impedir a eficácia do Direito Penal na realidade, como o baixo efetivo policial e a estrutura investigatória insuficiente em face da crescente ocorrência de cibercrimes, além da complexidade da prova pericial, da significativa dificuldade para identificar a autoria nesse tipo de crime e dos exíguos prazos de prescrição dos tipos penais aplicáveis às práticas de engenharia social.

Embora o Direito Penal seja ferramenta necessária para prevenir as práticas de engenharia social no ambiente virtual, ele se mostra insuficiente na atual conjuntura. Evidencia-se, portanto, a relevância da implementação de técnicas além do Direito Penal, visando impactar a crescente onda de casos de engenheira social praticados em ambiente virtual no Brasil.

---

[42] TEIXEIRA, Tarcísio, GUERREIRO, Ruth Maria, *Lei Geral de Proteção de Dados Pessoais (LGPD): comentada artigo por artigo*, São Paulo, Editora Saraiva, 2022, *e-book*, p.52.

Políticas públicas implementadas em outros países voltadas à educação do usuário, bem como o combate às *botnets*, entre outras medidas que podem ajudar a prevenir as práticas criminosas objeto deste estudo.

Experiências internacionais, como as observadas na Austrália, Coréia do Sul, Japão, Alemanha e Holanda demonstram a eficácia de uma regulamentação multilateral, realizada em conjunto com provedores de internet e empresas de antivírus, possibilitando, por exemplo, ações preventivas de bloqueio a *botnets* antes que eles sejam usados para enviar *spams* ou outros conteúdos nocivos.

Outras formas de prevenção podem incluir a adoção de selos de verificação em redes sociais, a utilização de *blacklists* para *websites* suspeitos e de *whitelists* para *websites* oficiais, a criação de um período de espera para a oposição de registros de domínios com nomes enganosos, a adoção de autenticação em múltiplos fatores e o aprimoramento de filtros de *spam.*

Políticas públicas em colaboração com o setor privado podem constituir maneiras eficazes de abordar os desafios apresentados pela engenharia social online e crimes cibernéticos em geral.

Este tipo de abordagem reconhece a necessidade de uma cooperação robusta entre o governo e o setor privado para lidar com questões de segurança cibernética.

No Brasil existem estrutura e ferramentas de Direito Administrativo Sancionador que, transcendendo abordagens inerentes unicamente ao Direito Penal, viabilizam a criação de melhores estratégias para conter as práticas de engenharia social online.

A Autoridade Nacional de Proteção de Dados já tem como missão garantir a proteção dos dados pessoais e pode servir como uma entidade importante para coordenar esforços no combate à engenharia social. Afinal, a ANPD dispõe de poder para criar medidas de proteção de dados, o que implica em medidas de prevenção às práticas de engenharia social que visem obter dados sensíveis.

O campo explorado neste artigo é fértil para a realização de pesquisas futuras, especialmente com o recente início de atividades da Autoridade Nacional de Proteção de Dados, cuja atuação empírica poderá ser analisada de modo a reforçar a hipótese aqui investigada.

6 REFERÊNCIAS

ARAUJO, Fábio Lucena de, "Aspectos jurídicos no combate e prevenção ao *ransomware*" *in* BRASIL, Ministério Público Federal, 2ª Câmara de Coordenação e Revisão, org., *Crimes Cibernéticos: coletânea de artigos*, vol. 3, Brasília, MPF, 2018.

BARRETO, Alessandro Gonçalves, BRASIL, Beatriz Silveira, *Manual de investigação cibernética à luz do Marco Civil da Internet*, Rio de Janeiro, Brasport, 2016, *e-book*.

BECK, Ulrich, *Sociedade de risco: rumo a uma outra modernidade*, 2. ed., São Paulo, Editora 34, 2011, Tradução de Sebastião Nascimento.

DUPONT, Benoit, "*Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime*", *Crime Law Soc Change*, v. 67, 2017, pp. 97-116.

BIANCAMANO, Paula, *Mais de 5 milhões de brasileiros foram vítimas do golpe de Clonagem de WhatsApp em 2020*, disponível em: <https://www.psafe.com/blog/mais-de-5-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-clonagem-de-whatsapp-em-2020/>, acesso em: 28 abr. 2023.

BRASIL, Câmara dos Deputados. *Relatório Final da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país*, Brasília, 2016, disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%253D%253E+RCP+10/2015>, acesso em 28 abr. 2023.

BRASIL, Decreto-Lei n°. 2.848, de 7 de dezembro de 1940, Código Penal, *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940, disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, acesso em: 29 abr. 2023.

BRASIL, Lei n°. 12.965, de 23 de abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, *Diário Oficial da União*, Brasília, 24 abr. 2014, disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>, acesso em: 29 abr. 2023.

BRASIL, Lei n°. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), *Diário Oficial da União*, Brasília, 15 ago. 2018, disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>, acesso em: 29 abr. 2023.

BRASIL, Lei n°. 13.853, de 8 de julho de 2019, Altera a Lei 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências, *Diário Oficial da União*, Brasília, 20 dez. 2019, disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>, acesso em: 29 abr. 2023.

BRASIL, Lei n°. 14.155, de 27 de maio de 2021, Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato, *Diário Oficial da União*, Brasília, 28 mai. 2021, disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>, acesso em: 29 abr. 2023.

BRASIL, Lei n°. 14.460, de 25 de outubro de 2022, Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei 13.853, de 8 de julho de 2019, *Diário Oficial da União*, Brasília, 26 out. 2022, disponível em: <in.gov.br/en/web/dou/-/lei-n-14.460-de-25-de-outubro-de-2022-439007249>, acesso em: 29 abr. 2023.

CRESPO, Marcelo Xavier de Freitas, *Crimes digitais*, São Paulo, Editora Saraiva, 2011, *e-book*.

CUNHA, Rogério Sanches, *Manual de Direito Penal: parte especial (arts. 121 ao 361)*, 11. ed., Salvador, Editora Juspodivm, 2019.

FORNASIER, Mateus de Oliveira, KNEBEL, Norberto Milton Paiva, SILVA, Fernanda Viero da, "*Phishing* e engenharia social: entre a criminalização e a utilização de meios sociais de proteção", *Meritum*, vol. 15, n°. 1, jan.-abr. 2020, pp. 116-129.

FORUM BRASILEIRO DE SEGURANÇA PÚBLICA, *Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas*, Anuário Brasileiro de Segurança Pública 2022, disponível em: https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf>, acesso em: 28 abr. 2023

FULLER, Greice Patricia, TATEOKI, Victor Augusto, "Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação", *Revista em Tempo*, vol. 22, n°. 1, fev. 2023, pp. 110-124.

GHAZI-TEHRANI, Adam Kavon, PONTELL, Henry N., "*Phishing evolves: analyzing the enduring cybercrime*", *Victims & Offenders*, vol. 16, n°. 3, 2021, pp. 316-342.

GIL, Antonio Carlos, *Como elaborar projetos de pesquisa*, 4. ed., São Paulo, Atlas, 2017.

HATFIELD, Joseph M., "*Social engineering in cybersecurity: The evolution of a concept", Computers & Security*, vol. 73, mar. 2018, pp. 1-28.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, Internet já é acessível em 90,0% dos domicílios do país em 2021, disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>, acesso em: 28 abr. 2023.

JESUS, Damásio de, MILAGRE, José Antônio, *Manual de crimes informáticos*, São Paulo, Editora Saraiva, 2016, *e-book*.

KULIKOVA, Tatyana *et al*, *El spam y el phishing en 2022*, disponível em: <https://securelist.lat/spam-phishing-scam-report-2022/97582/>, acesso em: 28 abr. 2023.

LYNCH, Jennifer "*Identity theft in cryberspace: crime control methods and their effectiveness in combating phishing attacks*", *Berkeley Techonology Law Journal*, vol. 20, 2005, pp. 259-300.

MARCONI, Marina de Andrade, LAKATOS, Eva Maria, *Fundamentos de metodologia científica*, 5. ed., São Paulo, Atlas, 2003.

PETHERS, Brent, BELLO, Abubakar, "*Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks*", *Future Internet*, vol. 15, n°. 1, jan. 2023, pp. 1-19.

PINTO, Luiz Tiago Souza, BERENGUEL, Orlando Leonardo, "Engenharia social: a porta de entrada para informações confidenciais", *Revista Científica E-Locução*, vol. 1, n°. 17, out. – dez. 2020, pp. 483-498.

REINO UNIDO, *National cyber security strategy 2016-2021*, disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf >, acesso em: 30 abr. 2023.

RODRIGUES, Alex, *Quase 50% dos brasileiros não têm acesso a redes de esgoto, diz MDR*, disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-12/quase-50-dos-brasileiros-nao-tem-acesso-redes-de-esgoto-diz-mdr>, acesso em: 28 abr. 2023.

SILVA, Francisco José Albino Faria Castro e, *Classificação taxonómica dos ataques de Engenharia Social: caracterização da problemática da segurança de informação em Portugal relativamente à Engenharia Social*, 131 p., Dissertação (Mestrado em Segurança dos Sistemas de Informação), Faculdade Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, disponível em: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, acesso em: 28 abr. 2023

SUMAN, Shreya, SRIVASTAVA, Neha, PANDIT, Renu, "*Cyber crimes and phishing attacks*", *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, n°. 2, fev. 2014, pp. 324-327.

TEIXEIRA, Tarcísio, GUERREIRO, Ruth Maria, *Lei Geral de Proteção de Dados Pessoais (LGPD): comentada artigo por artigo*, São Paulo, Editora Saraiva, 2022, *e-book*.

VILELA, Erica, UEDA, Eduardo Takeo, GAVA, Vagner Luiz, "*Phishing* e engenharia social: conceitos, modalidades, técnicas de detecção e prevenção de fraudes. Uma revisão sistemática da literatura" in 19th CONTECSI – *International Conferece on Information Systems and Technology Management*, São Paulo, *Anais Eletrônicos* [...], São Paulo 2022, disponível em: <https://www.tecsi.org/contecsi/index.php/contecsi/19CONTECSI/paper/view/7138>, acesso em 29 abr. 2023.

WENDT, Emerson, JORGE, Higor Vinicius Nogueira, *Crimes cibernéticos: ameaças e procedimentos de investigação*, 3. ed., Rio de Janeiro, Brasport, 2021, *e-book*.