

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

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

DOI: 10.19135/revista.consinter.00019.18

Recebido/Received 29/06/2023 – Aprovado/Approved 17/01/2024

Matheus de Quadros¹ – <https://orcid.org/0000-0001-7971-3799>

Fabrizio Bittencourt da Cruz² – <https://orcid.org/0000-0003-0538-9193>

Abstract

This article analyzes the effectiveness of criminal law in combating social engineering practices in virtual environments in Brazil. It adopts a deductive methodology, beginning with an analysis of the phenomenon of social engineering and then assessing the adequacy of the Brazilian criminal-law response. The research is qualitative and exploratory and draws on documentary and bibliographic sources. The article also examines international studies and experiences in order to identify potential approaches that may complement the fight against online social engineering. It concludes that, despite legislative efforts to bring social engineering practices in virtual environments within the reach of criminal law, structural obstacles undermine the effectiveness of this approach. The article further emphasizes the need for a preventive strategy on the part of the State, to be implemented through complementary public policies.³

Keywords: Social engineering; Prevention; Criminal law.

Summary: 1. Introduction; 2. Criminal typicality of social engineering techniques; 3. Challenges of criminal law in repressing social engineering in virtual environments; 4. Beyond criminal law: Sanctioning Administrative Law as a complementary means of combating social engineering practices; 5. Final considerations; 6. References.

¹ Master's degree in Applied Social Sciences from the State University of Ponta Grossa (UEPG); *lato sensu* postgraduate in Criminal Procedural Law and Criminal Forensic Practice from UEPG and in Constitutional Law from the Damásio Institute of Law (Instituto Damásio de Direito). Professor in the Law Program of the Telémaco Borba University Center. State University of Ponta Grossa, ZIP code 84010-330, Ponta Grossa, Paraná, Brazil. E-mail: mdqmatheus@gmail.com. <https://orcid.org/0000-0001-7971-3799>

² Doctor of Laws from the University of São Paulo (USP) School of Law. Associate Professor at UEPG (undergraduate, master's, and doctoral levels). Leader of the MindTheGap: Innovation in Law project (<https://mdgap.org>). Federal Judge. State University of Ponta Grossa, ZIP code 84010-330, Ponta Grossa, Paraná, Brazil. E-mail: fabriziobittercruz@gmail.com. <https://orcid.org/0000-0003-0538-9193>

³ The English version of this article was produced with the assistance of Claude, an artificial-intelligence system developed by Anthropic.

1 INTRODUCTION

Despite a range of social challenges, the spread of the internet in Brazil has advanced by leaps and bounds. According to data from the Brazilian Institute of Geography and Statistics (Instituto Brasileiro de Geografia e Estatística – IBGE), 90% of Brazilian households already had internet access in 2021.⁴ This broad access has reached levels of democratization far faster and more widespread than those of many other fundamental rights, such as basic sanitation, which remains out of reach for nearly half of the Brazilian population⁵.

The virtual world has imposed a new reality, profoundly reshaping the dynamics of society. As Ulrich Beck observes, modernity has brought about a globalization of risk that transcends class barriers and national borders.⁶ Moreover, with the wide democratization of the internet, new legal interests have emerged and others have been updated to address novel situations⁷.

Legal interests traditionally protected by criminal law, such as honor and property, are affected by the new risks brought about by the internet. There is also intense debate over the need to protect new legal interests, such as the integrity and confidentiality of digital personal data⁸.

As the internet expands, new harmful situations arise that the Brazilian legal system and State apparatus may be unprepared to address, given the scale and speed at which these structural changes occur. According to a survey conducted by the company Kaspersky, the Brazilian population was the world's leading target of phishing attacks on the WhatsApp application,⁹ highlighting the particular vulnerability of Brazilians in this scenario.

This situation relates to a broader concept of practices of manipulation, persuasion, and influence over human behavior aimed at obtaining confidential and/or highly valuable information—practices known as social engineering, which is the main focus of this study. Social engineering is a concept that predates the popularization of the internet, but it has reached a new level of harm with the

⁴ INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, *Internet já é acessível em 90,0% dos domicílios do país em 2021*, Available at: <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>, Accessed on: April 28, 2023.

⁵ RODRIGUES, Alex, *Quase 50% dos brasileiros não têm acesso a redes de esgoto, diz MDR*, Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-12/quase-50-dos-brasileiros-nao-tem-acesso-redes-de-esgoto-diz-mdr>, Accessed on: April 28, 2023.

⁶ BECK, Ulrich, *Sociedade de risco: rumo a uma outra modernidade*, 2. ed., São Paulo, Editora 34, 2011, Tradução de Sebastião Nascimento, p. 43.

⁷ BECK, Ulrich, *Sociedade de risco: rumo a uma outra modernidade*, 2. ed., São Paulo, Editora 34, 2011, Tradução de Sebastião Nascimento, p. 43.

⁸ FULLER, Greice Patricia, TATEOKI, Victor Augusto, “Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação”, *Revista em Tempo*, v. 22, n. 1, fev. 2023, pp. 110-124.

⁹ KULIKOVA, Tatyana et al, *El spam y el phishing en 2022*, Available at: <https://securelist.lat/spam-phishing-scam-report-2022/97582/>, Accessed on: April 28, 2023.

internet's expansion, owing to the ease of obtaining information and deceiving victims. In response to this problem, legislators and the general public commonly turn to criminal law, seeking to prevent these practices and to hold their perpetrators accountable.

But is criminal law adequate to deal with online scams that rely on social engineering?

To answer this question, we will examine the issue from a formal standpoint, in order to verify whether criminal law contains offenses that encompass situations of social engineering. We will then assess the question from a practical/material perspective, with the aim of observing whether Brazil's police and judicial structures have been effective in combating social engineering through criminal law.

Finally, we will explore whether other branches of law might be better suited to combating social engineering in cyberspace. In this regard, we suggest the use of Sanctioning Administrative Law (*Direito Administrativo Sancionador*)¹⁰ as a more effective alternative.

Following Gil's classification, this research is qualitative and exploratory,¹¹ seeking to obtain a broader perspective on the Brazilian criminal-law response to internet scams involving social engineering. We adopt a deductive approach, starting from an analysis of the phenomenon of social engineering in order to determine whether the criminal treatment given to the phenomenon in Brazil has proved satisfactory.

To build the theoretical framework underpinning this article, we used bibliographic and documentary research techniques, following the guidance of Marconi and Lakatos.¹² In the bibliographic research, we consulted specialized books on topics related to the object of study, as well as articles, with an emphasis on searches of the following databases: Scientific Electronic Library Online (SciELO) Brazil, Google Scholar, and the CAPES Journal Portal (Portal de Periódicos da CAPES), selecting the articles on the basis of their relevance to the object of study.

The literature review was carried out in the aforementioned databases, searching for the terms "regulation," "social engineering," "phishing," "prevention," "criminal law," "virtual crimes," and "public policies" in various combinations in Portuguese, Spanish, and English.

Despite the existence of various studies on computer crimes, there is little work on the effectiveness of criminal law in dealing with some of the new situations brought about by the popularization of the internet.

Many of the studies used come from different fields of knowledge, reflecting the interdisciplinarity and debate that the topic necessarily requires. Moreover,

¹⁰ Sanctioning Administrative Law is the branch of Brazilian public law that governs the State's power to impose administrative penalties; it is distinct from, though complementary to, criminal law.

¹¹ GIL, Antonio Carlos, *Como elaborar projetos de pesquisa*, 4. ed., São Paulo, Atlas, 2017, pp. 41-42.

¹² MARCONI, Marina de Andrade, LAKATOS, Eva Maria, *Fundamentos de metodologia científica*, 5. ed., São Paulo, Atlas, 2003.

owing to the rapid evolution of the digital world and to recent legislative innovations—such as the 2018 General Data Protection Law (Lei Geral de Proteção de Dados)—not all available materials are up to date.

The documentary research was carried out mainly through an analysis of the relevant legislation and of studies conducted by research agencies on the practice of social engineering in Brazil and its consequences.

This study adopts the hypothesis that criminal law is insufficient to adequately combat criminal practices related to social engineering. This hypothesis was formulated on the basis of empirical observations of everyday situations involving social engineering in the virtual environment which, in the authors' empirical perception, have not received adequate treatment.

As for the results obtained, this study concludes that criminal law is insufficient as the sole means of combating social engineering practices in the Brazilian virtual environment, despite the legislature's efforts to modernize Brazilian criminal legislation.

2 CRIMINAL TYPICALITY OF SOCIAL ENGINEERING TECHNIQUES

Social engineering encompasses a vast set of practices that employ manipulation, persuasion, and influence over victims as strategies for capturing information. Analyzing 134 definitions of the term in academic studies written between 1990 and 2017, Joseph M. Hatfield concluded that the term social engineering rests on three pillars: epistemic asymmetry, technocratic dominance, and teleological replacement¹³.

According to the author, social engineering occurs when a person (or a group of people) holds a certain advantage in technical knowledge over another and uses that advantage to alter the victim's behavior, leading the victim to take some action desired by that person or group¹⁴.

Considering the forms of social engineering that make use of the internet, several techniques frequently used in this context stand out: phishing, sextortion/catphishing, smishing, vishing, and watering holes¹⁵.

The phishing technique involves impersonating an entity or person trusted by the victim in order to obtain personal data. The social engineer typically sends, by e-mail or via social media messaging, a website designed to convey a sense of trust and/or familiarity to the victim, inducing the victim to reveal sensitive data or install malicious software^{16/17}.

¹³ HATFIELD, Joseph M., "Social engineering in cybersecurity: The evolution of a concept", *Computers & Security*, v. 73, mar. 2018, pp. 1-28.

¹⁴ HATFIELD, Joseph M., "Social engineering in cybersecurity: The evolution of a concept", *Computers & Security*, v. 73, mar. 2018, pp. 1-28.

¹⁵ In addition to the techniques described in this study, there are also several others that are commonly cited, such as dumpster diving, baiting, and shoulder surfing. However, owing to the manner in which these forms of social engineering are carried out, they fall outside the scope of this study.

¹⁶ PINTO, Luiz Tiago Souza, BERENGUEL, Orlando Leonardo, "Engenharia social: a porta de entrada para informações confidenciais", *Revista Científica E-Locução*, v. 1, n. 17, out. – dez. 2020, p. 489.

With the sextortion/catphishing technique, the social engineer obtains intimate images of the victim and uses them to embarrass the victim, coercing the person into handing over money, information, or performing a specific action, under threat of disclosing the content¹⁸.

Smishing is a variation of the phishing technique that uses text messages (SMS) to induce the victim to click on a suspicious link sent by the sender within the message. Through that link, the social engineer seeks to obtain the victim's sensitive data by means of forms or the installation of malicious software^{19/20}.

Vishing is likewise similar to the phishing technique. It consists of deceiving the victim with tactics that make the victim believe they are speaking with a trusted institution, such as their own bank. The social engineer—already in possession of some of the victim's data, which will be used to gain the victim's trust—telephones the victim while posing as an institution that needs “confirmation” of the person's sensitive data^{21/22}.

Through the watering holes technique, the social engineer infects websites while targeting a specific user or group of users. The aim is that the user(s) will not suspect the medium used and will trust the infected website, providing sensitive information or downloading malicious software²³.

Many of the practices mentioned fall within criminal offenses already on the books. Phishing, smishing, vishing, and watering holes fit Article 171 of the Penal Code (Código Penal), under which the crime of fraud consists of “obtaining, for oneself or for another, an unlawful advantage, to the detriment of another, by inducing or keeping someone in error, through artifice, ruse, or any other fraudulent means.”

¹⁷ 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 de Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, Available at: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, Accessed on: April 28, 2023, p. 27.

¹⁸ PETHERS, Brent, BELLO, Abubakar, “Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks”, *Future Internet*, v. 15, n. 1, jan. 2023, pp. 1-5.

¹⁹ PINTO, BERENGUEL, op. cit., p. 491.

²⁰ SILVA, op. cit., p. 28.

²¹ PINTO, Luiz Tiago Souza, BERENGUEL, Orlando Leonardo, “Engenharia social: a porta de entrada para informações confidenciais”, *Revista Científica E-Locução*, v. 1, n. 17, out. – dez. 2020, p. 490.

²² 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 de Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, Available at: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, Accessed on: April 28, 2023, p. 28.

²³ PINTO, BERENGUEL, loc. cit.

Reinforcing this point, Law No. 14,155/2021 broadened the offense of fraud by adding so-called electronic fraud, set out in Articles 171, §2-A, and 171, §2-B, of the Penal Code.

With this legislative innovation, the penalty for the crime of fraud was increased where the fraud is committed using information provided through social media, e-mails (phishing), telephone calls (vishing), or any other similar fraudulent means.

The legislature, aware of the harmful tendencies of globalization, further determined that if the crime of fraud through electronic means is committed using a server maintained outside Brazilian territory, the penalty set out in Article 171, §2-A, of the Penal Code is increased by one-third to two-thirds.

Thus, the legislature was concerned not only with clearly defining the situations in which fraud could occur through electronic means, but also with increasing the penalty for such cases.

It is worth noting that, depending on the specific case, the crimes of theft (Article 155 of the Penal Code), criminal damage (Article 163 of the Penal Code), and false identity (Article 307 of the Penal Code) may be established. In addition, where the practices involve the social engineer's unauthorized access to a victim's computer device, whether to obtain data or to install malicious software, the crime of invasion of a computer device (Article 154-A of the Penal Code) may be established.

With respect to the practice of sextortion, a variety of criminal offenses may apply, depending on how the intimate content was obtained and the purpose for which it is used. Sextortion involves obtaining the victim's intimate content as part of the social engineering practice.

The first act of this technique may constitute the offenses of violation of a computer device (Article 154-A of the Penal Code) or sexual violation through fraud (Article 215 of the Penal Code).

As for the second act, in which the intimate content is used to obtain advantages, it may unfold into several typified conducts.

In the view of Rogério Sanches Cunha, if the perpetrator coerces the victim into not doing what the law permits, or into doing what it does not require, the crime of unlawful coercion (Article 146 of the Penal Code) occurs. If the coercion of the victim is carried out with the intent to obtain an undue economic advantage—to do, tolerate the doing of, or refrain from doing something—the author considers that the crime of extortion (Article 158 of the Penal Code) is established. On the other hand, if the victim is coerced into engaging in sexual activity, the crime of rape (Article 213 of the Penal Code) arises²⁴.

²⁴ CUNHA, Rogério Sanches, *Manual de Direito Penal: parte especial (arts. 121 ao 361)*, 11. ed., Salvador, Editora Juspodivm, 2019, pp. 208-209.

Thus, it can be observed that social engineering practices may fall within various existing criminal offenses²⁵.

In recent years, the legislature has developed new categories of crimes, qualifying circumstances, and grounds for increasing penalties, with the aim of assisting legal practitioners in applying criminal rules to cases of social engineering.

Although there may be specific situations that do not fit within the criminal offenses currently in force, it is plausible to assert that, at least in formal terms, criminal law is prepared to combat the cybercrime arising from social engineering practices.

Nevertheless, one question imposes itself: has the current criminal-legislative framework proved effective in combating social engineering?

3 CHALLENGES OF CRIMINAL LAW IN REPRESSING SOCIAL ENGINEERING IN VIRTUAL ENVIRONMENTS

As discussed in the previous section, criminal law has advanced significantly as a State instrument for combating undesirable conduct in the virtual sphere. However, there is an important distinction between reality and the ideal.

Reports released by security companies and public institutions show that social engineering crimes committed in the virtual environment have reached previously unimaginable proportions, hampering the State's response.

According to a survey conducted by the digital security laboratory dfndr lab, more than five million people were victims of WhatsApp account cloning in 2020²⁶—conduct that fits the phishing technique already described in this study.

In a similar vein, the 2022 Brazilian Public Security Yearbook (Anuário Brasileiro de Segurança Pública 2022), produced by the Brazilian Forum on Public Security (Fórum Brasileiro de Segurança Pública), reports a 179.9% increase in fraud rates in the country between 2018 and 2021, driven by fraud crimes committed in the digital environment^{27/28}.

²⁵ JESUS, Damásio de, MILAGRE, José Antônio, *Manual de crimes informáticos*, São Paulo, Editora Saraiva, 2016, e-book, p. 21.

²⁶ BIANCAMANO, Paula, *Mais de 5 milhões de brasileiros foram vítimas do golpe de Clonagem de WhatsApp em 2020*, Available at: <<https://www.psafes.com/blog/mais-de-5-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-clonagem-de-whatsapp-em-2020/>>, Accessed on: April 28, 2023.

²⁷ The 2022 Brazilian Public Security Yearbook further notes that this figure was compiled without data from nine states of the Brazilian federation, which makes the number of crimes committed through social engineering by electronic means even more significant in the current scenario, since the real figure, considering all the states of the Federation, is probably much higher.

²⁸ FORUM BRASILEIRO DE SEGURANÇA PÚBLICA, “Os crimes patrimoniais no Brasil: entre novas e velhas dinâmicas”, *Anuário Brasileiro de Segurança Pública 2022*, Available at: <https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf>>, Accessed on: April 28, 2023, p. 8.

Additionally, according to data from the same Forum on Public Security, in 2021 at least 60,590 cases of fraud through electronic means were recorded²⁹.

It is evident, therefore, that a large share of crimes in present-day Brazil occurs in the virtual environment.

This new form of criminality adds a variable to the general increase in the number of crimes. Beyond common factors, such as population growth and social inequality, public authorities must now adjust to the rise in criminality resulting from the new scenarios of the contemporary world.

This brings us to the issue of scarcity of resources. There is a budgetary limit to dealing with a growing number of offenses.

How will the police authorities be able to handle their investigations with the same efficiency, for instance, in the face of an alarming increase in crimes committed in the digital environment? Will there be budgetary provision matching an increase in resources for public security in the same proportion as the numbers of crimes committed in the virtual environment rise? These questions appear to have negative answers.

As recorded in the 2016 final report of the Parliamentary Commission of Inquiry (Comissão Parlamentar de Inquérito – CPI) on Cybercrimes, one of the main problems identified in combating cybercrime in Brazil is the shortage of personnel in the Federal Police (Polícia Federal) in the face of the growing caseload, together with the deficient structures of the Civil Police (Polícia Civil) and the Federal Police³⁰.

Moreover, the manner of investigation has undergone a significant transformation. The nature of the evidence in crimes committed in the analog world is very different from that in digital crimes. For so-called street crimes, the authorship and materiality of the offenses are generally established through witness testimony, searches and seizures, security-camera footage, and other means obtained through predominantly physical procedures. In digital crimes, by contrast, the evidence is primarily forensic, which makes investigations more difficult and more expensive.

According to Emerson Wendt and Higor Vinicius Nogueira Jorge, the challenges in investigating cybercrime in Brazil include the lack of adequate training of police officers and other actors in criminal prosecution, as well as the absence of specialized bodies to handle cybercrimes³¹.

²⁹ Ibid., p. 8.

³⁰ 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, Available at: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codtcor=1455189&filename=REL+4/2016+CPICIBER+%253D%253E+RCP+10/2015>, Accessed on April 28, 2023, pp. 85-87.

³¹ 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.

Globalization and the popularization of the internet have eliminated the physical distances between the crime scene and the perpetrator, often rendering investigative activity unworkable. The criminal does not necessarily live in the same city, state, or region where the crime is consummated, since the social engineer may be based on the other side of Brazil or even in another country. This characteristic makes it necessary to issue letters rogatory, whether domestic (*cartas precatórias*) or international (*cartas rogatórias*)³², in order to question a possible suspect or witnesses, demanding a great deal of time and resources.

Furthermore, social engineers tend to use protocols or systems that hinder the collection of evidence of authorship. Alessandro Gonçalves Barreto and Beatriz Silveira Brasil point out that the first names to surface as perpetrators in investigations of social engineering crimes are false or “straw men” (*laranjas*)^{33/34}. Networks such as TOR (The Onion Router) make the investigators’ task even harder by masking the social engineer’s original IP (Internet Protocol) and location through several layers of other computers connected to the system³⁵.

Added to this is the race against time, since the criminal offenses discussed in this study do not have particularly long limitation periods under Article 109 of the Penal Code. Thus, the problems mentioned above may lead to the extinguishment of criminal liability before the perpetrators are effectively held accountable.

In short, there are several structural obstacles that prevent the criminal offenses pertaining to online social engineering from being effectively enforced against this practice in Brazil, evidencing the insufficiency of criminal law.

4 BEYOND CRIMINAL LAW: SANCTIONING ADMINISTRATIVE LAW AS A COMPLEMENTARY MEANS OF COMBATING SOCIAL ENGINEERING PRACTICES

The scenario is conducive to the use of other techniques for combating social engineering practices in the Brazilian virtual environment, in conjunction with criminal-law strategies.

We adopt the perspective of Jennifer Lynch, in which the strategies for combating social engineering offenses are divided into three levels: self-help (primary-level strategies); architecture and control by private entities (secondary-level strategies); and law enforcement (tertiary-level strategies)³⁶.

³² In Brazilian procedure, a *carta precatória* is a letter of request transmitted between courts within the country, whereas a *carta rogatória* is the equivalent instrument addressed to a foreign jurisdiction; both are forms of letters rogatory.

³³ In Brazilian usage, *laranjas* (literally “oranges”) are front persons whose names or accounts are used to conceal the true perpetrators of a fraud or financial crime.

³⁴ 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.

³⁵ 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.

³⁶ LYNCH, Jennifer “Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks”, *Berkeley Technology Law Journal*, v. 20, 2005, pp. 274-299.

According to Lynch, it would be necessary to adopt other strategies before legal involvement, mainly because of the difficulty and cost of investigations.³⁷ Along these lines, the study will turn to an analysis of other ways in which the State can contribute to the fight against social engineering–related activities in the virtual environment.

Along this argumentative line, it is suggested that the solution may lie in shifting the focus of State action, moving from a primarily repressive approach to a preventive one.

As mentioned earlier, the main obstacle to the effectiveness of criminal law lies in producing evidence of materiality and indications of authorship, given the material limitations faced by the State. Moreover, criminal law operates by attempting to hold perpetrators accountable after the harm has already materialized, often without any possibility of effective redress.

Therefore, a possible solution might lie not in punishing social engineers after the fact, but in creating a regulation of best practices that hinders social engineering. In this regard, the specialized literature is consistent in proposing some effective prevention techniques.

A primary point as a technique for preventing social engineering techniques is user education. To avoid such techniques, it is essential that users understand that, when online, they must take extra precautions, given the difficulty of verifying the legitimacy of people in virtual environments.

Thus, it is vital to broadly promote attitudes aimed at making people aware of the risks inherent in the virtual environment. This guideline is supported by the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), which provides that one of the objectives of internet use in Brazil is to promote “access to information, to knowledge, and to participation in cultural life and in the conduct of public affairs,” pursuant to Article 4, item II, of Law No. 12,965/2014.

In addition, as Mateus de Oliveira Fornasier, Norberto Milton Paiva Knebel, and Fernanda Viero da Silva emphasize, user education is directly linked to the concept of digital citizenship, which presupposes the technical empowerment of users in the face of the technological asymmetries of the social structure.³⁸

A study conducted by Adam Kavon Ghazi-Tehrani and Henry N. Pontell suggests that the main pillars of awareness campaigns should focus on understanding how social engineering scams work (awareness) and how to recognize a scam attempt (prevention)^{39/40}.

³⁷ Ibid., p. 292.

³⁸ 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*, v. 15, n. 1, jan.-abr. 2020, p. 123.

³⁹ GHAZI-TEHRANI, Adam Kavon, PONTELL, Henry N., “Phishing evolves: analyzing the enduring cybercrime”, *Victims & Offenders*, v. 16, n. 3, 2021, pp. 333-334.

⁴⁰ In this case, the study produced by the authors focuses on the phishing technique. However, its conclusions apply to all types of social engineering techniques carried out in the virtual environment.

As examples of public policies for raising awareness of the risks of cybercrime, it is relevant to mention two initiatives adopted by the United Kingdom: “10 Steps to Cyber Security” and “Cyber Essentials.” Both policies focus on educating businesses, going beyond mere awareness to persuade companies to take proactive measures to mitigate risks in the virtual environment.⁴¹

On another front, the preventive fight against botnets⁴², which are frequently used in phishing attacks, represents an effective large-scale strategy against social engineering practices.

International experiences, such as those observed in Australia, South Korea, Japan, Germany, and the Netherlands, demonstrate the effectiveness of multilateral regulation carried out jointly with internet service providers and antivirus companies.⁴³ This enables preventive action, blocking the effect of identified botnets before they are used to send spam or other harmful content.

Other forms of prevention include: the adoption of verification badges on social media; the use of blacklists for suspicious websites and whitelists for official websites; the creation of a waiting period for opposing domain-name registrations with misleading names; the adoption of multi-factor authentication; and the improvement of spam filters^{44/45}.

Public policies in collaboration with the private sector can be an effective way of addressing the challenges posed by social engineering and cybercrime in general.

This type of approach recognizes the need for robust cooperation between the government and the private sector to deal with cybersecurity issues. With a view to the effective adoption of these techniques, their incorporation into legislation is suggested.

Brazilian regulation of the digital space is advancing rapidly. Laws such as the Marco Civil da Internet and the General Data Protection Law (Lei Geral de Proteção de Dados) represent significant advances in creating a safer online

⁴¹ REINO UNIDO, *National cyber security strategy 2016-2021*, Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>, Accessed on: April 30, 2023.

⁴² The term botnet refers to a network of a large number of computers infected by trojan horses with the aim of being managed remotely for spam campaigns or DDoS attacks.

⁴³ 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. 107-111.

⁴⁴ SUMAN, Shreya, SRIVASTAVA, Neha, PANDIT, Renu, “Cyber crimes and phishing attacks”, *International Journal on Recent and Innovation Trends in Computing and Communication*, v. 2, n. 2, fev. 2014, p. 326.

⁴⁵ 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 Conference on Information Systems and Technology Management*, São Paulo, Anais Eletrônicos [...], São Paulo 2022, Available at: <<https://www.tecsi.org/contecsi/index.php/contecsi/19CONTECSI/paper/view/7138>>, Accessed on April 29, 2023, pp. 9-11.

environment. However, as suggested in this text, there is still room to advance in this direction and to explore the possibility of more effective legislation to combat social engineering practices.

This study points toward the enactment of best-practice laws against social engineering, with a view to adopting, as primary tactics, the procedures described above in addition to the entire legal and administrative structure already existing in Brazil. A dual approach combining the preventive action of Sanctioning Administrative Law with the repressive response of criminal law appears to constitute a promising strategy.

It is further suggested that, building on the structure already created by the General Data Protection Law, new tasks could be incorporated into the structure of the National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD), provided for in Article 55-J of the General Data Protection Law and recently established by Law No. 13,853/2019.

With respect to the ANPD, its recent elevation to the status of an autarchy (*autarquia*)⁴⁶ and the expansion of its responsibilities could play a crucial role in protecting citizens' data and preventing social engineering. The ANPD already has the mandate to ensure the protection of personal data and can serve as an important entity for coordinating efforts to combat social engineering within the scope of Sanctioning Administrative Law.

This is because, under the General Data Protection Law, it falls to the ANPD to lay down standards and techniques used in data anonymization processes and to carry out verifications regarding their security; to establish complementary rules for the activities of communication and shared use of personal data; and to recommend the adoption of standards and best practices for the processing of personal data by public authorities.

Also among the ANPD's responsibilities are to lay down minimum technical standards on security, technical, and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or unlawful processing, and to encourage the adoption of technical standards that facilitate control by data subjects over their personal data.

The ANPD has powers to create data protection measures, which entails measures to prevent social engineering practices aimed at obtaining sensitive data.

After all, the ANPD is expected to be a modern and dynamic autarchy, so as to act pragmatically with a view to bringing about an effective change of culture regarding data protection⁴⁷.

⁴⁶ In Brazilian administrative law, an *autarquia* is an autonomous public-law entity created by statute to carry out State functions with administrative and financial independence; the term does not correspond to the English "autarchy" in the sense of self-sufficiency.

⁴⁷ 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.

In short, there is a vast range of possibilities to be adopted to ensure protection against social engineering attacks in the virtual environment in the Brazilian context, with a particularly prominent role for a recent public entity, the ANPD.

5 FINAL CONSIDERATIONS

This article sought to conceptualize the term social engineering, to analyze its interaction within the information society permeated by the internet, and to investigate how the most common social engineering techniques are employed in the virtual environment, including phishing, smishing, vishing, sextortion, and watering holes.

It was found that these techniques fit various already existing criminal offenses and that, in recent years, the legislature has created criminal laws capable of encompassing the new situations of social engineering. It was therefore possible to observe that criminal law, at least formally, is prepared to confront this new reality brought about by the internet.

However, this study also found that there are obstacles preventing the full effectiveness of criminal law in practice.

Among the factors cited are the low police personnel levels and the inadequate structure of police departments in the face of the growing demand of cybercrimes; the costs and complexity of forensic evidence; the great distances between the victim, the crime scene, and the perpetrators; the use of systems by criminals to hinder their identification; and the short limitation periods of the criminal offenses applicable to social engineering practices.

For this reason, it was understood that, although criminal law is a necessary tool for combating social engineering practices in the virtual environment, it proves insufficient in the current circumstances.

Finally, this study addressed the implementation of techniques outside criminal law, with a view to easing the burden of the growing wave of social engineering cases carried out in the Brazilian virtual environment.

International experiences with public policies aimed at user education were observed, as well as the fight against botnets, among other measures that may help prevent the criminal practices that are the object of this study.

Additionally, the relevance of the National Data Protection Authority in the context of Brazilian Sanctioning Administrative Law was addressed, given that this autarchy holds broad powers that can assist in combating social engineering practices.

It was perceived that in Brazil there are structures and tools of Sanctioning Administrative Law which, transcending approaches inherent solely to criminal law, make it feasible to create better strategies for curbing online social engineering practices.

The field explored in this article is fertile ground for future research, especially given the recent commencement of the activities of the National Data Protection Authority, whose empirical performance may be analyzed in a way that reinforces the hypothesis investigated here.

6 REFERENCES

- ARAÚJO, 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*, Available at: <<https://www.psafec.com/blog/mais-de-5-milhoes-de-brasileiros-foram-vitimas-do-golpe-de-clonagem-de-whatsapp-em-2020/>>, Accessed on: April 28, 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, Available at: <https://www.camara.leg.br/proposicoesWeb/pop_mos-tranintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb?codeor=1455189&filename=REL+4/2016+CPICIBER+%253D%253E+RCP+10/2015>, Accessed on April 28, 2023.
- BRASIL, Decreto-Lei nº. 2.848, de 7 de dezembro de 1940, Código Penal, Diário Oficial da União, Rio de Janeiro, 31 dez. 1940, Available at: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>, Accessed on: April 29, 2023.
- BRASIL, Lei nº. 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, Available at: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>, Accessed on: April 29, 2023.
- BRASIL, Lei nº. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Diário Oficial da União, Brasília, 15 ago. 2018, Available at: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm>, Accessed on: April 29, 2023.
- BRASIL, Lei nº. 13.853, de 8 de julho de 2019, Altera a Lei nº 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, Available at: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm>, Accessed on: April 29, 2023.
- BRASIL, Lei nº. 14.155, de 27 de maio de 2021, Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato, Diário Oficial da União, Brasília, 28 mai. 2021, Available at: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm>, Accessed on: April 29, 2023.
- BRASIL, Lei nº. 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 nº 13.853, de 8 de julho de 2019, Diário Oficial da União, Brasília, 26 out. 2022, Available at: <in.gov.br/en/web/dou/-/lei-n-14.460-de-25-de-outubro-de-2022-439007249>, Accessed on: April 29, 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*, v. 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*, Available at: <https://forumseguranca.org.br/wp-content/uploads/2022/07/07-anuario-2022-os-crimes-patrimoniais-no-brasil-entre-novas-e-velhas-dinamicas.pdf>>, Accessed on: April 28, 2023
- FULLER, Greice Patricia, TATEOKI, Victor Augusto, “Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação”, *Revista em Tempo*, v. 22, n. 1, fev. 2023, pp. 110-124.
- GHAZI-TEHRANI, Adam Kavon, PONTELL, Henry N., “Phishing evolves: analyzing the enduring cybercrime”, *Victims & Offenders*, v. 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*, v. 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*, Available at: <<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>>, Accessed on: April 28, 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*, Available at: <<https://securelist.lat/spam-phishing-scam-report-2022/97582/>>, Accessed on: April 28, 2023.
- LYNCH, Jennifer “Identity theft in cyberspace: crime control methods and their effectiveness in combating phishing attacks”, *Berkeley Technology Law Journal*, v. 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*, v. 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*, v. 1, n. 17, out. – dez. 2020, pp. 483-498.
- REINO UNIDO, *National cyber security strategy 2016-2021*, Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>, Accessed on: April 30, 2023.
- RODRIGUES, Alex, *Quase 50% dos brasileiros não têm acesso a redes de esgoto, diz MDR*, Available at: <<https://agenciabrasil.ebc.com.br/geral/noticia/2021-12/quase-50-dos-brasileiros-nao-tem-acesso-rede-s-de-esgoto-diz-mdr>>, Accessed on: April 28, 2023.
- SILVA, Francisco José Albino Faria Castro e, *Classificação taxonômica 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 de Engenharia, Universidade Católica de Portugal, Porto (Portugal), 2013, Available at: <repositorio.ucp.pt/bitstream/10400.14/15690/1/Tese%20de%20Mestrado%20-%20Engenharia%20Social.pdf>, Accessed on: April 28, 2023
- SUMAN, Shreya, SRIVASTAVA, Neha, PANDIT, Renu, “Cyber crimes and phishing attacks”, *International Journal on Recent and Innovation Trends in Computing and Communication*, v. 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 Conference on Information Systems and Technology Management*, São Paulo, Anais Eletrônicos [...], São Paulo 2022, Available at: <<https://www.tecsi.org/contecsi/index.php/contecsi/19CONTECSI/paper/view/7138>>, Accessed on April 29, 2023.

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