PHISHING AND SOCIAL ENGINEERING: BETWEEN CRIMINALIZATION AND THE USE OF SOCIAL MEANS OF PROTECTION

PHISHING E ENGENHARIA SOCIAL: ENTRE A CRIMINALIZAÇÃO E A UTILIZAÇÃO DE MEIOS SOCIAIS DE PROTEÇÃO

Mateus de Oliveira Fornasier[1]
Norberto Milton Paiva Knebel[2]
Fernanda Viero da Silva[3]

ABSTRACT

This article aimed to study the need for criminal typification of phishing. In this sense, it investigated how the Brazilian legal system deals (and must deal) with the criminal aspects of digital crimes against property. Its hypothesis was that the crimes against the person committed by hacking were included in the Brazilian penal system, in line with the principles of defense of honor and vulnerability, but crimes against digital property have not been typified yet — however, the need for such a criminalization was considered doubtful, in view of the greater social importance that would have creative and alternative solutions, based on phishing prevention policies and vulnerabilities to social engineering. Methodologically, the research used the hypothetical-deductive procedure method, with a qualitative and technical approach to bibliographic-documentary research. In this sense, the work began with locating the practice of phishing within social engineering strategies. Soon afterwards, a legal-dogmatic study was carried out in order to identify whether such a practice is penalized in Brazil. Finally, it was considered if the best way to avoid the practice of phishing: whether it would be the specific typification of the conduct or if other non-criminal forms of phishing prevention would be more efficient than the criminal typification. As a result, it appeared that there are more creative, innovative and socially better alternatives for data protection and the prevention of cybercrime, than mere specific criminalization. These strategies go mainly through the development of (I) an informational education and empowerment of digital citizenship; (II) an organizational culture of data protection

[1] Professor of the Stricto Sensu Graduate Program (Master and Doctorate) in Human Rights at the Regional University of the Northwest of the State of Rio Grande do Sul (UNIJUI). Doctor in Public Law from the University of Vale do Rio dos Sinos (UNISINOS, Brazil), with Post-Doctorate in Law from the University of Westminster (United Kingdom). http://orcid.org/0000-0002-1617-4270. http://lattes.cnpq.br/3316861562386174. mateus.fornasier@gmail.com.

[2] Doctoral student of the Stricto Sensu Graduate Program in Human Rights at the Regional University of the Northwest of the State of Rio Grande do Sul (UNIJUI). http://orcid.org/0000-0003-0674-8872. http://lattes.cnpq.br/4232557221807840. norberto.knebel@gmail.com.

[3] Scientific Initiation Scholarship (PIBIC / CAPES). Student of the Law Course at the Regional University of the Northwest of the State of Rio Grande do Sul (UNIJUI). http://orcid.org/0000-0002-3978-7395. http://lattes.cnpq.br/3060049367537210. fefeviero@gmail.com.
Development agency: Research Foundation of the State of Rio Grande do Sul (FAPERGS).

Como citar esse artigo/How to cite this article:
FORNASIER, Mateus de Oliveira. KNEBEL, Norberto Milton Paiva. SILVA, Fernanda Viero da. *Phishing and social engineering: between criminalization and the use of social means of protection*. Revista Meritum, Belo Horizonte, vol. 15, n. 1, p. 117-131 jan./abr. 2020. DOI: https://doi.org/10.46560/meritum.v15i1.7771.

through corporate policies or compliance; and (III) self-regulation or regulation by design of the technology companies themselves, basing their algorithms on principles of privacy and human rights.

Keywords: Social Engineering. Phishing. Digital Scam. Criminalization.

RESUMO

Este artigo objetivou estudar a necessidade de tipificação criminal do phishing. Nesse sentido, investigou-se de que forma o ordenamento jurídico brasileiro trata (e deve tratar) dos aspectos penais dos crimes digitais contra o patrimônio. Sua hipótese é de que os crimes contra a pessoa praticados por hacking foram incluídos no sistema penal brasileiro, alinhados aos princípios de defesa da honra e da vulnerabilidade, mas os crimes patrimoniais digitais ainda não foram tipificados — contudo, duvidou-se da necessidade dessa criminalização frente à importância social maior que teriam soluções criativas e alternativas, baseadas em políticas de prevenção ao phishing e as vulnerabilidades à engenharia social. Metodologicamente, a pesquisa se valeu do método de procedimento hipotético-dedutivo, com abordagem qualitativo e técnica de pesquisa bibliográfico-documental. Nesse sentido, o trabalho iniciou com a localização da prática do phishing dentro de estratégias de engenharia social. Passou-se, logo após, à realização de um estudo jurídico-dogmático a fim de identificar se tal prática é tipificada penalmente no Brasil. Por fim, foi ponderado se o melhor caminho para evitar a prática do phishing: se seria a tipificação específica da conduta ou se outras formas não penais de prevenção ao phishing seriam mais eficientes do que a tipificação penal. Como resultados, apresentou-se que há alternativas mais criativas, inovadoras e socialmente mais adequadas para a proteção dos dados e a prevenção aos cibercrimes, do que a mera criminalização especifica. Essas estratégias perpassam, principalmente, pelo desenvolvimento de (I) uma educação informacional e empoderamento da cidadania digital; (II) de uma cultura organizacional de proteção de dados por meio das políticas corporativas ou compliance; e (III) da autorregulação ou regulação by design das próprias empresas de tecnologia, pautando seus algoritmos em princípios de privacidade e direitos humanos.

Palavras-Chave: *Engenharia Social. Phishing. Estelionato Digital. Criminalização.*

INTRODUCTION

The rise of digital relations and the ubiquity of virtual systems to promote commerce, banking and social networks have put the so-called "cybercrimes" in question, resulting in a multiplicity of proposed solutions. Social engineering has an impact on people's lives and company activities, affecting privacy and data security - and the vulnerability of information management systems isn't in technical aspects, but in human relations.

The growing theoretical sophistication about these digital crimes allows to expand the discussions even outside the scope of criminal dogmatics, linking political and social contexts to the need to resist and protect citizens from frauds that use social engineering to obtain patrimonial advantage. In this sense, phishing unites technological and non-technological practices of social engineering to deceive users on the internet, implying that it occurs through a logical and coherent decision by the user - however, it reveals itself as the delivery of important data to achieve the economic objective of the swindler. This legal asset (property) is already protected against fraud by the crime of fraud/scam; however, there is no specific typification for when using digital media - hence the nomenclature "digital fraud" or "digital scam" (*"estelionato digital"*).

The problem that caused this research can thus be described: how does the Brazilian legal system deal (and must deal) with the criminal aspects of digital crimes against property? It is hypothesized, for this questioning, that crimes against the person committed by hacking were included in the Brazilian penal system, in line with the principles of defense of honor and vulnerability of children and adolescents, for example; but, digital crimes against property (digital property crimes) have not yet been typified - however, there is doubt about the need for this specific criminalization, given the greater social importance that would have the creative and alternative solutions, based on phishing prevention policies and the vulnerabilities exposed to social engineering strategies.

The general objective of this article is to carry out a study on the need for criminal classification to reach social engineers who apply scams in the digital sphere with social protection means, ranging from individual practices to those of large corporations, including the obligation of the Public Power in promote digital citizenship. To achieve this general objective, its development was divided into three sections. The first is intended to study the practices of social engineering and its consequences for citizens and companies. The second is dedicated to understanding the criminalization process of certain digital practices, focusing mainly on the need to criminalize digital fraud/scam. Finally, the third part looks at non-criminal ways of preventing phishing.

Methodologically, it is listed that this research, of an academic nature, used the hypothetical-deductive procedure method, with a qualitative approach method and bibliographic--documentary research technique.

In this sense, the work begins with locating the practice of phishing within social engineering strategies. Soon afterwards, a legal-dogmatic study was carried out in order to identify if such a practice is criminally typified in Brazil. Finally, it is considered whether the best way to avoid the practice of phishing would be: the specific type of conduct, or if other non-criminal forms of phishing prevention would be more efficient than the criminal type.

1 SOCIAL ENGINEERING AS AN EXPLORATION OF THE HUMAN LINK OF DIGITAL FRAUD

The main methods used by so-called "social engineers" in search of digital information, as pointed out by Hadnagy (2011), can be listed as follows: (I) *information capture:* the ability to find suitable means and places to search for information; (II) *elicitation*: ability to confuse users, that is, make them take conclusions that seem logical, but that have the real meaning hidden by the social engineer; (III) *pretense*: ability to act as if it were someone else, to interfere in the personal identity of users, that is, make yourself who you aren't; and (IV) *mental tactics (psychological)*: corresponding to the ability to develop techniques using fundamentals of psychology to condition behaviors or change users' decisions.

These methods therefore correspond, as stated by Mann (2008, p. 87-141), correspond to the act of understanding and instrumentalizing human vulnerabilities in favor of the interest in violating the security of a system - through the creation of trust in the social engineer, in subconscious intuition by commands (such as neurolinguistic programming) and the abuse of 'digital vulnerable', people such as children and elderly. Social engineering is, therefore, according to Mitnick and Simon (2002, p. 3-12), the exploitation of the weakest point of security - the human element, as individuals tend to find information useful to hackers innocuous, in addition to being limited in their ability to process data (needing to make notes or unsafe records, for example)

In the context of users of digital systems, according to Abladi and Weir (2018, p. 4-6), it's possible to identify a framework of user vulnerabilities based on: (I) *behavior*: where virtual engagement can indicate adherence to scams; (II) *perception*: users who (do not) perceive the risks of their behavior; (III) *socio-psychological elements*: personality traits that social engineers identify as most susceptible; and (IV) *socio-emotional elements*: conditions that make people more vulnerable at specific moments.

The authors Long et al. (2008) describe three practical applications of information *capture* methods: (I) *dumpster diving*: which consists, literally, in the practice of looking for disposal or garbage, documents that contain sensitive data and can facilitate access to systems; (II) *tailgating*: ability to physically infiltrate protected locations simply by joining a group of authorized persons; e (III) *shoulder surfing*: practice of observing "over the shoulder" the use of an authorized person. Therefore, social engineering consists of '*hacker no tech*' practices, that is, the most simple or complex that help to access digital systems, in addition to or before the technical aspects.

This tendency to identify the human link as a weak point in the security of systems is what Heartfield and Loukas (2015, p. 1-4) point out as a "semantic attack", technological or not, promoting elicitation, that is, making people think they are accessing something they aren't — thus getting user data in a way that people don't even feel harmed. It's like the practice of promoting websites that look like a reliable service to the user, but aren't. For example, they can be sites that direct access to a fake e-mail account that looks like the real account, causing confusion justified by the user, that is, pretending to be something real, and confusing the user to reach conclusions that only appear to be logical.

The apparent logic of these scams also contemplates the "internal danger", that is, the one that is revealed when the vulnerability in relation to the data is close and within the same environment, as in corporate structures, where security focuses on external dangers and does not recognize the risks of internal communications (and, apparently, harmless) between internal users that can reveal weaknesses regarding passwords or accesses that challenge the integrity of digitally secured data (XIANGYU; QIUYANG; CHANDEL, 2017, p. 32-33).

The *intention* is the practice of being another person, that is, using another identity in the digital context or not, adopting the history, profile and personality of another, with a view to a specific interest, that is, to be the person who give greater conditions for access to some data. It's the staging, acting in a role to achieve a goal (HADNAGY, 2011, p. 111). The claim can be made digitally (e-mail, social networks, etc.), by phone and even by presenting a false identity document - passing the agent through a trusted person to achieve a specific objective. In this scenario, the social engineer creates a context to influence victims to reveal sensitive information by understanding that they are talking to someone reliable (WORKMAN, 2007, p. 664).

The intention allows the person to request information to which only another person has access, or without the consequences of the social engineer himself in accessing it. Pretending to be someone else is an essential tool for social engineering, either in technological and digital practices, as well as in non-technological methods used as aids in accessing systems. The intrusion using the identity of another may not be perceived as an intrusion, precisely because the identity used has the access requirements and the goals of the social engineer aren't expected. Also, it can serve for a social engineering attack that makes people in an organization or a private individual take actions that are foreign to their will, being influenced by someone they think is real (TETRI; VUORINEN, 2013, p. 1015).

For Hadnagy (2011, p. 139-186) the *mental tactics* concern the search, by social engineers, for their interests, analyzing micro personal expressions and suggesting behaviors through neurolinguistic programming. An example is the notion of rapport as a technique for gaining trust from others and showing confidence, suggesting to other people's minds that the social engineer is trustworthy, thereby reducing people's defenses ("lowering their guard") in relation to the security of your privacy. It's the use of a deep understanding of the ways of thinking (patterns) and the senses - there are those who, for the most part, think through what they see or hear or through their emotions -, and the social engineer being attentive to these behaviors and managing to foresee possible decision-making when knowing what people close to, the user have aversion or appreciation for.

Neurolinguistic programming (NLP) is a field of study of personalities and behavioral patterns, being the basis for social engineers to apply data acquisition techniques through effective communication procedures applied to subjective human experience (BERGER, 1999, p. 139-141). It's the ability to learn the 'physical representations of brain activities' and of the unconscious, seeking to predict decisions and impose commands for future acts - in other words, making subconscious suggestions to behavior (MANN, 2008, p. 115-126). While it's a behavioral analysis, it also becomes a behavioral suggestion.

The mental tactics of social engineering subject users to a specific type of victimization to fraud, in which susceptibility ends up simplifying vulnerable psychological categories, when, in fact, victimization in these processes occurs in a complex and often casual process (NORRIS; BROOKES; DOWELL, 2019, p. 242). Therefore, the use of mental tactics derived from the knowledge of psychology doesn't have the ability to point out groups of people who are especially vulnerable, but to recognize emotional or psychosocial vulnerabilities in specific cases.

2 PHISHING AND CRIMINALIZATION OF THE DIGITAL SCAM

An application of these social engineering methods is the practice of phishing, which is an attack on the user, causing the user to deliver personal and financial data to the social engineers, confusing him when making him access a link/website that he believes to be reliable, or respond to a message that at first appears legitimate (CHAUDHRY; CHAUDHRY; RITTENHOUSE, 2016, p. 247). The most applied form of this coup is made "attentive to the context", that is, according to Jagatic et al. (2005, p. 1), the social engineer gains the victim's confidence by knowing his environment and habits, becoming apparently legitimate - the social engineer knows part of the user's data, which he obtained through social engineering techniques, and the scam is effectively accomplished at the moment when the fraudster obtains the missing data, possibly linked to equity gain.

A practical example of what phishing is for the internet user is, as the computer security company Avast (2020) defines, simplifying the theme to its consequences for users: "it's a dishonest way that cybercriminals use to trick you into revealing personal information, such as passwords or credit cards, CPF and bank account numbers. They do this by sending fake emails or directing the user to fake websites" (our translation into english). The detail for the criminalization of this conduct is the objective of these practices, which can be differentiated in: crimes against the person (related to honor), and crimes against the patrimony (in which the data obtained illegally are used to obtain economic gain). The first ones, in the Brazilian penal system, were typified in Law nº 12.737/2012, but the assets are considered, mainly, as inserted in the criminal type of the fraud.

The emergence of digital crimes, which wouldn't exist without the relevance that digital systems have taken on the lives of people and companies/organizations, made a re-reading of Criminal Law necessary. And the use of the internet as a means to practice these acts gives rise to the so-called "cybercrimes" or "cyber crimes", defined, to Acha (2018, p. 8), as being "any typical, anti-legal and culpable actions committed against or through the use of automatic data processing or its transmission in which the internet is the main object or instrument of the crime" (our translation into english). However, there is an adequate distinction in these crimes, according to Fiorillo and Conte (2016, p. 139-145): there are those crimes that are 'computer crimes themselves' (or pure), practiced completely within a digital system, such as hacking and malware; and 'improper computer crimes', linked to the relation between digital and non-digital, such as digital fraud.

The social engineering used by phishing is included in the second category, of improper crime, as it encompasses the digital sphere, but goes beyond this sphere in terms of the act and the object of the crime. The definition of digital fraud is the most appropriate because it contemplates the notion of social engineering related to methods of capturing, eliciting, pretending and mental tactics, seeking objectives or having their means linked to digital data, that is, the local or non-local of the internet and digitized systems.[4] Therefore, this is the 'interpretation scenario' of an existing crime in criminal law, the crime of fraud (*estelionato*) in art. 171 of the Brazilian Penal Code.

The "digital" adjective to the crime of fraud is, therefore, an act of interpretation of the criminal law, understanding that: the advantage and prejudice of this offense are obtained through digital tools, and have as a legal asset/good the digital data related to privacy. The criminalization of this conduct, therefore, is characterized in the doctrinal environment and has effects on the jurisprudence (FREITAS, 2009, p. 64), despite the will of many that the penal

[4] The thesis of Fernando José da Costa (2011, p. 149-158) presents the *place of the crime*: for the purposes of criminal prosecution, it must follow the place of the criminal conduct, but respecting the case of the crime only being considered in the *place of the crime result*. Thus maintaining a criterion of competence, even recognizing the virtual space without borders.

legislation is adapted and provides specific conducts for the digital environment, in view of a need for criminal classification.[5]

The Law nº 12.737/2012 introduced into the legal system the classification of so-called 'pure computer crimes', in the crime of "computer device invasion" (art. 154-A of the Brazilian Penal Code): Invade someone else›s computer device, connected or not to the computer network, by undue violation of the security mechanism and in order to obtain, tamper with or destroy data [...]" (our translation into english), that is, it contemplates the legal good of individual freedom, privacy and intimacy in the digital environment. This 'breached computer device' can be any device capable of storing personal data, such as computers, tablets or cell phones, that are protected by passwords or another protection mechanism, and the intruder being a willful active person who circumvents the security system in the name of the breach of data privacy (KUNRATH, 2017, p. 68).

There is, however, a difference between the practices typified under Law nº 12.737 and that of the digital fraud (untyped); precisely because the behaviors typified in this law are related to crimes against persons, and untyped behavior is a property crime, not concerning honor. The digital fraud through phishing is intended to capture personal and financial data of users (victims of the scam) for economic purposes (COSTA, 2011, p. 99-100). Thus, in analogy to what Wendt's research presents (2016, p. 154-159), due to the expansion of risks and uncertainties promoted by internet communication, the intention to criminalize the act in Criminal Law will not reach the complexity of the practice. It's necessary to contemplate objective criteria for the application of the Law, fleeing the trend brought about by the expansion of the risk of expanding criminal law - forcing society to seek non-penal alternatives.[6] This is the case of fraud, which under the digital context maintains the need to protect the same legal asset, regardless of new means, from the point of view of criminalization, but exposing the need for educational and social forms of defense and resistance to new frauds/scams.

3 DATA PROTECTION AND DIGITAL CITIZENSHIP BY SOCIAL MEDIA OF DEFENSE

Among the challenges, 'to prevent cybercrime', it is necessary to face the distinction between criminal policies and innovative preventive policies, that is, between the formal criminalization of the typification of acts and the rise of policies such as: (I) digital security policies, (II) 'informational education policies' and ethics on the internet, (III) conflict resolution policies in virtual relations, according to Kunrath (2017, p. 72-146). This non-penal paradigm respects the tendency to search for alternatives to combat cybercrime at the international

[5] Art. 5º, XXXIX of the Brazilian Constitution/1988: there is no crime without a previous law that defines it, nor a penalty without prior legal agreement (Our translation into english) ("não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal").

[6] As Wendt states (2016, p. 165): "If Criminal Law has the same function as thorns in relation to flowers, supposedly to protect society, both thorn and Criminal Law are doomed to failure, because the ax of contemporary times is overwhelming and the cuts and wounds generated will not heal with more axes. It's necessary to rethink the normative-penal criterion as a way to solve social issues that are possible to be solved through behavioral, administrative or technical practices, or, perhaps, by other branches of Law other than Criminal". (Our translation into english)

level, more linked to information security than to criminal prosecution (SILVA, 2012, p. 103-104).

The simulation promoted by the study by Konradt, Schilling and Werners (2016, p. 10) indicates that in the context of the current digitalization of society, the professionalization of the analysis of the so-called "cybercrimes" has been promoted, making necessary to address the economic sources and the fruits arising from these techniques that use social engineering, considering that social engineers work under a multiplicity of risks and under the "trial and error", being more important to combat them protect privacy from the data that the punishment of these conducts with a new criminal type and a 'new arm' of the penal system.

The rise of a digital security policy contemplates that proposed in the '*Marco Civil da Internet*' (Law nº 12.965/2014) as principles and guarantees of internet use in Brazil, as respect for freedom of expression and human rights (art. 2) and the principle of protection of privacy and personal data. The guarantees (art. 7) are of the inviolability of intimacy and personal communication via the internet, the only alternative for providing personal data to third parties is free, express and informed consent. Also, it's the duty of the Public Power (Union, States and Municipalities) to develop the internet and a participatory and collaborative internet management structure, promoting digital inclusion and a digital culture (art. 27).

Digital inclusion and internet culture are directly linked to data protection, which is why it's instrumentalized in the 'General Law for the Protection of Personal Data' (*Lei Geral de Proteção de Dados Pessoais - LGPD*) (Law nº 13.709/2018), in force established for 2020, which provides for this aspect of the treatment of personal data and is disciplined by respect for privacy and informational self-determination (art. 2º, I and II), thus being a tool also with the aim of fostering a culture of data protection, for individuals and companies. In these aspects, the 'innovative policies of informational education' and 'ethics on the internet' can be understood as: a public defense tool against cybercrimes.

Digital inclusion, therefore, is the promotion of citizenship that recognizes the dimension of virtual space and recognizes digital security as something fundamental for insertion in the information society (MARTINI, 2005). Informational education, which empowers citizens in the digital sphere, is also associated with their under-sufficient position in consumer relations, recognizing the technical inequality that consumers have in relation to the extensive databases of retail companies, for example (MIRAGEM, 2019, p. 27-28). Therefore, digital citizenship presupposes the technical empowerment of the citizen, while recognizing the technological asymmetries of the social structure.

Also, from the companies point of view, the idea of information security policies and compliance is considered, paying attention to the principle of privacy and preservation of digital data, that is, corporate policies that establish administrative guidelines and standards for information security. The possible legacy for these regulatory frameworks, especially the *LGPD (Lei Geral de Proteção de Dados Pessoais)*, according to Bioni (2019, p. 32-33), is the strengthening of a data protection culture for organizations, taking into account important factors such as reputation and trust in the corporate environment. Also, that there is a regulatory culture in favor of the interpretation and systematic application of this protection in all technological development (DONEDA; MENDES, 2019, p. 322).

The mitigation of the risks brought by the techniques associated with social engineering, must go through the identification of the aggressors with these so-called ‘user weaknesses’, that is, the human part in digital systems. As Towsend notes (2019), Avast, when reporting the factors to be observed for social engineers to take advantage of users: time pressure (forcing the user to make immediate decisions), fear of loss, wrong direction, false assessments, false identity and partial information.

Phishing has broadened its context beyond digital fraud, and the act of ‘phishing for phools’, or “fishing for fools”, as stated by Akerlof and Shiller (2015, p. 10) covers the areas of commercial advertising and politics, in which consumer and electoral markets use data from internet users to interfere in their perceptions, acquiring them legally - even though these markets are adept at practices that hide the real reason for capturing information.

Education and collective awareness can contribute to collaborative ways of combating techniques such as phishing, and it's necessary to develop educational ways to create resistant and resilient defensive behavior against these attacks: they can be through games[7], they can be through games, booklets or newsletters that expose how users' data may or may not be used and how this use is legal, preventing or at least reducing user confusion when delivering personal data on digital platforms.

Thus, working with technological education - strengthening the human link (TAYOURI, 2015, p. 1096) -, as the study by Nicholson, Coventry and Briggs points out (2017, p. 292) understanding the importance of using social media, not just technological ones, to defend against attacks by social engineers - as well as paying attention to the data of the attacker, in cases of phishing.

For the corporate environment, an alternative is the individual empowerment of employees, forming resistant and resilient users to social engineering attacks, such as identity theft and ransomware. The recommendations made by the study by Thomas (2018, p. 17) are aimed at recognizing the different groups of users within a corporate network in view of the impact of their work, familiarity with phishing and levels of trust (in believing they are not susceptible to scams), improving specific vulnerabilities, empowering employees to behave in an active way that knows the risks and the forms of defense for each act performed in relation to digital data.

This is only possible through organizational policies appropriate to effective data security with participatory forms, which educate employees, and privacy protection practices in company activities — the *LGPD* legally represents this evolution in the organizational sector, whether in public governance or in private corporations, based on the foundation of accountability or corporate responsibility. Thus, it emerges: the need for organizations to comply with the law (compliance), maintaining in their practices the principle of informative self--determination, informed consent and the protection of personal data - empowering the institutions responsible for investigations and internal liability/responsibility in companies with a view to those principles. One of these practices is the so-called ‘private certification of compliance with data protection principles’.

[7] The text of the authors Arachchilage, Love and Beznosov (2016) shows interesting results on the education of users in a digital game that indicates anti-phishing tools.

The establishment of internal controls aims to reinforce state regulation, law enforcement, in the case of data protection, as described by Frazão, Oliva and Abilia (2019, p. 693-711), need to be adapted to the risk of activity, to the creation of a training program for employees about data security, to the regulation by design and effective monitoring of the compliance program itself. One of the direct consequences of this scenario is the creation of the data protection officer (RECIO, 2017), professional or sector responsible for data protection within a company, which aims to align business activity with the legal precepts about privacy and information security , making companies and people less vulnerable to scams classifiable as digital fraud/scams.

There remains, the social role given to technology companies, which manage the algorithms and digital systems used in all these operations (personal or business). It's what is called regulation by design, in which the creators of the algorithms are responsible for verifying the protection of fundamental rights, especially privacy, in the order of their systems, being systematically incorporated. That is, according to Magrani (2019), Law being used as metatechnology, that is, software engineering starts to consider fundamental rights and human rights, in this case the right to data security, in the sphere of technological production. It's the algorithmic accountability, in which the social responsibility of the developer is required (KITCHIN, 2017, p. 26-27).

It's a process that combines the self-regulation of these transnational (FORNASIER; FERREIRA, 2015, p. 409) technology companies with the need for social auditability, and the programming must be subjected to critical analysis by society, as well as caring for the legal principles that guide human rights, including the principle of informative self-determination. At the same time as there is a privatization of regulation, there must also be the privatization of responsibilities, such is the importance of algorithms guided by large technology companies (MARTIN, 2019). Programming needs to take into account the need to create spaces with democratic and social values, bringing the best of the objectives of the laws into the algorithms (WEBER, 2018, p. 705-706).

The disruptive characteristic of new technologies and their algorithms can allow for safer systems and empower users, making them more capable of resisting digital scams, and the Law should behave properly, not regressing to the positivism of the criminal typification of the conduct of the digital fraud or digital scam, but incorporating principles appropriate to the core of programming - creating a flexible law capable of dealing with technologies, making the relations between software engineering and law as something hybrid (SANTOS; MARCO; MOLLER, 2019, p. 3079-3081).

CONCLUSION

The defense against attacks and the protection of personal data in the face of social engineering and its most evident practice (phishing) doesn't go beyond the simple development of an invulnerable system, as this practice doesn't use digital tools or complex technologies. These practices depend on the exploration of human openings and weaknesses in social relations in relation to privacy. Phishing depends on a complexity of factors and feeds on them - its combat must be proportional, and it needs an adequate digital education, which contemplates a digital citizenship aware of everything that is shared in the networks and its consequences, restricting the holes in which a social engineer can take over the personal data of internet users.

This conclusion was possible after describing the phenomenon called: social engineering, understood as a set of methods that condition a series of practices, legal and illegal, technological and non-technological. In this case, phishing is a scam that uses social engineering practices to capture information, elicitation, pretentiousness and mental tactics to apply fraud in order to realize an economic advantage. It's a complex concept precisely because of its association between technological factors and practices that aren't related to technical complexity. In other words, the social engineer, even applying the fraud on digital systems, doesn't need to be a computer expert, a hacker - even for this reason they are considered 'improper digital crimes'.

The criminalization of digital fraud involves clarifying this practice, avoiding being dazzled by computer and digital issues, realizing that, often, the digital environment is simple and is associated with non-technological techniques for obtaining data. Thus, this practice differs from the crimes against the person typified by Law 12.735 / 2012, as there is no complex adulteration of a digital system for the protection of personal data, but the use of social techniques to trick victims into delivering data that subject their assets to misappropriation. Phishing uses new information and communication technologies as a means of applying these frauds, but its techniques are purely social.

The prevention of these practices is, therefore, much more accomplished through informational education and a culture of data protection, and the empowerment of the digital citizen, than through the criminalization of computer behavior.

Trying not to fall into the temptation of criminalization (criminal typification), responding to the problem proposed by this research: creative, innovative and socially more suitable alternatives for data protection and cybercrime prevention emerge, and in this article we list or divide these responses into three groups: (I) in informational education and the empowerment of digital citizenship; (II) in the organizational culture of data protection through corporate policies or compliance; and (III) self-regulation or regulation by design of the technology companies themselves, basing their algorithms on privacy and human rights principles.

And it should be noted that the development of preventive policies, in addition to mere criminal repression through new types, doesn't come here to mean the 'responsibility of the victim for the criminal's conduct', but, rather, 'to make the Public Power and the technology ', calling, in relation to such entities, for preventive and proactive attitudes against such practices. In other words: such entities and institutions must abandon the repression posture through legislation as being useful and necessary in itself.

These social means of prevention are the alternative solutions to the penal system, which seek more a culture of promoting digital citizenship and empowering users based on the notion of privacy and resilience to scams, than the criminalization/typification of conduct, with a view to that the specific and careful classification of the criminal type of digital fraud has more to do with the good functioning of criminal dogmatics, than with the effective protection of personal data. Anyway and thus, the proposed triad of alternatives – one for individuals, another for legal entities and, also, for those institutions/organizations that have instructed the functioning of digital systems – has in view the implementation of the principles of informational self-determination and digital inclusion.

REFERENCES

ACHA, Fernanda Rosa. Digital crimes: a necessary re-reading of criminal law in the light of new technologies. VII Seminar and IV Interdisciplinary Congress on Law and Medicine Palliative Care. August 20-22, 2018 (Crimes digitais: uma necessária releitura do Direito Penal à luz das novas tecnologias. *VII Seminário* e IV *Congresso Interdisciplinar Direito e Medicina Cuidados paliativos*, 20 a 22 de agosto de 2018). Itaperuna. Available in: http://revista.srvroot.com/linkscienceplace/index.php/linkscienceplace/article/view/621/347. Accessed on: January 13, 2020.

AKERLOF, George A.; SHILLER, Robert J. *Phishing for phools***:** the economics of manipulation and deception. Princeton: Princeton University Press, 2015.

ARACHCHILAGE, Nalin Asanka Gamagedara; LOVE, Steve; BEZNOSOV, Konstantin. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, v. 60, p. 185-197, 2016. DOI: 10.1016/j.chb.2016.02.065.

AVAST. The essential phishing guide: How it works and how to protect yourself (*O guia essencial sobre phishing***:** Como funciona e como se proteger). Available in: https://www.avast.com/pt-br/c-phishing. Accessed on: January 14, 2020.

BERGER, Leoni. Study of the use of transactional analysis techniques and neurolinguistic programming to improve personal and organizational communication. Dissertation (Master in Production Engineering) (*Estudo do emprego de técnicas da análise transacional e da programação neurolinguística na melhoria da comunicação pessoal e organizacional***.** Dissertação (mestrado em Engenharia de Produção)). 1999. Federal University of Santa Catarina. Available in: https://repositorio.ufsc.br/bitstream/handle/123456789/80569/139040.pdf?sequence=1. Accessed on: January 11, 2020.

BIONI, Bruno Ricardo. Innovate by Law (Inovar pela Lei). *Gv/Executivo*, v. 18, n. 4, p. 31-33, Jul./Aug. 2019. Available in: http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/download/79978/76432. Accessed on: January 20, 2020.

BRASIL. Federal Constitution of 1988 (*Constituição Federal de 1988*). Available in: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Accessed on: January 13, 2020.

BRASIL. Decree-Law Nº 2.848, of December 7, 1940. Penal Code (*Decreto-Lei nº 2.848, de 7 de dezembro de 1940.* Código Penal. Available in: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Accessed on: January 13, 2020.

BRASIL. Law Nº 13.709, of August 14, 2018. General law for the protection of personal data (*Lei 13.709, de 14 de agosto de 2018*. Lei geral de proteção de dados pessoais (LGPD)). Available in: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Accessed on: January 13, 2020.

BRASIL. Law Nº 12.965, of April 23, 2014. Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil (*Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil). Available in: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: January 13, 2020.

CHAUDHRY, Junaid Ahsenali; CHAUDHRY, Shafique Ahmad; RITTENHOUSE, Robert G. Phishing attacks and defenses. *International Journal of Security and Its Applications*, v. 10, n. 1, p. 247-256, 2016. DOI: 10.14257/ijsia.2016.10.1.23.

COSTA, Fernando José da. Locus Delicti in computer crimes (*Locus Delicti nos crimes informáticos*). Thesis (Doctorate in Law). Faculty of Law of the University of São Paulo. 2011. Available in: https://www.teses.usp.br/teses/

disponiveis/2/2136/tde-24042012-112445/publico/Fernando_Jose_da_Costa.pdf. Accessed on: January 14, 2019.

DONEDA, Danilo; MENDES, Laura Schertel. A profile of the new Brazilian General Data Protection Law (Um perfil da nova Lei Geral de Proteção de Dados brasileira). In: BELLI, Luca; CAVALLI, Olga. Government and 'Internet regulations in Latin America': analysis of infrastructure, privacy, cybersecurity and technological developments in honor of the ten years of South School on Internet Governance (*Governo e regulações da Internet na América Latina*: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance). Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2019, p. 309-324.

FIORILLO, Celso; CONTE, Christiany. Crimes in the digital environment and the information society (*Crimes no meio ambiente digital e a sociedade da informação*). 2 ed. São Paulo: Saraiva, 2016.

FORNASIER, Mateus de Oliveira; FERREIRA, Luciano Vaz. The regulation of transnational companies between state and non-state legal orders. International Law Review (A regulação das empresas transnacionais entre as ordens jurídicas estatais e não-estatais. *Revista de Direito Internacional*), v. 12, n. 1, 2015. DOI: http://dx.doi.org/10.5102/rdi.v12i1.3303.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIA, Vivianne da Silveira. Personal data compliance (*Compliance* de dados pessoais). *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (orgs). General law on the protection of personal data and its repercussions in Brazilian law (*Lei geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro*). São Paulo: Revista dos Tribunais, 2019.

FREITAS, Riany Alves de Freitas. Digital Security: digital fraud and security on e-commerce sites (Segurança Digital: estelionato digital e a segurança em sites de comércio eletrônico). *MPMG Jurídico*, n. 17, v. 1, p. 63-65, 2009. Available in: https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3. Accessed on: January 13, 2020.

HADNAGY, Christopher. *Social Engineering*: The Art of Human Hacking. Indianapolis: Wiley, 2011.

HEARTFIELD, Ryan; LOUKAS, George. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, v. 48, n. 3, p. 1-39, 2015. DOI: 10.1145/2835375.

JAGATIC, Tom N.; JOHNSON, Nathaniel; JAKOBSSON, Markus; MENCZER, Filippo. Social phishing. *Communications of the ACM*, v. 50, n. 10, p. 94-100, 2007. https://doi.org/10.1145/1290958.1290968.

KITCHIN, Rob. Thinking critically about and researching algorithms. *Information, communication & Society*, v. 20, n.1, p. 14-29, 2017. DOI: 10.1080/1369118X.2016.1154087.

KONRADT, Christian; SCHILLING, Andreas; WERNERS, Brigitte. Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, v. 58, p. 39-46, 2016. DOI: 10.1016/j.cose.2015.12.001.

KUNRATH, Josefa Cristina Tomaz Martins. The expansion of crime in cyberspace. Feira de Santana: State University of Feira de Santana (*A expansão da criminalidade no cyberespaço*. Feira de Santana: Universidade Estadual de Feira de Santana), 2017. Available in: http://www.uefs.br/modules/documentos/get_file.php?curent_file=3330&curent_dir=1772. Accessed on: January 14, 2019.

LONG; Johnny; PINZON, Scott; WILES, Jack; MITNICK, Kevin. *No tech hacking*: a guide to social engineering dumpster diving and shoulder surfing. Burlington: Syngress, 2008.

MAGRANI, Eduardo. Between Data and Robots: the ethics of "things": from the ethics of discourse and communicative rationality to the new materialism of socio-technical systems (*Entre Dados e Robôs*: a ética das "coisas": da ética do discurso e racionalidade comunicativa ao novo materialismo de sistemas sociotécnicos). 2 ed. Porto Alegre: Arquipélago, 2019.

MANN, Ian. *Hacking the human*: social engineering techniques and security countermeasures. Hampshire: Gower, 2008.

MARTIN, Kirsten. Ethical implications and accountability of algorithms. *Journal of Business Ethics*, v. 160, n. 4, p. 835-850, 2019. DOI: 10.1007/s10551-018-3921-3.

MARTINI, Renato. Digital inclusion and social inclusion. Social inclusion (Inclusão digital e inclusão social. *Inclusão* **social**), v.1, n. 1, 2005. Available in: http://revista.ibict.br/inclusao/article/view/1501/1685. Accessed on: January 14, 2020.

MIRAGEM, Bruno. The General Data Protection Law (Law 13,709 / 2018) and Consumer Law. Review of the Courts (A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. *Revista dos Tribunais*), v. 1009, p. 173-222, Nov. 2019.

MITNICK, Kevin D.; SIMON, William L. *The Art of Deception***:** controlling the human element of security. Indianapolis: Wiley, 2002.

NICHOLSON, James; COVENTRY, Lynne; BRIGGS, Pam. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).* Santa Clara, CA, EUA. Julho, 2017.Available in: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/nicholson. Accessed on: January 10, 2020.

NORRIS, Gareth; BROOKES, Alexandra; DOWELL, David. The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, v. 34, n. 3, p. 231-245, 2019. DOI: 10.1007/s11896-019-09334-5.

OLIVEIRA, Ana Paula de; ZANETTI, Dânton; LIMA, Flávia Santos; SAMPAIO, Themis Ortega. The Brazilian General Data Protection Law in Business Practice (A Lei Geral de Proteção de Dados Brasileira na Prática Empresarial). In: SILVA, Rafael Aggens Ferreira da (ed.). Law and Innovation - Crypto, Fintechs, Online Dispute Resolution (ODR), Data Analysis and Artificial Intelligence and the General Data Protection and Privacy Law (*Direito e Inovação - criptoativos, Fintechs, Oline Disput Resolution (ODR), Análise de Dados e Inteligência Artificial e a Lei Geral de Proteção de Dados e Privacidade*). Curitiba: OAB/PR, 2019. Available in: http://esa.sites.oabpr.org.br/wp-content/uploads/sites/7/2019/06/direito-e-inovacao-volume1.pdf. Accessed on: January 14, 2020.

RECIO, Miguel. Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability. *European Data Protection Law Review*, v. 3, n. 1, p. 114-118, 2017. DOI https://doi.org/10.21552/edpl/2017/1/18.

SANTOS, Paulo Junior Trindade dos; MARCO, Cristhian Magnus de; MÖLLER, Gabriela Samrsla. Disruptive Technology and Disruptive Law: Understanding Law in a New Technologies Scenario. Law and Praxis Magazine (Tecnologia Disruptiva e Direito Disruptivo: Compreensão do Direito em um Cenário de Novas Tecnologias. *Revista Direito e Práxis*), v. 10, n. 4, p. 3056-3091, dez. 2019. DOI: 10.1590/2179-8966/2019/45696.

SILVA, Marcelo Mesquita. International action to combat cybercrime and its influence on the Brazilian legal system (*A***ção internacional no combate ao cibercrime e sua influê***ncia no ordenamento jurídico brasileiro*). 2012. 109 p. Master's Dissertation in International Economic Law at the Catholic University of Brasilia. Brasília, 2012. Available in: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/276/1/Marcelo%20Mesquita%20Silva.pdf. Accessed on: January 13, 2019.

TAYOURI, David. The human factor in the social media security: combining education and technology to reduce social engineering risks and damages. *Procedia Manufacturing*, v. 3, p. 1096-1100, 2015. DOI: 10.1016/j.promfg.2015.07.181.

TETRI, Pekka; VUORINEN, Jukka. Dissecting social engineering. *Behaviour & Information Technology*, v. 32, n. 10, p. 1014-1023, 2013. DOI: 10.1080/0144929X.2013.763860.

THOMAS, Jason. Individual cyber security: empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*. v. 12, n. 3, p. 1-23, 2018. DOI: 10.5539/ijbm.v13n6p1.

TOWSEND, Kevin. Social engineering: it's not just about phishing scams (Engenharia social: não se trata apenas de golpes de phishing). Available in: https://blog.avast.com/pt-br/social-engineering-hacks. Accessed on: January 2, 2020.

WEBER, Rolf H. "Rose is a rose is a rose is a rose" - what about code and law? Computer Law & Security Review, v. 34, n. 4, p. 701-706, 2018. DOI: 10.1016/j.clsr.2018.05.005.

WENDT, Emerson. The internet and the fragmentation of criminal law in strengthening the culture of fear in Brazil: social perception and legislative perspective (*A internet e a fragmentação do direito penal no reforço da cultura* *do medo no Brasil:* percepção social e perspectiva legislativa). Dissertation (Master in Law) - La Salle University. Canoas, 2016. Available in: http://repositorio.unilasalle.edu.br/bitstream/11690/1029/1/ewendt.pdf. Accessed on: January 13, 2020.

WORKMAN, Michael. Wisecrackers: A theory grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology,* v. 59, n. 4, p. 662-674, 2007. DOI: 10.1002/asi.20779.

XIANGYU, Liu; QIUYANG, Li; CHANDEL, Sonali. Social engineering and insider threats. *In*: *2017 International Conference on Cyber-Enabled Distributed and Knowledge Discovery (CyberC),* p. 25-34, 2017. DOI: 10.1109/CyberC.2017.91.

Recebido/*Received: 26.03.2020.*

Aprovado/*Approved: 27.05.2020.*