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

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

MATEUS DE OLIVEIRA FORNASIER[1]
NORBERTO MILTON PAIVA KNEBEL[2]
FERNANDA VIERO DA SILVA[3]

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 empo-

1 Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). Doutor em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS, Brasil), com Pós-Doutorado em Direito pela University of Westminster (Reino Unido). http://orcid.org/0000-0002-1617-4270. http://lattes.cnpq.br/3316861562386174. mateus.fornasier@gmail.com.

2 Doutorando do Programa de Pós-Graduação Stricto Sensu em Direitos Humanos da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). http://orcid.org/0000-0003-0674-8872. http://lattes.cnpq.br/4232557221807840. norberto.knebel@gmail.com.

3 Bolsista de Iniciação Científica (PIBIC/CAPES). Acadêmica do Curso de Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI). http://orcid.org/0000-0002-3978-7395. http://lattes.cnpq.br/3060049367537210. fefeviero@gmail.com.
Agência de fomento: Fundação de Amparo à Pesquisa do Estado do 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 e engenharia social: entre a criminalização e a utilização de meios sociais de proteção.* Revista Meritum, Belo Horizonte, vol. 15, n. 1, p. 116-129, jan./abr. 2020. DOI: https://doi.org/10.46560/meritum.v15i1.7771.

deramento 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.

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 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.*

INTRODUÇÃO

A ascensão das relações digitais e a ubiquidade dos sistemas virtuais para promover o comércio, a atividade bancária e as redes sociais têm colocado os chamados "cibercrimes" em questão, tendo por consequência uma multiplicidade de soluções propostas. A engenharia social possui um impacto na vida das pessoas e nas atividades das empresas, atingindo a privacidade e a segurança de dados — sendo que a vulnerabilidade dos sistemas de gestão de informação não estão nos aspectos técnicos, mas sim nas relações humanas.

A crescente sofisticação teórica acerca desses crimes digitais permite ampliar as discussões até mesmo para fora do âmbito da dogmática penal, interligando contextos políticos e sociais à necessidade de resistir e proteger os cidadãos das fraudes que se utilizam da engenharia social para obter vantagem patrimonial. Nesse sentido, o *phishing* une práticas tecnológicas e não tecnológicas da engenharia social para enganar usuários na internet, dando a entender que ocorre por uma decisão lógica e coerente do usuário — porém, se revela como a entrega de dados importantes para a obtenção do objetivo econômico do estelionatário. Esse bem jurídico (patrimônio) já é protegido contra fraudes pelo crime de estelionato; todavia, não há uma tipificação específica para quando utiliza meios digitais — por isso a nomenclatura "estelionato digital".

REVISTA MERITUM • v.15 • n.1 • p. P. 116-129 • Jan./Abr. 2020

O problema que provocou esta pesquisa pode assim ser descrito: de que forma o ordenamento jurídico brasileiro trata (e deve tratar) dos aspectos penais dos crimes digitais contra o patrimônio? Apresenta-se como hipótese, para esse questionamento, 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 da criança e do adolescente, por exemplo; mas os crimes patrimoniais digitais ainda não foram tipificados — contudo, duvida-se da necessidade dessa criminalização específica frente à importância social maior que teriam soluções criativas e alternativas, baseadas em políticas de prevenção ao *phishing* e às vulnerabilidades expostas a estratégias de engenharia social.

O objetivo geral deste artigo é realizar um estudo acerca da necessidade de tipificação criminal para alcançar os engenheiros sociais que aplicam golpes no âmbito digital com os meios sociais de proteção, que vão das práticas individuais às das grandes corporações, passando pela obrigação do Poder Público em promover a cidadania digital. Para a consecução desse objetivo geral, dividiu-se o seu desenvolvimento em três seções. A primeira delas se destina a estudar as práticas da engenharia social e suas consequências para o cidadão e as empresas. Já a segunda é dedicada a compreender o processo de criminalização de certas práticas digitais, focando-se principalmente na necessidade de criminalização do estelionato digital. Por fim, a terceira parte observa formas não penais de prevenção ao *phishing*.

Metodologicamente, elenca-se que esta pesquisa, de natureza acadêmica, se valeu do método de procedimento hipotético-dedutivo, com método de abordagem qualitativo e técnica de pesquisa bibliográfico-documental. Nesse sentido, o trabalho inicia com a localização da prática do *phishing* dentro de estratégias de engenharia social. Passa, logo após, à realização de um estudo jurídico-dogmático a fim de identificar se tal prática é tipificada penalmente no Brasil. Por fim, é 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 do *phishing* seriam mais eficientes do que a tipificação penal.

1 ENGENHARIA SOCIAL COMO EXPLORAÇÃO DO ELO HUMANO DAS FRAUDES DIGITAIS

Os principais métodos utilizados pelos chamados "engenheiros sociais" em busca de informações digitais, conforme aponta Hadnagy (2011), podem ser assim elencados: (I) *captação* de informações*:* a capacidade de achar meios e locais adequados de busca por informações; (II) *elicitação*: habilidade de confundir os usuários, ou seja, que eles tomem conclusões que parecem lógicas, mas que tem o sentido real ocultado pelo engenheiro social; (III) *pretensão*: aptidão de agir como se fosse outro, de interferir na identidade pessoal dos usuários, ou seja, em fazer-se ser quem não se é; e (IV) *táticas mentais (psicológicas)*: correspondentes à capacidade de desenvolver técnicas com uso de fundamentos da psicologia para condicionar comportamentos ou alterar decisões dos usuários.

Esses métodos, portanto, correspondem, também como afirma Mann (2008, p. 87-141), ao ato de compreender e instrumentalizar as vulnerabilidades humanas em prol do interesse em violar a segurança de um sistema — por meio da criação da confiança no engenheiro

social, na intuição subconsciente por comandos (como a programação neurolinguística) e o abuso de vulneráveis digitais, como crianças e idosos. A engenharia social é, portanto, conforme Mitnick e Simon (2002, p. 3-12), a exploração do ponto mais fraco da segurança — o elemento humano, pois os indivíduos tendem a considerar inócuas informações úteis para os *hackers*, além de serem limitados na sua capacidade de processar dados (precisando fazer anotações ou registros não seguros, por exemplo).

No contexto dos usuários dos sistemas digitais, segundo Abladi e Weir (2018, p. 4-6), é possível identificar um quadro (*framework*) de vulnerabilidades de usuários baseadas em: (I) *comportamento*: em que o engajamento virtual pode indicar a adesão aos golpes; (II) *percepção*: usuários que (não) percebem os riscos de seu comportamento; (III) *elementos sócio-psicológicos*: traços de personalidades que os engenheiros sociais identificam como mais suscetíveis; (IV) *elementos sócio-emocionais*: condições que tornam as pessoas mais vulneráveis em momentos específicos.

Long et al. (2008) descrevem três aplicações práticas dos métodos de *captação* de informação: (I) *dumpster diving*: que consiste, literalmente, na prática de procurar no descarte ou lixo, documentos que contenham dados sensíveis e possam facilitar o acesso aos sistemas; (II) *tailgating*: habilidade de infiltração física em locais protegidos simplesmente ao se incorporar a um grupo de pessoas autorizadas; e (III) *shoulder surfing*: prática de observar "por cima do ombro" o uso de uma pessoa autorizada. Portanto, a engenharia social consiste em práticas *hacker no tech*, ou seja, das mais simples ou complexas que ajudem a acessar sistemas digitais, para além ou antes dos aspectos técnicos.

Essa tendência de identificar o elo humano como ponto frágil da segurança dos sistemas é o que Heartfield e Loukas (2015, p. 1-4) apontam como "ataque semântico", tecnológicos ou não, promovendo a *elicitação*, ou seja, fazer com que as pessoas pensem que estão acessando algo que não estão — obtendo assim dados dos usuários de uma maneira pela qual as pessoas sequer se sintam prejudicadas. É como a prática de promover sites que parecem de um serviço confiável ao usuário, mas não o são. Por exemplo, podem ser sites que direcionam para o acesso a uma falsa conta de e-mail com aparência da real, causando uma confusão justificada pelo usuário, ou seja, fazendo-se passar por algo real e confundindo o usuário a chegar a conclusões que apenas aparentam ser lógicas.

A aparente lógica desses golpes contempla também o "perigo interno", ou seja, aquele que se revela quando a vulnerabilidade em relação ao dados é próxima e dentro de um mesmo ambiente, como nas estruturas corporativas, onde a segurança foca nos perigos externos e não reconhece os riscos das comunicações internas e, aparentemente, inofensivas entre os usuários internos que podem revelar fragilidades quanto a senhas ou acessos que desafiam a integridade dos dados assegurados digitalmente (XIANGYU; QIUYANG; CHANDEL, 2017, p. 32-33).

A *pretensão* é a prática de ser outra pessoa, ou seja, se utilizar de outra identidade no contexto digital ou não, adotar a história, o perfil e a personalidade de outro, tendo em vista um interesse específico, ou seja, ser a pessoa que dê maior condições para acesso a algum dado. É a encenação, atuação de um papel para alcançar um objetivo (HADNAGY, 2011, p. 111). A pretensão pode ser feita por via digital (e-mail, redes sociais, etc.), por telefone e até mesmo mediante a apresentação de documento de identidade falso — passando o agente por pessoa confiável para a consecução de um objetivo específico. Nesse cenário o enge-

REVISTA MERITUM • v.15 • n.1 • p. P. 116-129 • Jan./Abr. 2020

nheiro social cria um contexto para influenciar as vítimas a revelar informações sensíveis por entender estar falando com alguém confiável (WORKMAN, 2007, p. 664).

A pretensão permite que a pessoa requisite informações às quais somente outra pessoa tem acesso, ou sem as consequências do próprio engenheiro social as acessar. Fingir ser outra pessoa é uma ferramenta essencial para a engenharia social, tanto nas práticas tecnológicas e digitais, como nos métodos não tecnológicos utilizados como auxiliares no acesso a sistemas. A intrusão utilizando a identidade de outro pode não ser percebida como intrusão, justamente porque a identidade utilizada possui os requisitos de acesso e não se espera os objetivos do engenheiro social. Também, pode servir para um ataque de engenharia social que faça as pessoas de uma organização ou um particular tomarem atitudes alheias às suas vontades, sendo influenciadas por alguém que pensam ser real (TETRI; VUORINEN, 2013, p. 1015).

Para Hadnagy (2011, p. 139-186) as *táticas mentais* dizem respeito à busca, pelos engenheiros sociais, pelos seus interesses, analisando as micro expressões pessoais e sugerindo comportamentos pela programação neurolinguística. Um exemplo é a noção de *rapport* como técnica para ganhar confiança dos outros e demonstrar confiança, sugerindo à mente de outras pessoas que o engenheiro social é confiável, minando-se assim as defesas ("baixando a guarda") das pessoas em relação à segurança de sua privacidade. Trata-se do uso de uma profunda compreensão dos modos de pensar (padrões) e dos sentidos — há quem, majoritariamente, pense por meio do que vê, ouve ou pelas suas emoções —, sendo o engenheiro social atento a esses comportamentos e conseguindo antever possíveis tomadas de decisões ao saber a que as pessoas próximas têm aversão ou apreço.

A programação neurolinguística (NLP) é um campo de estudos das personalidades e dos padrões de comportamento, sendo base para os engenheiros sociais aplicarem técnicas de obtenção de dados por meio de procedimentos eficazes de comunicação aplicadas à experiência humana subjetiva (BERGER, 1999, p. 139-141). É a capacidade de aprender as representações físicas das atividades cerebrais e do inconsciente, buscando prever decisões e impor comandos para atos futuros — em outras palavras, realizar sugestões subconscientes ao comportamento (MANN, 2008, p. 115-126). Ao mesmo tempo que é análise comportamental, se transforma também em sugestão comportamental.

As táticas mentais da engenharia social sujeitam os usuários a um tipo específico de vitimização a fraudes, em que a suscetibilidade acaba simplificando categorias psicológicas vulneráveis, quando, na verdade, a vitimização nesses processos se dá em um processo complexo e muitas vezes casual (NORRIS; BROOKES; DOWELL, 2019, p. 242). Portanto, o uso de táticas mentais oriundas do conhecimento da psicologia não tem o condão de apontar grupos de pessoas especialmente vulneráveis, mas de reconhecer vulnerabilidades emocionais ou psicossociais em casos específicos.

2 PHISHING E CRIMINALIZAÇÃO DO ESTELIONATO DIGITAL

Uma aplicação desses métodos de engenharia social é a prática do *phishing*, que é um ataque ao usuário, fazendo com que este entregue dados pessoais e financeiros aos engenheiros sociais, confundindo-o ao fazê-lo acessar um *link*/site que creia ser confiável, ou estar respondendo a alguma mensagem que a princípio aparenta legitimidade (CHAUDHRY; CHAUDHRY; RITTENHOUSE, 2016, p. 247). A forma mais aplicada desse golpe é feita "atenta ao contexto", ou seja, conforme Jagatic et al. (2005, p. 1), o engenheiro social ganha a confiança da vítima ao conhecer seu ambiente e seus hábitos, tornando-se aparentemente legítimo — o engenheiro social conhece parte dos dados do usuário, que obteve pelas técnicas da engenharia social, sendo dado o golpe efetivamente no momento em que o estelionatário obtém o dado que faltava, possivelmente ligado a ganho patrimonial.

Um exemplo prático do que é *phishing* para o usuário da internet é como define a empresa de segurança informática Avast (2020), simplificando o tema a suas consequências para os usuários: "é uma maneira desonesta que cibercriminosos usam para enganar você para revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando para websites falsos". O detalhe para a criminalização da conduta é o objetivo dessas práticas, podendo ser elas diferenciadas em: crimes contra a pessoa (relativos à honra), e crimes contra o patrimônio (em que os dados obtidos ilicitamente são utilizados para obter ganho econômico). Os primeiros, no sistema penal brasileiro, estão tipificados desde a Lei 12.737/2012, mas os patrimoniais são considerados, principalmente, como inseridos no tipo penal do estelionato.

A emergência de crimes digitais, que não existiriam sem a relevância que os sistemas digitais têm tomado na vida das pessoas e das empresas/organizações, tornou necessária uma releitura do Direito Penal. E a utilização da internet como meio para a prática desses atos faz surgirem os chamados "cibercrimes" ou "crimes cibernéticos", definidos, conforme Acha (2018, p. 8), como sendo "quaisquer ações típicas, antijurídicas e culpáveis cometidas contra ou pela utilização de processamento automático de dados ou sua transmissão em que a internet seja o principal objeto ou instrumento do crime". Entretanto, há uma distinção adequada nesses crimes, conforme Fiorillo e Conte (2016, p. 139-145): há aqueles que são delitos informáticos próprios (ou puros), praticadas completamente dentro de um sistema digital, tais como o *hacking* e os *malwares*; e os delitos informáticos impróprios, ligados à relação entre o digital e o não-digital, tais como o estelionato digital.

A engenharia social utilizada pelo *phishing* é compreendida na segunda categoria, de delito impróprio, pois abrange a esfera digital, mas a ultrapassa no ato e no objeto do delito. A definição de estelionato digital é a mais adequada pois contempla a noção de engenharia social relativa aos métodos de captação, elicitação, pretensão e táticas mentais, buscando objetivos ou tendo seus meios ligados a dados digitais, ou seja, o local ou não-local da internet e os sistemas digitalizados.4 Portanto, esse é um cenário de interpretação de um crime existente na legislação penal, o crime de estelionato do art. 171 do Código Penal.

4 A tese de Fernando José da Costa (2011, p. 149-158) apresenta o local do crime para fins da persecução penal deve seguir o local da conduta considerada criminosa, mas respeitando o caso de o crime só for assim considerado no local do resultado. Mantendo assim um critério de competência, mesmo reconhecendo o espaço virtual sem fronteiras.

REVISTA MERITUM • v.15 • n.1 • p. P. 116-129 • Jan./Abr. 2020

A adjetivação "digital" ao crime do estelionato é, portanto, um ato de interpretação da lei penal, compreendendo-se que a vantagem e o prejuízo alheio desse delito são obtidos por meio de ferramentas digitais, e ter como bem jurídico protegido os dados digitais relacionados à privacidade. A criminalização dessa conduta, portanto, se caracteriza no ambiente doutrinário e tem efeitos na jurisprudência (FREITAS, 2009, p. 64), apesar da vontade de muitos que a legislação penal se adapte e preveja condutas específicas para o ambiente digital, tendo em vista uma necessidade de tipificação penal.5

A Lei nº 12.737/2012 introduziu no sistema jurídico a tipificação de delitos informáticos puros, no crime de "invasão de dispositivo informático" (art. 154-A do Código Penal): "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida do mecanismo de segurança e com o fim de obter, adulterar ou destruir dados [...]", ou seja, contempla o bem jurídico da liberdade individual, privacidade e intimidade no meio ambiente digital. Esse dispositivo informático violado pode ser qualquer aparelho capaz de armazenar dados pessoas, como computadores, tablets ou celulares, que sejam protegidos por senhas ou outro mecanismo de proteção, sendo o invasor um sujeito ativo doloso que burla o sistema de segurança em nome da violação da privacidade dos dados (KUNRATH, 2017, p. 68).

Há, entretanto, uma diferença entre as práticas tipificadas no âmbito da Lei nº 12.737 e a do estelionato digital (não tipificado), justamente porque as primeiras são relativas aos crimes contra pessoa e a segunda é um crime patrimonial, não relativo a honra. O estelionato digital por meio de *phishing* tem o intuito de capturar dados pessoais e financeiros dos destinatários do golpe para fins econômicos (COSTA, 2011, p. 99-100). Dessa forma, em analogia ao que apresenta a pesquisa de Wendt (2016, p. 154-159), devido à expansão de riscos e incertezas promovida pela comunicação da internet, o intuito criminalizar do Direito Penal não alcançará a complexidade da prática. É preciso contemplar critérios objetivos de aplicação do Direito, fugindo da tendência trazida pela expansão do risco da ampliação da lei penal — obrigando a sociedade a buscar alternativas não-penais.6 É o caso do estelionato, que sob o contexto digital mantém a necessidade de proteger o mesmo bem jurídico, independente dos novos meios, do ponto de vista da criminalização, mas expondo a necessidade de formas educativas e sociais de defesa e resistência aos novos golpes.

3 PROTEÇÃO DE DADOS E CIDADANIA DIGITAL PELOS MEIOS SOCIAIS DE DEFESA

Os desafios para prevenção do cibercrime enfrentam, portanto, a distinção entre políticas criminais e políticas preventivas inovadoras, ou seja, entre a criminalização formal da tipificação dos atos e a ascensão de políticas como (I) políticas de segurança digital, (II) polí-

5 Art. 5º, XXXIX da CRFB/1988: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

6 Como afirma Wendt (2016, p. 165): "Se o Direito Penal tiver função igual à dos espinhos em relação às flores, supostamente de proteger a sociedade, tanto espinho quanto Direito Penal estão fadados ao insucesso, porquanto o machado da contemporaneidade é avassalador e os cortes e feridas geradas não se curarão com mais machadadas. Há que se repensar o critério normativo-penal como forma de solucionar questões sociais que são possíveis de se solucionar através de práticas comportamentais, administrativas ou técnicas, ou, quiçá, por outros ramos do Direito que não o Penal."

ticas de educação informacional e ética na internet, (III) políticas de solução de conflitos nas relações virtuais, conforme Kunrath (2017, p. 72-146). Esse paradigma não-penal respeita a tendência de busca de alternativas para o combate ao cibercrime em âmbito internacional, mais ligadas a segurança da informação que a persecução penal (SILVA, 2012, p. 103-104).

A simulação promovida pelo estudo de Konradt, Schilling e Werners (2016, p. 10) indica que no contexto da corrente digitalização da sociedade tem sido promovida a profissionalização das análises dos chamados "cibercrimes", sendo necessário abordar as fontes econômicas e os frutos advindos dessas técnicas que se utilizam da engenharia social, tendo em vista que os engenheiros sociais trabalham sob uma multiplicidade de riscos e "tentativa e erro", sendo mais importante para combatê-los proteger a privacidade dos dados que a punição dessas condutas com um novo tipo criminal e um novo braço do sistema penal.

A ascensão de uma política de segurança digital (I) contempla aquilo proposto no Marco Civil da Internet (Lei 12.965/2014) como princípios e garantias do uso da internet no Brasil, como o respeito à liberdade de expressão e os direitos humanos (art. 2) e o princípio da proteção da privacidade e dos dados pessoais. As garantias (art. 7) são da inviolabilidade da intimidade e da comunicação pessoal via internet, sendo a única alternativa para fornecimento de dados pessoais para terceiros o consentimento livre, expresso e informado. Também, é dever do Poder Público (União, Estados e Municípios) o desenvolvimento da internet e de uma estrutura participativa e colaborativa de sua gestão, promovendo inclusão digital e uma cultura digital (art. 27).

A inclusão digital e a cultura de internet estão diretamente ligadas à proteção dos dados, por isso ela se instrumentaliza na Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei n. 13.709/2018) com vigência estabelecida para 2020, que dispõe sob esse aspecto do tratamento dos dados pessoais e é disciplinada pelo respeito à privacidade e a autodeterminação informativa (art. 2º, I e II), sendo assim uma ferramenta também com intuito de fomentar uma cultura de proteção de dados, tanto das pessoas físicas como jurídicas. Nesses aspectos podem ser compreendidas as políticas inovadoras de educação informacional e ética na internet (II) como ferramenta pública de defesa aos cibercrimes.

A inclusão digital, é, portanto, a promoção de uma cidadania que reconhece a dimensão do espaço virtual e reconhece a segurança digital como algo fundamental para inserção na sociedade da informação (MARTINI, 2005). A educação informacional que empodera o cidadão no âmbito digital também está associada à sua posição hipossuficiente nas relações de consumo, reconhecendo a desigualdade técnica que o consumidor possui frente às amplas bases de dados das empresas varejistas, por exemplo (MIRAGEM, 2019, p. 27-28). Portanto, a cidadania digital pressupõe o empoderamento técnico do cidadão ao mesmo tempo que reconhece as assimetrias tecnológicas da estrutura social.

Também, do ponto de vista das empresas, contempla-se a ideia de políticas de segurança de informação e *compliance* atentos ao princípio da privacidade e da preservação dos dados digitais, ou seja, políticas corporativas que estabeleçam diretrizes e normas administrativas de segurança da informação. O legado possível para esses marcos normativos, principalmente a LGPD, conforme Bioni (2019, p. 32-33), é do fortalecimento de uma cultura de proteção de dados para as organizações, tendo em vista fatores importantes como reputação e confiança no ambiente corporativo. Também, que haja uma cultura regulatória em

REVISTA MERITUM • v.15 • n.1 • p. 116-129 • Jan./Abr. 2020

REVISTA MERITUM • v.15 • n.1 • p. P. 116-129 • Jan./Abr. 2020

prol da interpretação e aplicação sistemática dessa proteção em todo o desenvolvimento tecnológico (DONEDA; MENDES, 2019, p. 322).

A mitigação dos riscos trazidos pelas técnicas associadas à engenharia social precisam passar pela identificação dos agressores com essas chamadas fragilidades dos usuários, ou seja, da parte humano nos sistemas digitais. Como observa Towsend (2019), a empresa Avast, ao relatar os fatores a serem observados para que os engenheiros sociais se aproveitem dos usuários: pressão do tempo (forçando o usuário a tomar decisões imediatas), medo da perda, direção errada, avaliações falsas, identidade fala e informações parciais. O *phishing* ampliou seu contexto para além do estelionato digital, sendo que o ato de *phishing for phools,* ou "pescando tolos", como afirma Akerlof e Shiller (2015, p. 10) contempla as áreas da publicidade comercial e da política, em que os mercados de consumo e eleitorais se utilizam dos dados dos usuários da internet para interferir em suas percepções, adquirindo-os de maneira legal — mesmo sendo adeptos de práticas que escondem o real motivo da captação de informação.

A educação e a consciência coletiva podem contribuir para formas colaborativas de combate contra técnicas como a de *phising*, sendo preciso desenvolver formas educativas para criar um comportamento defensivo resistente e resiliente contra esses ataques: podem ser *games,*[7] cartilhas ou informativos que exponham como os dados dos usuários podem ou não ser utilizados e de que forma esse uso é legal, impedindo ou ao menos diminuindo a confusão do usuário quando entrega dados pessoais em plataformas digitais. Assim, trabalhando a educação tecnológica — fortalecendo o elo humano (TAYOURI, 2015, p. 1096) —, como aponta o estudo de Nicholson, Coventry e Briggs (2017, p. 292) compreendendo a importância de utilizar meios sociais, não apenas tecnológicos, para se defender dos ataques dos engenheiros sociais — como a atenção aos dados de quem envia o ataque nos casos de *phishing*.

Para o ambiente corporativo, uma alternativa é o empoderamento individual dos empregados, formando usuários resistentes e resilientes aos ataques de engenharia social como o roubo de identidade e os *ransomware*. As recomendações feitas pelo estudo de Thomas (2018, p. 17) se dão no sentido de se reconhecer os grupos distintos de usuários dentro de uma rede corporativa tendo em vista o impacto de seus trabalhos, a familiaridade com o *phishing* e os níveis de confiança (em acreditar não ser suscetível a golpes), aprimorando as vulnerabilidades específicas, empoderando os funcionários a um comportamento ativo que saiba os riscos e as formas de defesa para cada ato executado em relação aos dados digitais.

Isso só é possível por meio de políticas organizacionais adequados à efetiva segurança de dados com formas participativas e que eduquem funcionários e práticas protetivas a privacidade nas atividades das empresas — a LGPD representa legalmente essa evolução no setor organizacional, seja na governança pública ou nas corporações privadas, ao se basear no fundamento da *accountability* ou responsabilidade empresarial. Daí sucede a necessidade das organizações entrarem em *compliance* com a lei, mantendo em suas práticas o princípio da autodeterminação informativa, do consentimento informado e da proteção dos dados pessoais — dando poder às instituições responsáveis pelas investigações e responsa-

7 O texto de Arachchilage. Love e Beznosov (2016) demonstra interessantes resultados sobre a educação dos usuários em um jogo digital que indica ferramentas anti-*phishing*.

bilização internas nas empresas tendo em vista esses princípios. Uma dessas práticas são as certificações privadas de adequação a princípios de proteção de dados.

A fixação de controles internos tem por objetivo ser um reforço à regulação estatal, ao cumprimento da lei, no caso da proteção de dados, conforme descrevem Frazão, Oliva e Abilia (2019, p. 693-711), precisam ser adequados ao risco da atividade, à criação de um programa de treinamento dos empregados em relação à segurança de dados, à regulação *by design* e um efetivo monitoramento do próprio programa de *compliance*. Uma das consequências diretas desse cenário é a criação do *data protection officer* (RECIO, 2017), profissional ou setor responsável pela proteção de dados dentro de uma empresa,8 o que objetiva alinhar a atividade empresarial com os preceitos legais acerca da privacidade e da segurança informacional, tornando empresas e pessoas menos vulneráveis a golpes classificáveis como estelionato digital.

Ainda, resta o papel social determinado às empresas de tecnologia, que gerenciam os algoritmos e os sistemas digitais utilizados em todas essas operações (pessoais ou empresariais). É o que se chama de regulação *by design*, em que os criadores dos algoritmos são responsáveis por verificar a proteção aos direitos fundamentais, principalmente à privacidade, na ordem de seus sistemas, sendo sistematicamente incorporados. Isto é, conforme Magrani (2019), o Direito sendo usado como metatecnologia, ou seja, a engenharia de *software* passa a considerar os direitos fundamentais e direitos humanos, no caso o direito à segurança de dados, na esfera da produção tecnológica. É o *accountability* algorítmico, em que se exige a responsabilidade social do desenvolvedor (KITCHIN, 2017, p. 26-27).

É um processo que alia a autorregulação dessas empresas transnacionais (FORNASIER; FERREIRA, 2015, p. 409) de tecnologia à necessidade de auditabilidade social, devendo a programação ser submetida à análise crítica da sociedade, bem como a se importar com os princípios jurídicos que orientam os direitos humanos, estando entre eles o princípio da autodeterminação informativa. Ao mesmo tempo que há a privatização da regulação, também deve haver a privatização das responsabilidade, tamanha é a importância dos algoritmos orientados pelas grandes empresas de tecnologia (MARTIN, 2019). A programação precisa atentar a necessidade de criação de espaços com valores democráticos e sociais, trazendo o que há de melhor nos objetivos das leis para dentro dos algoritmos (WEBER, 2018, p. 705-706).

A característica disruptiva das novas tecnologias e seus algoritmos pode permitir sistemas mais seguros e empoderar usuários mais capazes de resistir a golpes digitais, devendo o Direito se portar de maneira adequada, não regredindo ao positivismo da criminalização penal da conduta do estelionato digital, mas sim incorporando princípios adequados ao núcleo da programação — criando um direito flexível e capaz de lidar com as tecnologias, tornando a relação entre engenharia de *software* e Direito como algo híbrido (SANTOS; MARCO; MOLLER, 2019, p. 3079-3081).

8 Acerca da figura do *Data Protection Officer* (DPO): "Para isso, será de suma importância que o encarregado desempenhe suas funções com autonomia e imparcialidade dentro das organizações, podendo ele interferir nos processos internos, e sugerir mudanças e adequações, mesmo que isso afete economicamente a empresa, tendo em vista que sua motivação principal deve ser a de fazer com que a empresa cumpra as normas impostas pela legislação" (OLIVEIRA et al., 2019, p. 18).

REVISTA MERITUM • v.15 • n.1 • p. P. 116-129 • Jan./Abr. 2020

4 CONCLUSÃO

A defesa contra ataques e a proteção dos dados pessoais frente à engenharia social e sua mais evidenciada prática (*phishing*) não passa pelo simples desenvolvimento de um sistema invulnerável, pois essa prática não se utiliza de ferramentas digitais ou de tecnologias complexas. Essas práticas dependem da exploração de aberturas humanas e de fragilidades das relações sociais em relação a privacidade. O *phishing* depende de uma complexidade de fatores e se alimenta deles — devendo sua defesa ser proporcional, e necessitar de uma educação digital adequada, que contemple uma cidadania digital consciente de tudo aquilo que se compartilha nas redes e suas consequências, restringindo os buracos em que um engenheiro social possa se apropriar dos dados pessoais de usuários da internet.

Essa conclusão foi possível após descrever o fenômeno que é a engenharia social como um conjunto de métodos que condicionam uma série de práticas, legais e ilegais, tecnológicas e não tecnológicas. No caso, o *phishing* é um golpe que utiliza das práticas da engenharia social de captação de informações, elicitação, pretensão e táticas mentais para aplicar fraudes com intuito de perceber vantagem econômica. É um conceito complexo justamente pela sua associação entre fatores tecnológicos e práticas que nada tem a ver com a complexidade técnica. Ou seja, o engenheiro social, por mais que aplique estelionato em sistemas digitais, não precisa ser um *expert* informático, um *hacker* — até mesmo por isso são considerados crimes digitais impróprios.

A criminalização do estelionato digital passa pelo esclarecimento acerca da prática, evitando o deslumbre com as questões informáticas e digitais, percebendo que, por muitas vezes, o meio digital é simples e está associado a técnicas não tecnológicas de obtenção de dados. Assim, diferencia-se dos crimes contra a pessoa tipificados pela Lei 12.735/2012, pois não há uma complexa adulteração de um sistema digital de proteção de dados pessoais, mas a utilização de técnicas sociais para enganar as vítimas a entregar dados que sujeitam seu patrimônio a apropriação indevida. O *phishing* utiliza as novas tecnologias de informação e comunicação como meio para aplicação dessas fraudes, mas suas técnicas são puramente sociais. A prevenção dessas práticas passa, portanto, mais pela educação informacional e uma cultura de proteção de dados, um empoderamento do cidadão digital, que pela criminalização de condutas informáticas.

Buscando não cair na tentação da criminalização, respondendo ao problema de pesquisa deste, surgem alternativas criativas, inovadoras e socialmente mais adequadas para a proteção dos dados e a prevenção aos cibercrimes, neste trabalho elencamos ou dividimos essas respostas em em três grupos: (I) na educação informacional e no empoderamento da cidadania digital; (II) na cultura organizacional de proteção de dados por meio das políticas corporativas ou *compliance*; e (III) na autorregulação ou regulação *by design* das próprias empresas de tecnologia, pautando seus algoritmos em princípios de privacidade e direitos humanos. E saliente-se que o desenvolvimento de políticas preventivas, para além da mera repressão penal mediante novos tipos, não vem aqui a significar a responsabilização da vítima pela conduta do criminoso, mas sim, de responsabilizar o Poder Público e as empresas de tecnologia, clamando, em relação a tais entes, por atitudes preventivas e proativas contra tais práticas. Ou seja: tais entes devem abandonar a postura de repressão mediante legislação como sendo útil e necessária por si só.

Esses meios sociais de prevenção são as soluções alternativas ao sistema penal, que buscam mais uma cultura da promoção da cidadania digital e do empoderamento dos usuários baseados na noção de privacidade e resiliência aos golpes do que a criminalização das condutas, tendo em vista que a tipificação específica e cuidadosa do tipo penal do estelionato digital tem mais a ver com o bom funcionamento da dogmática penal que da efetiva proteção dos dados pessoais. A tríade de alternativas propostas, uma para as pessoas físicas, outra para as jurídicas e, também, daquela que instrui o funcionamento dos sistemas digitais, tem em vista a efetivação dos princípios da autodeterminação informativa e da inclusão digital.

REFERÊNCIAS

ACHA, Fernanda Rosa. 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. Disponível em: http://revista.srvroot.com/linkscienceplace/index.php/linkscienceplace/article/view/621/347. Acesso em: 13 jan 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. *O guia essencial sobre phishing*: Como funciona e como se proteger. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em: 14 jan 2020.

BERGER, Leoni. *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. Universidade Federal de Santa Catarina. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/80569/139040.pdf?sequence=1. Acesso em: 11 jan 2020.

BIONI, Bruno Ricardo. Inovar pela Lei. *Gv/Executivo*, v. 18, n. 4, p. 31-33, jul/ago 2019. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/download/79978/76432. Acesso em: 20 jan 2020.

BRASIL. *Constituição Federal de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 13 jan 2020.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 13 jan 2020.

BRASIL. *Lei 13.709, de 14 de agosto de 2018*. Lei geral de proteção de dados pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 jan 2019.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 jan 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 nos crimes informáticos*. Tese (Doutorado em Direito). Faculdade de Direito da Universidade de São Paulo. 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/publico/Fernando_Jose_da_Costa.pdf. Acesso em: 14 jan 2019.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira In: BELLI, Luca; CAVALLI, Olga. *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 no meio ambiente digital e a sociedade da informação*. 2 ed. São Paulo: Saraiva, 2016.

FORNASIER, Mateus de Oliveira; FERREIRA, Luciano Vaz. 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. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (orgs). *Lei geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro.* São Paulo: Revista dos Tribunais, 2019.

FREITAS, Riany Alves de Freitas. Segurança Digital: estelionato digital e a segurança em sites de comércio eletrônico. *MPMG Jurídico*, n. 17, v. 1, p. 63-65, 2009. Disponível em: https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/502/Estelionato%20digital.pdf?sequence=3. Acesso em: 13 jan 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. *A expansão da criminalidade no cyberespaço*. Feira de Santana: Universidade Estadual de Feira de Santana, 2017. Disponível em: http://www.uefs.br/modules/documentos/get_file.php?curent_file=3330&curent_dir=1772. Acesso em: 14 jan 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. *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. Inclusão digital e inclusão social. *Inclus*ão social, v.1, n. 1, 2005. Disponível em: http://revista.ibict.br/inclusao/article/view/1501/1685. Acesso em: 14 jan 2020.

MIRAGEM, Bruno. 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.Disponível em: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/nicholson. Acesso em: 10 jan 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. A Lei Geral de Proteção de Dados Brasileira na Prática Empresarial In: SILVA, Rafael Aggens Ferreira da (ed.). *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. Disponível em: http://esa.sites.oabpr.org.br/wp-content/uploads/sites/7/2019/06/direito-e-inovacao-volume1.pdf. Acesso em 14 jan 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. 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. *A*ção internacional no combate ao cibercrime e sua influê*ncia no ordenamento jurídico brasileiro*. 2012. 109 p. Dissertação de Mestrado em Direito Internacional Econômico da Universidade Católica de Brasília. Brasília, 2012. Disponível em: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/276/1/Marcelo%20Mesquita%20Silva.pdf. Acesso em: 13 jan 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. Engenharia social: não se trata apenas de golpes de phishing. Disponível em: https://blog.avast.com/pt-br/social-engineering-hacks. Acesso em: 02 jan 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. *A internet e a fragmentação do direito penal no reforço da cultura do medo no Brasil:* percepção social e perspectiva legislativa. Dissertação (mestrado em Direito) - Universidade La Salle. Canoas, 2016. Disponível em: http://repositorio.unilasalle.edu.br/bitstream/11690/1029/1/ewendt.pdf. Acesso em: 13 jan 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.