UNIVERSIDADE TIRADENTES – UNIT
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO – ARTIGO CIENTÍFICO

SEGURANÇA NA REDE E AUTODERTERMINAÇÃO DOS USUÁRIOS COMO INSTRUMENTOS DE PROTEÇÃO CONTRA CIBER *PHISHING*

José Cícero Correia Alves
Orientador: Prof. Me. Jéffson Menezes de Sousa

Propriá
2019

JOSÉ CÍCERO CORREIA ALVES

SEGURANÇA NA REDE E AUTODERTERMINAÇÃO DOS USUÁRIOS COMO INSTRUMENTOS DE PROTEÇÃO CONTRA CIBER *PHISHING*

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovado em _____/_____/_____.

Banca Examinadora

Professor Orientador – Me. Jéffson Menezes de Sousa
Universidade Tiradentes

Profa. Ma. Fernanda Oliveira Santos
Universidade Tiradentes

Profa. Ma. Valquíria Nathali Cavalcante Falcão
Universidade Tiradentes

SEGURANÇA NA REDE E AUTODERTERMINAÇÃO DOS USUÁRIOS COMO INSTRUMENTOS DE PROTEÇÃO CONTRA CIBER *PHISHING*

LEGAL REINFORCEMENTS REQUIRED FOR NETWORK SECURITY AND USERS SELF-DETERMINATION AS INSTRUMENTS OF PROTECTION AGAINST CIBER *PHISHING*

José Cícero Correia Alves[1]

RESUMO

Phishing, assim é conhecida uma das modalidades de golpes virtuais mais populares da internet. Seguindo um princípio básico de lançamento de iscas falsas no ambiente digital, milhões de indivíduos ao redor do mundo são expostos ao enorme perigo de ter seus dados, e mesmo suas finanças, atacadas por fraudadores. Como os mecanismos jurídicos devem reagir a isso? Uma cultura de cibersergurança pode garantir uma camada de proteção à convivência social? Como fomentar essa cultura? Qual é o lugar do indivíduo na cibersergurança? Partindo dessas perguntas buscou-se através do presente artigo fornecer argumentos em prol do incentivo ao fomento de mecanismos de segurança digital contra o *Phishing* , que passam por incentivar empresas, organismos e instituições a implementar boas práticas, mas que não prescinde de chamar toda a sociedade para engajar-se em educação digital massiva, como ferramenta para inclusão digital segura.

Palavras-chave: Crimes cibernéticos; Educação midiática e informacional; Responsabilidade civil da Empresa.

ABSTRACT

Phishing its known as one of the most popular types of virtual scams on the internet. Following a basic principle of casting fake baits in the digital environment, millions around the world are exposed to the enormous danger of their data, and even their finances, being attacked by fraudsters. How should legal mechanisms react to this? Can a cybersecurity culture guarantee a layer of protection for social life? How to foster this culture? What is the individual's place in cybersecurity? Based on these and other questions, we sought to present arguments in favor of encouraging the promotion of digital security mechanisms against Phishing, which involves incentives for companies, institutions and organization to implement good practices, but which does not do without calling all society to engage in massive digital education, as a tool for secure digital inclusion.

Keywords: Cyber crimes; civil responsability; media and informational education.

[1] Bacharelando em Direito pela Universidade Tiradentes – UNIT, *campus* Propriá. E-mail: jose.cicero@souunit.com.br

1 INTRODUÇÃO

Os debates pertinentes à Internet, Sociedade em Rede, suas múltiplas problemáticas e impactos na interação social, são um vasto e complexo emaranhado que comporta toda uma erudição peculiar. Espalham-se pelo mundo, diversos pesquisadores e pensadores em variada e multidisciplinar tarefa de melhor compreender e lidar com a nova e intrincada teia que se estende aproximando distâncias e modificando paradigmas civilizacionais. Notório se mostra que a emergência da rede como amalgama do mundo, trouxe desafios para múltiplos setores, e para a esfera do Direto, diversas instigações que exigem progressiva e constante atualização e análise.

Este é exatamente o quadro que se delineia quando pensamos nos crimes cometidos através do ambiente virtual de interação, visto que, à medida que o acesso e a universalização da rede avançam, problemas do mundo real eclodem com ênfase e periculosidade também nos espaços virtuais. Em decorrência disto, os Estados em sua persecução criminal passam a ter um ambiente a mais para vigiar. E os operadores do direito por seu turno, passam a ter um fértil campo com o qual se ocupar.

Nesse contexto, o presente trabalho tem como objetivo norteador a análise do fenômeno do *phising* ou ciberpescaria, uma das modalidades de golpes mais comuns de fraude na rede. A partir daí, almeja-se abordar a responsabilidade civil dos agentes no ambiente virtual. Parte-se da problemática proemial: como pensar a responsabilidade civil diante da "pescaria digital"?

Especialmente, em casos de , qual a responsabilidade das empresas que tem suas marcas indevidamente utilizadas no cometimento de cribercrimes? As mesmas possuem responsabilidade objetiva? Que mecanismos de precaução estas empresas devem tomar? Deve o Estado exigir que empresas adotem procedimentos que reforcem a segurança no ambiente virtual?

Tomadas estas como perguntas meio, quer-se ao final, em consonância com o relatório "As pedras angulares para a promoção de sociedades do conhecimento inclusivas: Acesso à informação e ao conhecimento, liberdade de expressão e ética na Internet global", (UNESCO, 2017), propor alternativas voltadas à Alfabetização Midiática e Informacional como mecanismos de proteção dos indivíduos contra a cibercriminalidade.

Para responder as provocações geradoras, lança-se mão de pesquisa bibliográfica, além de consultas a bancos de dados de artigos científicos, às legislações e jurisprudências pertinentes ao tema, também nos servindo de matérias do jornalismo especializado.

2 *PHISHING*: Conceito e modalidades

Pescaria, assim é denominado um dos golpes mais comuns no ambiente virtual. O *phishing* pode ser bem descrito como a digitalização do crime de estelionato ou do furto mediante fraude, e indubitavelmente tem potencial lesivo extremamente semelhante ao estelionato tradicional. É interessante como conceituar este golpe frequentemente passa, por uma demonstração quase gráfica, criando-se uma triangularização da relação, que consiste em um "estelionatário" que usa uma "isca virtual" para atingir um "usuário desavisado".

De fato, há diversas modalidades de veiculação de "estelionato digital", aqui serão listadas as mais relevantes. Entrementes, a título introdutório, vale conceituar de forma genérica o fenômeno. Invariavelmente, o cibercriminoso, ao lançar-se na pescaria, dispara iscas pelo espaço virtual, em geral por meio de e-mail ou links falsos, a partir dos quais pode praticar diversas condutas lesivas as suas vítimas, a isto Pinheiro (2016, p. 395) chama "*Phishing Scan*".

O crime acima descrito tem dimensões a serem analisadas à luz do Direito, no âmbito penal e civil, sem dispensar a erudição do Direito Digital, o que será feito em tempo oportuno. Mas antes que se parta para esta análise mais jurídica, necessário discorrer sobre as diversas modalidades de *phishing* que vem sendo praticadas e que vem atingindo usuários por todo mundo.

2.1 Modalidades de *Phishing*

Neste ponto, é válido trazer a lume alguns mecanismos que partem do mesmo princípio de ataque, isto é, o disparo virtual de iscas como meio de se atingir o intento criminoso, o dolo de obter vantagem indevida por meio de fraude, bem como roubar e sequestrar, por meio digital, dados e máquinas.

As designações utilizadas a seguir foram encontradas em sites de divulgação de conteúdo sobre internet e tecnologia de um modo geral. Leia-se, de sites que tem como pano de fundo a difusão de informação sobre internet e tecnologia em linguagem comum aos usuários médios. Interessante notar que nesse meio cada modalidade recebe uma designação, que em geral, tenta representar o golpe de forma gráfica e objetiva. Além disto, importante

destacar que é bem possível que uma ou outra modalidade entre em desuso bem como podem surgir outras técnicas partindo do mesmo princípio da pescaria digital.

Acima se descreveu o *Phishing Scan* ou "*Phishingi* Tradicional", que consiste em disparos massivos de iscas rudimentares e sem alvo objetivo, em outras palavras, na modalidade mais tradicional, o crime não tem uma vitima objetiva sendo uma pulverização de iscas; todos os usuários que eventualmente venham a receber e-mails falsos ou acessar links com propaganda podem vir a ser lesados.

Irmanada a esta categoria, MALWAREBYTES (2020, n.p) cita um procedimento extremamente semelhante que, porém, comporta peculiaridades. O "*Clone Phishing*", que consiste simplesmente em introduzir no conteúdo de comunicações eletrônicas ou de "sites falsos" iscas promocionais. Em geral, apresentam-se produtos com preços deliberadamente abaixo do valor comum de mercado, valendo-se da vulnerabilidade e, muitas vezes, do comportamento compulsivo de compradores que não estejam alerta.

No bojo destas condutas, os cibercriminosos chegam a criar simulacros de comunicação e mesmo de sites de grandes empresas. Literalmente, o ciberpescador tenta se passar por aquela grande empresa utilizando-se de sua marca, dando aos compradores a sensação de que estão se envolvendo em um negócio seguro. Veja-se bem, oferta-se serviço barato, em "ofertas iscas" que, pelo menos para leigos, parecem ser de lojas destacadas no mercado.

A diferença básica entre o *Phishing* Tradicional e o *Clone Phishing* é a qualidade do acabamento das iscas recebidas pela vitima. Naquele *modus operandi* mais antigo, há ausência de logomarcas e imagens, e quando muito os sites a que as vitimas são direcionadas em nada se parecem com lojas de empresas tradicionais, ali há uma simplesmente apresentação grosseira de propagandas. Já na modalidade clonagem, os e-mails são mais bem trabalhados dificultando a identificação inicial do conteúdo como falso. De fato, esta segunda modalidade é muito comum ainda hoje e muito perigosa, Patríca Peck diz sobre isto:

> Pela nossa experiência, grandes empresas estão mais expostas, portanto, são alvos mais fáceis. Quanto mais famosa e conhecida uma marca, mais incidentes ela está sujeita a passar na Internet no tocante a uso não autorizado de marca, abuso de liberdade de expressão por terceiros, registro indevido de domínio ou similar a domínio existente para fins de cybersquatting, uso da marca em e-mails falsos para ludibriar pessoas a passarem dados e a se contaminarem por arquivos maliciosos. (PINHEIRO, 2016, p. 391)

As duas modalidades citada acima são veiculadas massivamente. Há, contudo, segundo Mirella Stivani (2018) e Malwarebytes (2020) a efetivação deste golpe utilizando-se alvos individualizados, isto é, o fraudatário dirige sua pescaria a pessoas e entidades específicas. Avança-se ainda mais, o conteúdo das iscas lançadas é extremamente

personalizado, fazendo com que o receptador sinta que esta recebendo algo pensado para si. Esta forma de pescaria tem sido popularmente denominada *Spear Phishing*.

Se na tradicional e na modalidade clonagem a pesca é no atacado, no *Spear Phishing* existe ação controlada, ação no varejo. Contudo, em ambos os casos o estelionato tem potencial de dirigir-se aos fins de obtenção de vantagem financeira indevida e obtenção criminosa de dados particulares.

Duas modalidades interessantes são o *Phone Phishing* e o *SMS Phishing* , citadas por Malwarebytes (2020), estas seguem princípios semelhantes, utilizando ligações e torpedos respectivamente. O diferencial aqui, segundo Malwarebytes (2020) é que, por meios de ligações ou torpedos, os fraudatários enviam para suas vítimas informações assustadoras ou que induzem a pessoa que recebe a agir com celeridade. Exemplos disto seriam: a necessidade de pagamento de determinado valor para liberação de alguém sequestrado ou a necessidade de um depósito para pagar um guincho no meio da estrada.

De fato, as modalidades de *phishing* acima trabalhadas se beneficiaram das primeiras expansões do ambiente virtual, isto é, do início da popularização dos computadores. Aqui, interessante fazer nota ao que diz Pierre Lévy, ao tratar da potencialização da capacidade de armazenamento de dados: “desde o início da informática, as memórias têm evoluído sempre em direção a uma maior capacidade de armazenamento, maior miniaturização, maior rapidez de acesso e confiabilidade, enquanto seu custo cai constantemente" (LÉVY,1999, p. 34).

Esta dinâmica de miniaturização descrita acompanha, se não possibilita, a afluência massiva de usuários. Daí decorre a complexificação das interações cibernéticas, o que, mais e mais, tem profundo impacto na comunicação humana. Este fenômeno parece alcançar seu auge com o advento das redes sociais, pois daí a humanidade passou, como explica LÉVY (1999, p. 63), de uma comunicação de “um-um” ou “um-todos” (um indivíduo para um indivíduo ou um indivíduo para todos os indivíduos), para uma comunicação “todos-todos” (em que todos os indivíduos falam e, potencialmente, podem ser ouvidos por todos), isto é, uma comunicação intensamente pública.

De tal sorte que algo lançado na rede agora, numa fração milionésima de segundo, está em todo o mundo. E esta transformação, sem nenhuma dúvida, impactou profundamente a ciberpescaria. Hoje, basta um link falso replicável a exaustão por mensagens instantâneas, ou mesmo em um post em rede social, para que se exponham milhares de usuários desavisados a diversos riscos, inclusive as mesmas e velhas técnicas dos pescadores virtuais, as invasões, e sequestros de dados e máquinas. Neste cenário de redes sociais massificadas e de

armazenamento em nuvem, identificamos diversas novas formas de instrumentalização da ciberpescaria.

Mirella Stivani (2018) relata casos interessantes desse impacto, ao se referir a *phishing* por links falsos que se passam por links da plataforma de armazenamento em nuvem Dropbox e da plataforma online de edição de texto Google Docs. Utilizando-se destes links falsos enviados para os usuários, "hackers pescadores", logram êxito em roubar chaves de acesso e apropriar-se de arquivos armazenados naquelas plataformas, utilizadas por milhões de usuários ao redor do planeta. Ao ter esses dados vulnerados diversos usuários passaram a ser expostos às situações vexatórias, na medida que os invasores conseguiam se apropriar de arquivos sensíveis, tais como documentação, ou mesmo imagens eróticas de armazenamento privado. Nesse tipo de invasão, como em um tradicional crime de extorsão, os invasores potencialmente cobram resgate sob pena de expor o conteúdo ao público.

Indo mais adiante, há duas modalidades especialmente que não necessariamente se enquadram no conceito de *Phishing Scan* apresentado por Patrícia Peck Pinheiro e citado acima. Nestas modalidades os ataques são veiculados por "invasão hacker" para obtenção e potencial destruição de dados de usuários específicos. Mirella Stivani (2018) referiu-se à Phishing Pharming e do *Phishing* por *Ransomware*, duas modalidade especialmente perigosas de ciberpescaria, na visão da autora.

No *Phishing Pharming*, o fraudatário dirige sua atenção às empresas, instituições e órgãos públicos. Os ataques nesta modalidade consistem, segundo Mirella Stivani (2018) em invadir e se apropriar de dados através dos servidores DNS (*Domain Name System*), tendo potencial para roubar dados de todos os usuários conectados ao referido servidor local. Já no *Phishing* por *Ransomware*, segundo a mesma autora, o invasor sequestra a máquina da vítima por meio de malware (software malicioso) e exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

À guisa de arremate, é importante frisar que estas nomenclaturas são extraídas de matérias publicadas em portais dedicados à difusão de conhecimento sobre temas ligados à informática e tecnologia, especialmente essas nomenclaturas constam em portais de empresas que trabalham com cibersegurança (venda de pacotes popularmente conhecidos como antivírus) o que lhes empresta nível razoável de credibilidade. Pode haver outras tantas nomenclaturas, sendo citadas no presente momento a título de subsídio e sem pretensão de exaustão. O intuito final é apresentar a realidade e a periculosidade dessas diversas modalidades.

Levantadas essas considerações gerais, passa-se a breves considerações ciber-criminais, para em seguida promover a reflexão sobre a responsabilidade civil e o papel dos múltiplos agentes que povoam as redes na promoção de um ambiente virtual mais seguro e civilizado.

2.2 Breves considerações ciber-criminais.

Pois bem, feitas ponderações gerais sobre as modalidades de aplicação desses cibergolpes, passa-se a uma breve pontuação sobre a relação do mesmo com a alçada do Direito penal. Aqui é importante vincar que por ser um fenômeno complexo e com diversas modalidades, o *phishing* não pode ser enquadro em um único dispositivo do encarte penal pátrio. Em que pese nossa preferência, expressa desde o exórdio este writ, pela expressão estelionato. Deveras, a depender da modalidade utilizada o agente pode transitar por diversos dispositivos do Código Penal.

Patrícia Peck Pinheiro (2016, p. 394) tende a compreender que o furto majorado pela fraude (Art. 155, §4º, II) seria o tipo penal mais afeito ao *phishing* "no qual há envio de um e-mail falso" e no qual "são capturados dados de sua conta bancária mediante a instalação de um arquivo malicioso em seu equipamento", aqui podemos ampliar a aplicação do referido tipo penal para qualquer modalidade assemelhada, em que haja inversão da posse de valores, bens ou dados da vítima. Tendemos a concordar com a mesma nestes casos em que há lesão patrimonial, isto é em que o criminoso realmente adentra na esfera patrimonial da vítima. Já quando a fraude se dirige a dados, junto com determinado apontamento da doutrina sublinhado por PINHEIRO (2016, p. 396), é salutar o entendimento de que tal ação encontraria melhor cominação no artigo 171 do Código Penal (crime de estelionato), caso os dados permaneçam disponíveis para o proprietário.

Dando seguimento, PINHEIRO (2016, p. 396) diz que "no Brasil, a tendência é de que sejam tipificadas algumas condutas criminosas próprias da Internet". A mesma doutrinadora diz alhures que "Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente" PINHEIRO (2016, p. 396).

Neste sentido, não obstante a dificuldade, é cogente a necessidade de tipificação mais específica para um quantitativo maior de condutas lesivas em ambientes digitais, visto que determinadas condutas no ciberespaço tem sido genericamente enquadradas em crimes como os citados até aqui. Deveras, uma sociedade vulnerável à ciberpescaria está em risco. Desde

usuários comuns até grandes corporações precisam mais e mais, cuidar rigorosamente do material que adentra suas máquinas e investir generosamente em segurança e aquisição de informação para se evitar prejuízos.

O dilema jurídico que surge a partir da constatação da gravidade do perigo dos ataques virtuais é: Como cuidar da sociedade para que amadureça e lide melhor com essas questões? Também é inafastável levantar considerações sobre: como corporações, instituições e órgãos governamentais devem institucionalizar e mesmo regular a atividade dos diversos agentes cibernéticos, criando protocolos de segurança e vigilância digital, capazes de evitar a disseminação de iscas criminosas que se utilizem da marca destas instituições? Vamos a isso.

3 A RESPONSABILIDADE CIVIL DA EMPRESA EM CASOS DE *PHISHING*

Até aqui temos a reflexão sobre o fenômeno da ciberpescaria em si, e apresentamos brevemente seu impacto cibercriminal e algumas das cominações legais que tais práticas podem acarretar. Cabendo neste momento dirigir o foco a discussão sobre a responsabilidade civil dos agentes que atuam no meio digital.

Pelo que fixamos anteriormente, é perceptível que há modalidades de *phishing* em que os fraudatórios, invasores ou sequestradores de dados podem utilizar-se do nome ou marca de determinada empresa como maquiagem para suas iscas lançadas no ambiente virtual, como ocorre nas modalidades que denominamos "*Clone Phishing" e "Spear Phishing"*.

Já em modalidade como o *Phishing Pharming* e *Phishing* por Ransomware o sequestro de servidores e máquinas e eventual vazamento de dados internos da instituição é o que mais assusta, podendo pôr em risco a segurança da própria empresa, diversas pessoas que conectam suas máquinas as suas redes, e tão grave quanto ou ainda mais grave por seu potencial de abrangência, atingir dados dos clientes ou usuários dos serviços da empresa.

Frente à vulnerabilidade de indivíduos desavisados nas redes e mesmo frente a ataque a servidores DNS uma questão se arvora: como deve funcionar a responsabilização civil dos agentes que atuam no meio digital em casos como estes? Outra importante inquietação que pretende-se explorar aqui é: em casos de *phishing*, é possível falar em responsabilidade das empresas que têm suas marcas indevidamente utilizadas, ou seu Servidor DNS invadido? As mesmas possuem responsabilidade objetiva? Que mecanismos de precaução estas empresas devem tomar? E, afinal, o Estado deve exigir que empresas adotem procedimentos que reforcem a segurança no ambiente virtual?

3.1 Aspectos gerais da responsabilidade civil.

No direito brasileiro, a reparação civil dos danos foi estabelecida como direito fundamental na carta republicana, incisos V e X do artigo 5º, além de dedicar, não ignorável quantidade de artigos no Código Civil de 2002 ao tema da responsabilização. Além da atenção especial prestada ao tema pelo Código de Defesa do Consumidor.

Aproximando a discussão sobre responsabilidade civil da tenra área do direito digital, Silvio de Salvo Venosa, pensando em sintonia com tantos outros juristas, levanta a seguinte reflexão, dizendo "o direito informático" tem em suas mãos para desenvolver e "adaptar os institutos tradicionais para criar outros ligados às novas conquistas eletrônicas" (VENOSA, 218, p. 787), assim certamente o é o clássico instituto da responsabilidade civil, que como dito alhures, primitivamente admitia a retorsão imediata e a vingança privada, e chegou-se a um nível de civilidade que dá ao estado juiz a análise dos critérios constitutivos da responsabilidade.

Em que pese a dinâmica da responsabilidade civil no ambiente cibernético, em diversos aspectos, se assemelhar a responsabilização civil no foro tradicional, e nas lições triviais de direito, encará-la tendo como pressuposto o meio cibernético e especialmente os crimes digitais nos fará compreender algumas complexidades peculiares.

Na mesma linha de pensamento Patrícia Peck Pinheiro (2016, p. 513) diz que "a responsabilidade civil é um instituto em transformação no contexto da sociedade digital", à medida que os valores que devem prevalecer, e ser protegidos no ambiente impessoal da internet, estariam sendo reordenados para contemplar a singularidade do ambiente informacional enquanto "território global e atemporal".

Aprioristicamente falando, há que se concordar com Sílvio Venosa (2018, p. 787) quando diz que "qualquer que seja o caminho a ser seguido, não se foge dos princípios tradicionais da responsabilidade" ou seja, os digitalistas não vão como se diz no jargão "inventar a roda". O instituto jurídico existente precisa, contudo, ser pensado e adaptado às exigências do novo ambiente em que deve ser aplicado. De fato, o fundamento da responsabilidade civil no ambiente natural como no ambiente informacional se pauta nos conceitos clássicos de ato culposo, nexo causal e dano, como ensina o eminente mestre Sílvio Venosa.

Acrescenta-se a isto, que no direito tradicional tais elementos são classicamente analisados à luz de duas principais teorias, a saber: "a teoria da culpa e a teoria do risco.

Patrícia Peck Pinheiro pontua que para "o Direito Digital, a teoria do risco tem maior aplicabilidade" e explica esta pressuposição apontando a origem da teoria como sendo a era da industrialização, e expondo que a mesma surgiu para "resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações" (PINHEIRO 2016, p. 514).

Lançadas estas bases, contudo, é preciso aproximar nossa discussão da temática de fundo. Em casos da prática de crime em uma das múltiplas modalidade de *Phishing*, qual a responsabilidade das empresas que tem suas marcas indevidamente utilizadas, ou seu Servidor DNS invadido.

3.2 Responsabilidade civil e crimes cibernéticos

Do instituto clássico da responsabilidade civil exsurgem as clássicas teses de defesa conhecidas como culpa exclusiva da vítima e culpa de terceiro. De fato, tais teses defensivas são convenientes e capazes de afastar a responsabilidade objetiva daquele que não deu causa à lesão a bem jurídico, e neste pisar, enxergamos a problemática da responsabilidade no que toca ao *Phishing*.

Mas afinal, podem as empresas em todo e qualquer caso de uso irregular de suas marcas, ou na invasão para sequestro de dados e computadores alegar essas exculpantes? Pela construção lógica do Art. 14, § 3º, II, do Código consumerista o fornecedor de serviços só não será responsabilizado quando provar, por exemplo, a culpa exclusiva do consumidor ou de terceiro.

As referidas dinâmicas criminosas descritas neste escrito inauguram importante desafio para a responsabilização civil. Por razões de justiça (moral e legal), os únicos agentes que cometem dano no contexto de *phishing* são os fraudatários que se passaram pela empresa ou marca, ou que sequestram dados e máquinas.

Assim, não obstante, as lições tradicionais de direito civil, em que as empresas têm sua responsabilização alargada, o que chamamos responsabilidade civil objetiva, corolário da teoria do risco, a pessoa fraudada não vai encontrar no instituto da responsabilidade civil um amparo, visto que não poderá cobrar da empresa (vendedora apenas aparente), pelo prejuízo que sofreu, e que muitas vezes os fraudadores dificilmente serão identificados, ficando a vítima absolutamente sem meios.

É interessante pontuar que Venosa (2016, p. 453) se refere à teoria do risco como teoria do "risco criado" e explica que "o que se leva em conta é a potencialidade de ocasionar

danos; a atividade ou conduta do agente que resulta por si só na exposição a um perigo". Pois bem, cada atividade empresarial possui peculiaridade e expõe quem as pratica (trabalhador da empresa) e quem é por elas afetada (a sociedade) a certos riscos, e por óbvio não é razoável pensar que o simples fato de ter uma empresa online seja expor pessoas ao risco de serem fraudadas com usos irregular do nome de sua loja online, *verbi gratia*. No entanto, na internet o risco muitas vezes não decorre propriamente na natureza da empresa ou não guarda qualquer nexo com a própria atividade empresarial, ficando a vítima da fraude, ainda por este argumento, a ver navios.

A reflexão sobre responsabilidade civil e golpes digitais nos leva a outra problemática. Não serem alcançadas pela responsabilização civil nos casos clássicos de *phishing*, não exime as empresas de promover parâmetros éticos civilizacionais por meio de sua atuação, possibilitando uma ciberconvivência mais segura, e transações confiáveis.

Não obstante a conclusão a que chegamos pela argumentação até então expendida, vislumbramos que caberia responsabilização civil por parte de instituições empresas em algumas hipóteses. Para tecer esta consideração separemos dois tipos de empresas para lê-las à luz da responsabilidade civil. De um lado empresas que possuem boas práticas de segurança na internet; de outro, empresas que são relapsas apesar de atuarem na internet.

Como dissemos, na maioria dos casos é perfeitamente legítimo que empresas e instituições aleguem culpa de terceiro ou exclusiva da vítima como exculpantes processuais. Contudo, cremos que seria salutar que, para além de afastar a responsabilidade objetiva, sempre que uma empresa seja notificada quanto ao cometimento de um cibercrime através do uso irregular de sua marca ou invasão de seus servidores com roubo de dados de usuários, a mesma fosse chamada a demonstrar as medidas de segurança virtual que promove e demonstrar que tipo de medida pretende implementar para reforçar a proteção às suas marcas e distintivos, ou mesmo o reforço de segurança a ser promovido em sua segurança de rede.

Quanto ao segundo grupo, empresas relapsas no quesito segurança de rede, partido do pressuposto da promoção de uma ética civilizada no ambiente virtual, entendemos que é dever do poder público estimular ao máximo que empresas promovam boas práticas em cibersegurança, o que inclui a vigilância sobre sua própria marca, e proteção aos seus servidores e sua intranet.

Neste sentido, inclinamo-nos inclusive a eventual sustentação de teses de responsabilização das empresas em ambiente virtual, quando comprovada negligência no ambiente virtual, mesmo que diante de culpa de terceiro fraudador, especialmente em casos de fraudes internas através dos servidores da referida empresa, isto é quando, por meio de

Phishing Pharming ou *Phishing por Ransomware* fraudatário atingem vitimas, por negligência da empresa no cuidado e proteção de seus domínios e máquinas, a empresa relapsa deveria ser responsabilizada objetivamente, como medida que de reforço às boas práticas em cibersegurança.

A almejada segurança virtual é uma construção coletiva, que amalgama todos os ciberagentes, e neste sentido passamos a nos servir do espírito por trás do relatório da UNESC "As pedras angulares para a promoção de sociedades do conhecimento inclusivas, que exploraremos um pouco a seguir", com o intuito de refletir sobre outros mecanismos de proteção individual contra ciberfraudes.

À guisa de arremate, sintetizemos o argumento. Por um lado, o Estado deve exigir que empresas, e instituições em geral, inclusive entidades públicas, adotem procedimentos que reforcem a segurança no ambiente virtual, a lei em sentido amplo deve exigir isso dos agentes que tem capacidade técnica para promover boas práticas. Além disso, necessário e indispensável um esforço dos próprios agentes no sentido de se construir mecanismos de precaução contra cibercrimes.

Doutro giro, apenas exigências estatais e boas práticas da parte de pessoas jurídicas não responde a toda a questão. Acreditamos que é necessário um nível de intervenção cultural que passa essencialmente pelo que a Unesco vem chamando de "alfabetização midiática e informacional". A sociedade mais protegida é aquela em que mais agentes podem de *per si*, ser fatores que ampliam a segurança, a isto as nações unidas chamam de empoderamento do indivíduo. Focamos nisso no tópico seguinte.

4 A ALFABETIZAÇÃO MIDIÁTICA INFORMACIONAL COMO FERRAMENTA DOS INDIVÍDUOS CONTRA O *PHISHING*

Pelo que trouxemos até aqui fica evidente a necessidade de fomentar uma cultura dentro das instituições, públicas e privadas, que privilegie a ênfase na proteção de dados, evitando-se os efeitos nefastos da ciberpescaria; quer nas modalidades que visam atingir a vítima em suas finanças, quer nas que focam em sequestro de dados e máquinas. De sorte que, como primeira camada de proteção ao indivíduo, já viemos sinalizando para a necessidade de responsabilização civil de organizações relapsas com a questão da segurança de suas marcas e dos dados armazenados em seus bancos de dados.

Outra dimensão da mesma problemática, que cumpre abordar agora, como prenunciado, é a capacitação do usuário, aqui enfocado como indivíduo, para que o mesmo se torne um elemento a somar na segurança do ambiente virtual. Isto parte da premissa de que indivíduos mais preparados para atuar no ambiente cibernético dificilmente estariam suscetíveis a serem vitimados por crimes cometidos através de iscas, como as usadas nas diversas modalidades de *phishing*. Bem como que, se os indivíduos forem cuidadosos, adotando posturas de segurança recomendadas por especialistas, podem ampliar a segurança de sua própria usabilidade dos meios digitais.

Para prosseguir com a abordagem da capacitação dos indivíduos, lançaremos mão de importante estudo realizado pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) denominado "as pedras angulares para a promoção de sociedades do conhecimento inclusivas: acesso à informação e ao conhecimento, liberdade de expressão e ética na Internet global" (UNESCO, 2017).

Num primeiro momento, pede-se licença para fazer comentários breves e gerais, sobre o relatório em si, a seguir retomando o ponto da capacitação dos indivíduos. Para a cominação do referido documento, aquele importante organismo internacional protagonizou relevante estudo que contou com a colaboração de diversos atores espalhados pelo mundo, e eminentemente, sua análise possui natureza multissetorial. Ali, parte-se de alguns paradigmas, lá referidos como "pedras angulares", expressão adotada para designar os grandes temas que delimitam o estudo. São "pedras angulares" para a promoção de sociedades do conhecimento inclusivas, segundo o referido estudo o acesso à informação e ao conhecimento, liberdade de expressão e ética na Internet global.

O todo daquele documento gira em torno da ideia da construção desta "sociedade do conhecimento", e favorece a premissa do ambiente virtual como meio que possibilita esta experiência, sendo um amalgama entre povos e culturas diversos. Deste modo as pedras fundamentais, ali lançadas, visam erguer como edifício final uma sociedade do conhecimento.

Retornando, pois, à capacitação dos indivíduos, ao refletir sobre a construção desta sociedade, o relatório traz uma expressão muito pertinente: "alfabetização midiática e informacional", também referida pela sigla: "AMI". Nesse sentido, para a UNESCO (2017), é preciso ir além do acesso, isto é, é preciso transcender a mera implementação de infraestruturas físicas de rede ou a simples garantia de que os indivíduos possam se conectar à Internet. Se o objetivo é uma sociedade do conhecimento é preciso olhar além:

> O acesso ao conhecimento implica em ambientes formais e informais de educação. Também envolve a promoção de competências de alfabetização midiática e

> informacional (AMI) que permitam que usuários se empoderem e façam uso pleno do acesso à Internet. (UNESCO, 2017)

Na constatação do estudo as inovações técnicas estão modificando os modelos tradicionais de negócios e organizações, bem como o próprio emprego, além disto, na mesma medida, a mídia digital tem tomado o lugar de diversas tecnologias, que até pouco tempo eram individualizadas no correio, no telefone e da mídia de massa (veículos de impressa, por exemplo), o advento de novas tecnologias teve como impacto, entre outras cosias, a defasagem de políticas e regulamentações, o que leva a que regulamentos potencialmente inadequados sigam em vigor, e consequentemente, não se conseguem integrar novas soluções como a AMI, expõe o documento da UNESCO (2017).

Isto quer dizer que, apesar das profundas mudanças promovidas pelo contexto cibernético, muitos Estados e sociedades ainda não tomaram pé da necessidade de adaptação e capacitação de cidadãos comuns através de meios de educação formal e informal que possibilitem o que o relatório chama de alfabetização midiática informacional.

Em outras palavras, há em diversos lugares, e sem dúvida é o caso de muitos lugares no Brasil, imenso vácuo de inserção qualificada de indivíduos no ambiente virtual. Muito se tem progredido em uma das pedras fundamentais da Unesco, o chamado “acesso”, mas, há sério prognóstico de que este acesso não tem vindo acompanhado de educação para o uso do ambiente digital.

Ao nos depararmos com um contexto de ampliação do acesso à rede mundial de computadores, inclusive muito impulsionada pela popularização de smartphones, e aproximar isso da constatação da UNESCO, de que o acesso não tem vindo acompanhado de ampliação do acesso a conhecimento especial voltado para o empoderamento do indivíduo no meio digital, ficamos perplexos com como isso tem potencial para ampliar e muito a base de atuação de ciberpescadores.

Patrícia Peck Pinheiro endossa nossa perplexidade ao salientar que dois são os problemas dos quais decorre o crescimento de fraudes eletrônicas no Brasil, a doutrinadora diz que isto é uma associação entre “a falta de conhecimento do usuário sobre segurança da informação, tornando-se vítima fácil dos golpes digitais” (PINHEIRO,2016, p. 396), e a escassez de recursos humanos e arcabouço tecnológico para as autoridades públicas competentes, que segundo seu diagnóstico, carecem de treinamento voltado à “prevenção desses crimes e também para condução de investigações apropriadas que possam ter maior resultado na punição dos criminosos.”

Endossa também nossa perplexidade, dados como os levantados por Kaspersky (2018), em que se aponta que brasileiros são maiores vítimas de golpes *phishing* no mundo. Segundo dados da Kaspersky (2018), seu serviço de segurança cibernética bloqueou em 2017 quase 37 milhões de ataques na América Latina e nos primeiros 7 meses do ano de 2018 foram mais de 40 milhões de bloqueios. Esses números, apenas de uma das muitas empresas de segurança cibernética são ilustrativo da dimensão hercúlea do problema que são as tentativas de fraude envolvendo iscas digitais pelo mundo. Imagine-se quantas outras iscas não são disseminadas, quantas outras são bloqueadas por outros dispositivos de segurança, e quantas acabam chegando a seus alvos finais.

Se por um lado a visão parece desnorteadora, mas uma vez recorremos às ideias de Patrícia Peck Pinheiro quanto à correlação entre o aumento desenfreado de crimes e a ausência de presença de alfabetização midiática e informacional como fator de exposição dos indivíduos, e mais ainda não é outra sua opinião, senão que "a melhor maneira de combater o crescimento das fraudes eletrônicas ainda é por meio da conscientização dos usuários, que representam a linha de frente da defesa" (PINHEIRO, 2016, p. 396).

Isto é consonante com o relatório da UNESCO (2017), a tese central com a qual este artigo converge é que os usuários, por representarem esta linha de defesa precisam ser capacitados para tanto, e por isso explorar mais a temática da alfabetização midiática e informacional é importante, com a finalidade de reforçar políticas de fomento. Enfatizando que o próprio relatório evoca a ideia de uma composição entre educação digital formal e informal como proposta de alfabetização midiática e informacional.

Logo, é válido salientar que o Marco Civil da Internet (Lei 12.965/14) aponta como o Estado deve atuar no que concerne ao fomento da internet no país, frisando em seu artigo 26 a promoção da educação digital, ao salientar que:

> O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico. (BRASIL, 2014, n.p)

Note-se que a lei relembra ao Estado, que o ele tem o dever constitucional de promover a educação. A educação está em mudança, com os novos paradigmas e novas tecnologias, a pandemia da Covid-19 que o diga, pelo que urge que o Estado constitucionalmente regido promova a prestação da educação, também nos novos níveis de exigência que a vida moderna trouxe consigo.

O legislador foi mais além para atrelar ao estado a obrigação pela educação formal "em todos os níveis de ensino", visando à finalidade de capacitar os cidadãos para um "uso

seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico" (BRASIL, 2014, n.p).

Na mesma senda, e muito vinculado ao anseio que emana do relatório da UNESCO, entendemos que tal como reza a constituição da república em seu Art. 205, a educação é um dever sim do Estado, portanto, não seria diferente na educação digital. Mas também a Constituição chama as famílias a participarem desta educação, bem como o texto constitucional diz que a educação "será promovida e incentivada com a colaboração da sociedade" (BRASIL, 1988, n.p).

Assim entendemos que a alfabetização midiática e informacional deveria ser largamente incentivada por todos os agentes sociais, quer estatais quer privados; visando à construção de um ambiente cibernético mais seguro e eficaz na contenção de cibercriminosos.

5 CONSIDERAÇÕES FINAIS

O presente trabalho, portanto, conclui que por sua complexidade e pelo perfil diverso de vítimas que a ciberpescaria pode atingir não se pode ignorá-la. Há que se lançar mão de todas as ferramentas possíveis de dissuasão deste tipo de prática.

No tocante à forma como as empresas que interagem com os meios digitais devem proceder, demonstrou-se que em que pese a responsabilidade das empresas, via de regra, seja afastada nos casos de *phishing*, pela incidência do instituto da culpa exclusiva de terceiro, é preciso amadurecer o instituto da responsabilização civil no âmbito digital, para atingir as pessoas jurídicas que sejam relapsas com suas marcar, com os dados de usuários e mesmo com suas redes internas.

É importante dizer que não só de pessoas jurídicas de direito privado devem ser cobradas atitudes cautelosas no meio digital, cada dia mais a sociedade confia a organizações, empresas e órgãos públicos, dados que vem sendo acumulados, podendo a qualquer instante se tornar alvo de criminosos. A proteção a esses dados é imperiosa e deve ser parte da cultura de cada organização, governamental ou não governamental. A legislação deve ser aperfeiçoada tanto para exigir que protocolos de cibersegurança vigorem, como também para punir instituições relapsas.

Além disto, considerando, que pessoas físicas são frequentemente alvos fáceis dos cibercriminosos, conclui-se que a alfabetização midiática e informacional é uma iniciativa que

viabilizaria o fomento de uma cultura digital, que tornaria a sociedade mais preparada para lidar com os meios digitais sem cair em golpes. Sólido é o argumento, de que o indivíduo é um parceiro impreterível na promoção da cibersegurança. Portanto, Estado e demais agentes da sociedade devem se unir para promover a proliferação de competências digitais (alfabetização midiática e informacional), para que o usuário comum possa se esquivar de fraudadores.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 15 set. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.> . Acesso em: 15 set. 2020.

LÉVY, Pierre. **Cibercultura**. São Paulo: Saraiva, 2017.

KASPERSKY. **Brasileiros são maiores vítimas de golpes *Phishing* no mundo**. Cidade do Panamá, Panamá, 13 ago. 2018. Disponível em: <https://www.kaspersky.com.br/blog/*Phishing* -klsec-brasil-assolini/10642/?utm_source=newsletter&utm_medium=Email&utm_campaign=kd%20weekly%20digest>. Acesso em 19 out. 2020.

MALWAREBYTES. **Tudo sobre *Phishing*** . Disponível em: <https://br.malwarebytes.com/*Phishing* /#Types-of-*Phishing* -attacks>. Acesso em 10 set. 2020.

SANTINO, Renato. Ransomware que afeta STJ já atingiu empresas e governos fora do Brasil. **Olhar Digital**. São Paulo, 11 Nov. 2020. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/ransomware-que-afeta-stj-ja-atingiu-empresas-e-governos-fora-do-brasil/109866>. Acesso em 11 Out. 2020.

PINHEIRO, Patricia Peck. **Direito Digital**. São Paulo: Saraiva, 2016.

STIVANI, Mirella. **Os dez tipos de phishing mais comuns**. Disponível em: <https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml>. Acesso em 10 Set. 2020.

UNESCO. As pedras angulares para a promoção de sociedades do conhecimento inclusivas: acesso à informação e ao conhecimento, liberdade de expressão, privacidade, e ética na

Internet global.**UNESCO. Paris. 2018** Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000260742/PDF/260742por.pdf.multi>. Acesso em 03 Out. 2020.

VENOSA, Sílvio Salvo. **Direito Civil - Vol. 2 - Obrigações e Responsabilidade Civil**, 18. ed. São Paulo: Atlas, 2018.