GIULIA GABRIELE REZENDE

O PHISHING E A RESPONSABILIDADE EMPRESARIAL: ASPECTOS SOBRE AS MEDIDAS PROTETIVAS DO EMPRESÁRIO FACE AO PREJUÍZO DE SEUS USUÁRIOS

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO
Uberlândia - MG
2022

O PHISHING E A RESPONSABILIDADE EMPRESARIAL: ASPECTOS SOBRE AS MEDIDAS PROTETIVAS DO EMPRESÁRIO FACE AO PREJUÍZO DE SEUS USUÁRIOS

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Uberlândia.

Orientador: Prof. *Dr. Almir Garcia Fernandes*

Uberlândia - MG

2022

Sumário

INTRODUÇÃO

O *phishing* é uma forma de ciberataque comum atualmente que utiliza da imagem de empresas conhecidas para obter os dados de clientes e, até mesmo, de seus funcionários. Nele, o criminoso envia mensagens aos clientes ou funcionários de uma determina empresa, seja por *e-mail* ou *Whatsapp*, por exemplo, de forma que o receptor seja levado a erro e passe a ofertar seus dados para o fraudador, inclusive contaminando seus dispositivos de *hardware* com vírus, tais como os *malwares*.

Muito se diz acerca da proteção do consumidor contra esse tipo de crime, observando-se diplomas legais que determinam a responsabilização das organizações que ofereceram o serviço, face à pouca existência de trabalhos que abordem os danos sofridos pelas empresas, que também foram vítimas de um ataque e, ainda assim, devem ressarcir seus clientes pelos danos ocorridos, ainda que não causados por suas ações.

Assim, observa-se que também há dano gerado à organização, principalmente se consideradas as indenizações a ela atribuídas e a dificuldade de se encontrar o responsável pelo ataque. Por esta razão, é necessário que se observe os meios de proteção destas personalidades jurídicas responsáveis pelo fornecimento do produto.

Assim sendo, este trabalho possui como objetivo tratar as consequências geradas pelo *phishing* à empresa que tem sua identidade reproduzida, delimitando providências que podem ser tomadas antes e após o ataque, tendo em vista o prejuízo de seus usuários e as possíveis decorrências jurídicas a serem enfrentadas.

Neste artigo, os problemas a serem discutidos são a extensão da responsabilidade pelo *phishing* à sociedade empresária, as formas de mitigação dos riscos de ocorrência do ataque, as consequências de se atribuir toda a responsabilidade à empresa e a possibilidade de atribuição da responsabilidade a outra figura caso realizadas medidas preventivas.

Será utilizado como método de pesquisa o indutivo, a saber, aquele destinado a verificar constatações particulares e, possibilitar, que se produzam generalizações sobre o tema, além do método dedutivo, na tentativa de se fazer das regras gerais, a solução para casos específicos.

Os processos metodológicos a serem utilizados serão o estudo dogmático jurídico, visto a impossibilidade de um estudo profundo sem que se recorra à lei, à doutrina ou à jurisprudência neste sentido; o estudo de casos, especialmente aqueles referentes a ataques sofridos por instituições bancárias e *e-commerces*; comparativo, analisando e relacionando diferentes casos.

CAPÍTULO I – O PHISHING

Kevin Mitnick foi um hacker que passou a trabalhar na área de segurança contra crimes cibernéticos após sua liberação da prisão pelo cometimento desses mesmos delitos. O principal enfoque dos seus trabalhos reside na área de engenharia social, que é definida por ele da seguinte forma: "A Engenharia Social usa influência e persuasão para enganar pessoas ao convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou por manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter informações com ou sem o uso de tecnologia." (MITNICK e SIMON, 2003, p. 6)

Desta maneira, pode-se dizer que a engenharia social é uma estratégia de ciberataque cuja defesa independe do uso de mecanismos técnicos, como os antivírus, haja vista que o alvo, ou seja, o usuário, é o elemento mais suscetível a fornecer os dados de interesse sem que seja preciso um trabalho para realizar a quebra de mecanismos de segurança.

Aqui, portanto, evidencia-se que o *phishing* é justamente uma modalidade de engenharia social, que consiste no uso pelo criminoso da figura de determinada pessoa ou instituição para adquirir dados e informações pessoais da vítima. Dessa maneira, o foco não reside na vulnerabilidade do sistema, mas sim na vulnerabilidade do próprio usuário, que, na maioria das vezes, é leigo e não possui condições de identificar o ataque.

Esse cibercrime é uma das formas mais comuns de ataque cibernético ocorridas na atualidade conforme estudos de diversas organizações. Nesse sentido, considera-se a pesquisa realizada pela *Osterman Research*[1], que informa 84% das organizações dos Estados Unidos já teriam sofrido alguma forma de ataque, ameaça de *phishing* ou *ransomware* desde 2020. Além disso, conforme estatísticas apresentadas pela *Internet Crime Complaint Center* (IC3), organização que integra o *Federal Bureau of Intelligence* (FBI), 241.324 dos ataques informados pelas vítimas foram identificados como a modalidade estudada, de modo que o prejuízo totalizado se deu no valor de US$ 51.241.075,00[2].

A forma mais comum de *phishing* ocorre por meio de *e-mail*, enviado de forma que seja similar àqueles provenientes de fontes confiáveis, como a *Microsoft*, a *Google* e a *Amazon*, com conteúdo e modelo que seguem o padrão daqueles enviados por estas organizações. Aqui, o

---

[1] OSTERMAN RESEARCH. **How to Reduce the Risk of Phishing and Ransomware**. Disponível em: https://resources.trendmicro.com/Osterman-Email-Security-WP.html. Acesso em: 06 jul. 2021.

[2] INTERNET CRIME COMPLAINT CENTER. **Internet Crime Report**. 2020. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Acesso em: 06 jul. 2021.

indivíduo abre o *e-mail* e acessa o arquivo anexado, permitindo o acesso do criminoso às informações desejadas.

Esta modalidade pode ocorrer tanto dentro do ambiente corporativo quanto em relação aos clientes da empresa. Internamente, são enviados *e-mails* maliciosos aos funcionários da organização, que, ao acessar o conteúdo enviado, permitem o vazamento de dados sensíveis da entidade que fazem parte, assim como as próprias informações, resultando no uso inadequado desses dados e até mesmo na perda deles. Esse tipo de *phishing*, conhecido como *Business Email Compromise*, é um dos mais dispendiosos, resultando geralmente em prejuízos de US $5.01 milhões por vazamento, conforme pesquisa realizada pela IBM[3].

Já no aspecto externo, considera-se o envio de *e-mails* para clientes ou possíveis clientes da empresa, que acessam o anexo acreditando pertencer à fonte confiável e sofrem com o ataque que usualmente resulta em perda financeira. De maneira geral, para realizar esse tipo de ataque é simulado o endereço de *e-mail* da instituição, com diferenças de caracteres que não são identificados caso não sejam observados com atenção.

Não obstante, em relação também a terceiros, pode-se ocorrer uma situação na qual se torna mais delicada a identificação do ataque, que se dá quando o criminoso simula o ambiente de compras da empresa e tem acesso às informações bancárias do consumidor, que realiza o pagamento na plataforma e não recebe a contraprestação esperada.

Observado o disposto acima, passo a discorrer sobre o enquadramento legal do *phishing* no ordenamento jurídico brasileiro. A princípio, para que seja realizada esta análise é importante ressaltar que essa modalidade de ataque possui como alvo o usuário, e não o computador em si, ou seja, ainda que seja utilizado o elemento virtual como instrumento para a obtenção da vantagem desejada, a fraude é realizada contra o indivíduo.

Nesse sentido, o Código Penal brasileiro traz o crime de estelionato definido da seguinte forma:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Nota-se aqui como no *phishing* o fraudador obtém vantagem ilícita, seja por meio dos dados captados ou pelo pagamento realizado para destinatário diverso daquele que o usuário

[3] IBM. **X-Force Threat Intelligence Index**. Disponível em: https://www.ibm.com/downloads/cas/M1X3B7QG. Acesso em: 07 jul. 2021.

inicialmente pretendia, por meio da indução deste indivíduo a erro, utilizando para isso *e-mail*, *site* ou qualquer outro ambiente digital que pareça pertencer a fonte confiável. Assim sendo, este crime já poderia ser enquadrado na hipótese prevista pelo artigo supracitado, ou seja, de estelionato.

Não obstante, de modo a evitar eventuais discussões acerca da tipificação penal do crime de *phishing*, o legislador realizou a especificação deste crime por meio da Lei nº 14.155/2021, acrescendo ao artigo acima os parágrafos 2º e 3º as disposições referentes à fraude eletrônica desta maneira:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, **se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo**.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

O *phishing* é, portanto, figura já reconhecida pelo ordenamento jurídico brasileiro com sanção penal devidamente determinada àquele que o praticar, devido aos potenciais e significativos danos a ele relacionados, conforme apresentado por diversos relatórios institucionais.

No Brasil, inclusive, a pandemia causada pelo Covid-19 e o aumento das relações comerciais feitas pelo meio virtual impulsionou a ocorrência desse crime em 41%[4], tornando o país o líder mundial em vítimas de *phishing*.

Visto esse panorama geral, torna-se possível observar os reflexos deste crime no âmbito civil, principalmente no que tange às empresas, haja vista que são os principais alvos dessa prática, seja como meio empregado para obter vantagem ou como vítima direta.

---

[4] R7. **Ataques por phishing no Brasil crescem 41% em 2021**. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/ataques-por-phishing-no-brasil-crescem-41-em-2021-12122021. Acesso em: 05 fev. 2022.

CAPÍTULO II – A EMPRESA

Muito se diz acerca da importância da proteção do indivíduo hipossuficiente face às empresas, *lato sensu*, contudo, não se deve deixar de observar a relevância delas para a sociedade em diversos aspectos.

Em primeiro lugar, é primordial que seja observado o princípio da função social da propriedade, previsto pelos artigos 5º, XXIII e 170, III da Constituição Federal de 1988, que determina a necessidade de os bens deverem se prestar a promover os interesses da sociedade. Nesse sentido, a propriedade do empresário também deve obedecer a tal princípio, do qual decorre, portanto, o princípio da função social da empresa, conforme menciona André Santa Cruz (2019, p. 48):

> Assim, quando se fala em função social da empresa faz-se referência à atividade empresarial em si, que decorre do uso dos chamados bens de produção pelos empresários. Como a propriedade (ou o poder de controle) desses bens está sujeita ao cumprimento de uma função social, nos termos do art. 5º, inciso XXIII, da CF/1988, o exercício da empresa (atividade econômica organizada) também deve cumprir uma função social específica (...)

Também, define Fábio Ulhôa Coelho (2012, p. 89) a função social da empresa da seguinte maneira:

> Cumpre sua função social a empresa que gera empregos, tributos e riqueza, contribui para o desenvolvimento econômico, social e cultural da comunidade em que atua, de sua região ou do país, adota práticas empresariais sustentáveis visando à proteção do meio ambiente e ao respeito aos direitos dos consumidores. Se sua atuação é consentânea com estes objetivos, e se desenvolve com estrita obediência às leis a que se encontra sujeita, a empresa está cumprindo sua função social; isto é, os bens de produção reunidos pelo empresário na organização do estabelecimento empresarial estão tendo o emprego determinado pela Constituição Federal.

Tende-se a tratar as empresas meramente como estruturas com objetivo de obter lucro, o que não deixa de ser verdade, apesar de essa não ser sua única finalidade. A princípio, é necessário considerar que as empresas podem ser definidas como estruturas propulsoras do desenvolvimento social e econômico. Elas proporcionam avanço tecnológico, geração de riquezas e de empregos, de forma que não só os indivíduos que se encontram no controle das organizações são beneficiados por elas, mas também a população em geral.

Dessa maneira, ainda que a geração de lucro seja sua intenção final, os meios empregados para tanto ensejam em um desenvolvimento geral para a sociedade.

Nesse sentido, veja que o próprio Direito do Trabalho consagra diversos princípios par a proteção do trabalhador, como o da continuidade do emprego[5], e, no entanto, justamente com base nele permite a flexibilidade de outros princípios estabelecidos, como o que ocorre com a exceção ao princípio da irredutibilidade salarial previsto pelo art. 503 da Consolidação das Leis Trabalhistas, em que é possibilitada a redução dos salários em até 25% em caso de "força maior ou prejuízos devidamente comprovados".

O preceito acima mencionado coaduna com o princípio da preservação da empresa, uma concepção doutrinária que visa a proteção da atividade de empresa, além do próprio empresário. Em razão dele, diz Fábio Ulhôa (2012, p. 93) que

> O princípio da preservação da empresa reconhece que, em torno do funcionamento regular e desenvolvimento de cada empresa, não gravitam apenas os interesses individuais dos empresários e empreendedores, mas também os metaindividuais de trabalhadores, consumidores e outras pessoas; são estes últimos interesses que devem ser considerados e protegidos, na aplicação de qualquer norma de direito comercial.

Isso se dá porque são justamente essas unidades de produção que possibilitam a existência dos empregos e a consequente subsistência da população em geral, devendo a lei também, portanto, garantir um certo equilíbrio e fornecer mecanismos para permitir a manutenção do funcionamento dessas organizações, conforme demonstrado anteriormente. Por exemplo, no que diz respeito aos princípios do Direito do Trabalho anteriormente citados, estes são balanceados de modo que a existência da empresa seja preservada, haja vista que no caso do seu encerramento diversos empregos deixariam de existir.

Nesse mesmo sentido, Coelho (2012) menciona o princípio do impacto social da crise da empresa, pelo qual se passa a considerar a empresa não como uma entidade por si só, mas também por todas as figuras que são afetadas direta ou indiretamente pelos resultados que a empresa obtém. Aqui, verifica-se que os reflexos são sentidos também pelos parceiros comerciais, pelo Estado, por meio do fisco, pelos trabalhadores da instituição, pelos consumidores e por toda a sociedade em geral. Por esse motivo, o autor mencionado ressalta o seguinte:

---

[5] "Princípio da Continuidade da Relação de Emprego — Informa tal princípio que é de interesse do Direito do Trabalho a permanência do vínculo empregatício, com a integração do trabalhador na estrutura e dinâmica empresariais. Apenas mediante tal permanência e integração é que a ordem justrabalhista poderia cumprir satisfatoriamente o objetivo teleológico do Direito do Trabalho, de assegurar melhores condições, sob a ótica obreira, de pactuação e gerenciamento da força de trabalho em determinada sociedade". (DELGADO, 2019, p. 245)

> Em razão do impacto social da crise da empresa, sua prevenção e solução serão destinadas não somente à proteção dos interesses do empresário, de seus credores e empregados, mas também, quando necessário, à proteção dos interesses metaindividuais relacionados à continuidade da atividade empresarial. (COELHO, 2012, p. 116)

Destarte, no que diz respeito aos crimes cibernéticos, existem diversos mecanismos para defender o usuário dos danos, sendo atribuída às empresas inclusive a responsabilidade objetiva de reparar a lesão sofrida, como se verá a seguir, assim como as diversas penalidades impostas pela Lei Geral de Proteção de Dados.

Entretanto, pouco se diz acerca dos mecanismos de proteção dessas empresas para garantir o seu funcionamento mesmo após ataques que prejudiquem a si mesma assim como aos seus usuários, como ocorre nos casos de *phishing*.

O *phishing* é um evento danoso que afeta de maneira direta as empresas, utilizando dos seus elementos de identificação, como a marca. A marca é definida no art. 122 da Lei nº 9.279/1996 como "os sinais distintivos visualmente perceptíveis, não compreendidos nas proibições legais", e suas modalidades estão definidas no artigo 123 e parágrafos do referido dispositivo legal.

Estes elementos distintivos, que podem ser visuais ou até mesmo sonoros, são protegidos pelo Direito de Propriedade Industrial, considerados bens imateriais. A sua importância é tal que expedida a patente da marca pelo INPI, o seu detentor passa a ter direito exclusivo sobre ela, sem que qualquer outro possa utilizar das suas características de modo que possa gerar uma confusão na identificação.

Nesse caso, a Lei de Propriedade Industrial define, em seu art. 189, sanção para aquele que dizer uso proibido de marca, como se vê a seguir:

> Art. 189. Comete crime contra registro de marca quem:
> I - reproduz, sem autorização do titular, no todo ou em parte, marca registrada, ou imita-a de modo que possa induzir confusão; ou
> II - altera marca registrada de outrem já aposta em produto colocado no mercado.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Essa proteção à marca garantida legalmente se dá devido à relevância de tal elemento na atividade comercial do empresário. O uso dela por um concorrente é vedado, gerando consequências jurídicas a ele, no entanto, surge aqui a possibilidade de que seja aplicada esta

penalidade também àquele que pratica o *phishing*, visto que este ataque consiste justamente no uso dos símbolos distintivos de forma a induzir confusão.

CAPÍTULO III – A RESPONSABILIDADE

Antes de se discorrer especificamente acerca da responsabilidade do controlador, é importante observar que os titulares dos dados atingidos podem ser considerados também consumidores, haja vista que são destinatários finais do serviço ou produto que envolva o uso de meios virtuais. Neste aspecto, ressalta-se que a vulnerabilidade do consumidor, aqui caracterizado como usuário, é estabelecida como um princípio regente do Código de Defesa do Consumidor[6].

Assim sendo, conforme afirmado por Rizzatto Nunes (2018), o consumidor possui uma hipossuficiência técnica, não fazendo parte da produção dos produtos e serviços, o que o deixa à mercê daquele que fornece o elemento a ser consumido com pouca ou nenhuma possibilidade de escolha. Observa-se que esta hipossuficiência se dá não apenas pela falta de alternativas a serem escolhidas, mas também pelo pressuposto de que a população em geral é leiga em relação à tecnologia.

Desta forma, no que diz respeito ao *phishing*, o Código de Defesa do Consumidor se apresenta como um instrumento que possibilita a mitigação dos danos gerados aos indivíduos em geral que são afetados pelo ciberataque. Nesse mesmo sentido, a Lei Geral de Proteção de Dados surge com o objetivo de ampliar a possibilidade de escolha do usuário no que diz respeito aos seus dados, determinando, por exemplo, a especificação dos *cookies* presentes na página da internet e, inclusive, o consentimento do indivíduo em relação ao seu uso.

Assim, entendendo-se o usuário como consumidor, parte-se à análise das teorias do risco criadas pela doutrina com o objetivo de definir as hipóteses de responsabilidade civil. A primeira delas é o risco integral, pelo qual independente de qualquer culpa o agente deve ser responsabilizado, sem possiblidade de excludente de responsabilidade.

---

[6] "Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo" (BRASIL, 1990)

Também, há o risco profissional, pelo qual o dano sofrido decorre da atividade laboral do indivíduo, de modo que o empregador deveria realizar o ressarcimento independente de culpa. Por outro lado, no risco-proveito a necessidade de indenizar vem da aferição de lucro, que geraria a necessidade objetiva de arcar com os ônus em razão dos bônus da atividade.

Enquanto isso, o risco-excepcional decorre de atividade alheia àquela habitualmente realizada pela vítima, e o risco-criado surge quando a atividade regularmente praticada pelo autor gerar por si só risco para os direitos de outrem, conforme previsto pelo art. 927, parágrafo único do Código Civil de 2002[7].

Observado o exposto, abre-se a possibilidade da aplicação da Teoria do Risco do Empreendimento[8] nas relações consumeristas, que atribui responsabilidade objetiva ao fornecedor acerca de eventuais danos causados pelo produto ou pelo serviço, ou seja, confere à empresa toda a responsabilidade pelo evento do ponto de vista do consumidor.

Conforme afirma a parte da doutrina que adota esta teoria, ao iniciar o negócio, o fornecedor fica sujeito aos riscos dele imediatamente, realizando todas as análises necessárias acerca do balanceamento entre os riscos e a possibilidade de lucro. Dessa maneira, a ameaça de eventuais prejuízos estaria embutida na receita obtida na comercialização, sendo que o defeito, portanto, seria do produto, não cabendo sequer uma análise da presença ou não de culpa do fornecedor.

Em relação ao ordenamento brasileiro, conforme expõe Tartuce e Neves (2017, p. 156),

> o CDC adotou expressamente a ideia da teoria do risco-proveito, aquele que gera a responsabilidade sem culpa justamente por trazer benefícios, ganhos ou vantagens. Em outras palavras, aquele que expõe aos riscos outras pessoas, determinadas ou não, por dele tirar um benefício, direto ou não, deve arcar com as consequências da situação de agravamento. Uma dessas decorrências é justamente a responsabilidade objetiva e solidária dos agentes envolvidos com a prestação ou fornecimento.

---

[7] "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem." (BRASIL, 2002)

[8] "Nosso conceito de risco do empreendimento está ligado à ideia de responsabilidade ou encargo acerca da perda ou dano por situação de risco, no ato de uma pessoa - física ou jurídica -, que assume uma tarefa ao empreender uma atividade econômica, na qual está ínsita a probabilidade de insucesso, em função de acontecimento eventual, incerto, cuja ocorrência não dependa exclusivamente da vontade dos interessados. Nestes termos, esta é a responsabilidade que, independentemente de culpa, assumem todos aqueles que se disponham a exercer uma atividade no mercado de consumo, atraindo para si o dever de responder pelos eventuais vícios ou defeitos dos produtos ou serviços postos à disposição dos consumidores." (WOLKOFF, 2009)

Em contraponto, ainda que o Código de Defesa do Consumidor consagre a responsabilidade objetiva do fornecedor, alguns doutrinadores são críticos à teoria do risco, apontando-a como prejudicial, de modo que seria possível de se pensar na sua não aplicação neste caso. Venosa (2018, p. 456) afirma que

> Essa norma da lei mais recente transfere para a jurisprudência a conceituação de atividade de risco no caso concreto, o que talvez signifique perigoso alargamento da responsabilidade sem culpa. É indiscutível a conveniência, ao menos na atualidade, de uma norma genérica nesse sentido. Melhor seria que se mantivesse ainda nas rédeas do legislador com norma descritiva a definição das situações da aplicação da teoria do risco (...)

Por conseguinte, observa-se que a responsabilidade escolhida pela legislação brasileira, apesar de críticas existentes, é objetiva. Ainda assim, deixada de lado a análise acerca da possibilidade de responsabilidade subjetiva, resta a discussão acerca da possibilidade de excludente da responsabilidade devido a fato de terceiro, conforme definido pela doutrina e pela lei.

Sabe-se que o Código de Defesa do Consumidor não adota a teoria do risco integral, de modo que a responsabilização do fornecedor não se dá independentemente do nexo de causalidade e da atividade de terceiros. Dessa maneira, o ordenamento jurídico estabelece hipóteses em que é possível a exclusão da responsabilidade do fornecedor, estando elas dispostas nos arts. 12, §3º e 14, §3º do CDC:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:
> I - que não colocou o produto no mercado;
> II - que, embora haja colocado o produto no mercado, o defeito inexiste;
> III - a culpa exclusiva do consumidor ou de terceiro.
> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.

Em relação ao *phishing*, tendo a empresa tomado as medidas de segurança estabelecidas pela Lei Geral de Proteção de Dados, trata-se de um evento em que está caracterizada a hipótese do art. 12, §3º, III e do art. 14, §3º, II acima mencionados. Isto porque, como já dito anteriormente, esta modalidade de ciberataque possui uma característica particular em que é explorada a vulnerabilidade do usuário, sem que seja atacada a empresa em si, mas sim os indivíduos que fazem uso do seu produto.

Nesse sentido, ressalto os apontamentos de Fábio Ulhôa Coelho (2012, p. 391):

> Na verdade, o fornecedor real ou presumido, demandado por defeito do produto, deixará de ser responsabilizado se provar uma das hipóteses aventadas pelo art. 12, § 3º, do CDC. Isto é, a ilegitimidade passiva, a inexistência do defeito ou a culpa exclusiva do consumidor ou de terceiro. No primeiro caso, o empresário deve provar que o produto defeituoso não foi fabricado, produzido, construído ou importado por ele. **Nessa excludente de responsabilização, encaixa-se não somente a hipótese de equívoco do consumidor na identificação do fornecedor responsável, mas também os defeitos provocados por produtos falsificados ou com marca usurpada**. *(grifo meu)*

Conforme mencionado anteriormente, o *phishing* também pode ser considerado uma forma de usurpação de marca, pelo uso dos símbolos distintivos que identificam determinada empresa, de modo que é possível aqui que seja aplicada a excludente de responsabilidade prevista no Código de Defesa do Consumidor.

Aqui, existem poucas aplicações que a companhia possa realizar para evitar a replicação das suas estruturas oficiais, sendo que a principal forma de proteção contra o ataque é realizada por meio da educação dos usuários, ensinando-os a reconhecer as fontes confiáveis e aquelas que não são.

A partir dessa educação do usuário, além da culpa do terceiro pelo crime cometido, é possível se dizer em até mesmo a responsabilidade do consumidor, haja vista que foram fornecidos meios pela empresa para que ele se protegesse dos ataques e ainda assim não foram tomadas as cautelas necessárias.

Neste sentido alguns tribunais já têm passado a se manifestar, como se vê a seguir:

> APELAÇÃO CÍVEL PROCESSUAL CIVIL - AÇÃO DE INDENIZATÓRIA - FRAUDE BANCÁRIA - "PHISHING" - RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA - AUSÊNCIA - FATO EXCLUSIVO DE TERCEIRO - OCORRÊNCIA - AÇÕES PARA MINIMIZAR OS EFEITOS DA FRAUDE - COMPROVAÇÃO - DANOS MATERIAIS - CONDENAÇÃO DO BENEFICIÁRIO DO GOLPE - OCORRÊNCIA - SOLIDARIEDADE COM A INSTITUIÇÃO

> FINANCEIRA - INEXISTÊNCIA. 1- Como fornecedor na relação de consumo, a instituição financeira responde objetivamente pelos danos ocasionados aos consumidores pela ocorrência de falha na prestação dos serviços. 2- Não configura falha na prestação dos serviços por parte da instituição financeira a ocorrência de fraude bancária pela aplicação do golpe denominado "*phishing*", sobretudo quando há comprovação de que o agente financeiro, ciente da existência do golpe, adotou todas as medidas que estava ao seu alcance para cientificar os consumidores e minimizar a incidência da fraude. 3- Incabível a condenação solidária da instituição financeira em conjunto com o terceiro beneficiário do produto da fraude, a devolver a quantia depositada pelas vítimas quando não é reconhecida a responsabilidade daquela pela aplicação do golpe. (TJMG - Apelação Cível 1.0324.17.010372-9/001, Relator(a): Des.(a) Claret de Moraes , 10ª CÂMARA CÍVEL, julgamento em 10/08/2021, publicação da súmula em 16/08/2021).
>
> AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO C.C. INDENIZAÇÃO POR DANOS MORAIS – Sentença de improcedência – Recurso da parte autora – Boleto falso recebido por *whatsapp* e pago pelo autor – Golpe perpetrado por terceiros, adotando prática conhecida como "*phishing*" – Falta de cautela do autor – Responsabilidade do réu não caracterizada (CDC, art. 14, § 3º, II) – Ratificação do julgado – Honorários recursais devidos – RECURSO NÃO PROVIDO. (TJSP; Apelação Cível 1002760-66.2021.8.26.0066; Relator (a): Spencer Almeida Ferreira; Órgão Julgador: 38ª Câmara de Direito Privado; Foro de Barretos - 2ª Vara Cível; Data do Julgamento: 10/12/2021; Data de Registro: 10/12/2021)

Em situações análogas, em que se discute a responsabilização dos provedores de aplicação[9] por manifestações de terceiros que constituam ato ilícito em suas plataformas, foi estabelecido que a responsabilidade é subjetiva e subsidiária, como demonstram Roth e Nunes (2019, p. 149).

> Percebe-se que tal disposição propõe que, na hipótese de um consumidor (usuário) se sentir lesado por qualquer tipo de ofensa/publicação feita nas plataformas dos provedores de aplicação estes, por sua vez, somente serão civilmente responsáveis quando após serem certificados judicialmente e não tomarem as providências cabíveis.

Assim sendo, arrisco dizer que, aplicadas todas as medidas ao alcance da empresa para a proteção do usuário contra essa forma de ataque, não se reputa correto atribuir a

[9] "Por sua vez, utilizando as definições estabelecidas pelo art. 5º, VII, do Marco Civil da Internet, uma aplicação de internet é o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet. Como é possível perceber, essas funcionalidades podem ser as mais diversas possíveis, tais como serviços de e-mail, redes sociais, hospedagem de dados, compartilhamentos de vídeos, e muitas outras ainda a serem inventadas. Por consequência, os provedores de aplicação são aqueles que, sejam com ou sem fins lucrativos, organizam-se para o fornecimento dessas funcionalidades na internet" (BRASIL. **Superior Tribunal de Justiça. Recurso Especial nº 1.642.560/SP**. Relator: Ministro Marco Aurélio Belizze. Pesquisa de Jurisprudência. Ementa, 29 de Novembro de 2017. Disponível em https://processo.stj.jus.br/processo/revista/inteiroteor/?num_registro=201602427774&dt_publicacao=29/11/2017 . Acesso em: 21/01/2022.

responsabilidade integralmente à instituição, haja vista que ela não foi responsável pelo ataque em si. Por outro lado, pode a empresa até mesmo ser considerada também vítima do crime, tendo em vista as perdas econômicas que virá a sofrer resultantes de fatores diretos, como a alteração do destinatário do valor que ele viria a receber, bem como indiretos, como a perda de credibilidade perante o mercado.

A atribuição de responsabilidade integral à empresa realiza uma dupla vitimização desta e retira a responsabilidade do Estado em realizar a correta atribuição de culpa pelo dano, esta permitida pela correta aplicação do art. 171, §2º e seguintes do Código Penal brasileiro. A partir da penalização correta do hacker, o usuário deveria ajuizar ação contra aquele que efetivamente recebeu a vantagem indevida, e não contra a empresa que fez o que estava ao seu alcance para impedir o ataque.

CAPÍTULO IV – O COMPLIANCE DIGITAL

O *compliance* é definido como "um conjunto de medidas que implicam procedimentos internos no âmbito das empresas visando à conformidade com a lei", conforme Durães e Ribeiro (2020, p. 2), possuindo como função "monitorar e assegurar que todos os envolvidos com uma empresa estejam de acordo com as práticas de conduta da mesma", como definido por Ubaldo (2017, p. 121).

Também, o Conselho Administrativo de Defesa Econômica (CADE) no seu Guia para Programa de *Compliance*, o define como "um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores".

Dessa maneira, ainda que esse conjunto de medidas seja, na maioria das vezes, considerado apenas em relação às leis de escopo penal, elas podem também ser elaboradas tendo em vista as mais diversas áreas. Assim sendo, o *compliance* digital pode ser definido como as regras adotadas pelas empresas com o objetivo de prevenir ou minimizar riscos de violação às leis referentes ao âmbito digital e a proteção de dados, principalmente ao que se refere à Lei nº 13.709/2018.

Ressalta-se aqui que a Lei Geral de Proteção de Dados estabelece em seu art. 46 a necessidade de se estabelecer medidas de prevenção contra eventuais violações dos dados dos usuários, de forma que referidos mecanismos devem ser objeto de procedimentos e políticas internos e normalmente abrangidos pelo *compliance* da empresa.

Essas medidas são fundamentais não somente para impedir que o fato danoso ocorra, mas, também, para que caso ele chegue a ocorrer as sanções respectivas sejam de menor proporção.

> Uma vez que a indenização é medida pela extensão do dano (artigo 944 do Código Civil), a existência dos programas de integridade e das políticas de governança poderia balizar um sancionamento mais severo do ofensor, em caso de violação mais acentuada dos parâmetros definidos pela lei e pelos programas e políticas advindos do *compliance*, ou mesmo um abrandamento de eventual reparação, se demonstrada sua efetividade, na forma do artigo 50, §2o, inc. II, da LGPD. (FALEIROS JÚNIOR; MARTINS, 2020, p. 292)

Nesse sentido, notada a necessidade de instituir essas medidas, passa-se a discorrer acerca do *phishing*, uma forma de engenharia social conforme já definido anteriormente, devendo ser também abrangida pelo *compliance* da companhia, haja vista que o alvo do ataque é justamente os dados pessoais do indivíduo.

Sendo uma modalidade de engenharia social, os mecanismos de prevenção aplicados devem estar voltados ao usuário. Atualmente, existem *softwares* de proteção contra as mais diversas formas de ataque, sendo eles os antivírus *firewall*, cuja instalação não pode ser determinada ao público em geral, mas pode ser garantida ao menos nas máquinas destinadas aos funcionários da empresa, reduzindo a possibilidade de ocorrência de *phishing* no âmbito interno e consequente vazamento de dados.

Em âmbito externo, relembra-se que os *e-mails* maliciosos são enviados por endereços similares aos oficiais, devendo o destinatário observar eventuais erros de ortografias e conteúdo de mensagens que pareçam alarmantes, induzindo ao clique nos links e arquivos lá anexados.

Algumas empresas utilizam de algumas formas para conscientizar seus clientes acerca destes golpes, seja por notícias veiculadas em canais de comunicações, *pop-ups* ao adentrar na tela inicial do site, assim como notificações e os próprios *e-mails*, o que se caracteriza como forma realmente mais eficiente para a proteção contra o *phishing*.

Métodos como desconectar o computador da rede e não o acessar até que o *malware* seja resolvido e checar frequentemente se o antivírus instalado na máquina colocou algum elemento suspeito em quarentena são medidas que podem ser utilizadas pelo usuário para evitar os danos pelo ataque por *phishing*[10], podendo eles ser indicados pelas empresas provedoras.

---

[10] "Remediation Steps: 1. Disconnect the computer from the network and notify the user that the computer cannot be re-connected until all malware has been successfully removed; 2. Find out if the user is familiar

Um estudo realizado por pesquisadores Wright, Johnson e Kitchens da Universidade da Virgínia verificou que as medidas realizadas com o fim de ressarcir o usuário pelos danos causados pelo *phishing* possuem, na verdade, o efeito de reduzir a conscientização destes e aumentar o número de casos.

> "O resultado mais inesperado da nossa pesquisa é que indivíduos que procuram recomendações mais frequentemente do seu pessoal de apoio de TI designado ao contrário daqueles em sua rede social são mais, não menos, suscetíveis ao *phishing*. O pessoal de apoio de TI é frequentemente encarregado com a tarefa de educar outros funcionários sobre as melhores práticas para cumprir com as políticas organizacionais de segurança de TI. Triangulando ainda mais essa descoberta, o resultado indica que os indivíduos que confiam na função de suporte de TI são mais propensos a clicar em uma mensagem de *phishing*. (...) De modo similar a como as companhias de cartão de crédito indenizam usuários por qualquer transação não autorizada, o suporte frequente pode indenizar empregados por brechas nas políticas de segurança porque o "*Help Desk* vai consertar o problema. Outra possível razão por este resultado é que a maior confiança no Help Desk aumentaria o comportamento de tomada de riscos do indivíduo. Existe evidência que aponta para o risco da homeostase na cibersegurança (RENAULD e WARKETIN, 2017). Esse conceito postula que pessoas tomarão mais riscos nos seus comportamentos lhes for proporcionado um sentimento de segurança. O *Help Desk* pode estar fornecendo essa rede de segurança que é na verdade contraproducente para a segurança do usuário". (WRIGHT; JOHNSON; KITCHENS, 2010) [11]

---

with the destination or action that the malware or bot is trying to access; 3. Make sure the infected machine has an Anti-Virus application installed, running and updated. Check to see if any malware has been quarantined by the Anti-Virus application." (CHECK POINT RESEARCH, 2022)

[11] "The most unexpected result from our research is that individuals who seek advice most frequently from their designated IT support personnel as opposed to others in their social network are more, not less, susceptible to phishing. IT support personnel are frequently tasked with educating other employees about best practices to comply with organizational IT security policies. Further triangulating this finding was the result indicating those individuals that trust the IT support function are more likely to click on a phishing message. (…) Similar to how credit card companies indemnify users from any unauthorized transaction, frequent support may indemnify employees from breeches in the security policies because "the Help Desk will fix the problem". Another possible reason for this result is the greater confidence in the Help Desk would increase one's risk taking behaviors. There is evidence that points to risk homeostasis in cybersecurity (Renauld and Warkentin 2017). This concept posits that people will take more risk in their behaviors when they are provided a feeling of safety. The Help Desk may be providing this safety net that is in fact counterproductive to the user's security." (WRIGHT; JOHNSON; KITCHENS, 2010)

Por esta razão, o *compliance* deve visar não somente auxiliar o usuário com o problema no momento do ataque, mas sim conscientizá-lo sobre quais os foram os sinais de que o conteúdo não seria confiável o indivíduo não identificou, de forma que seja evitada uma nova situação semelhante e, consequentemente, evitando custos para a empresa.

Também, é válido ressaltar o princípio do consentimento, aplicado ao tratamento de dados pessoais, conforme a Lei Geral de Proteção de Dados. Faleiros (2019, p. 217) menciona que "na medida em que o consentimento passa a ser o critério fundamental para a coleta, torna-se essencial que o indivíduo saiba os limites e os riscos que enfrentará com o fornecimento de determinado conjunto de dados".

Assim sendo, nos termos de uso geralmente apresentados ao usuário no momento de entrada na plataforma, deve ser delimitada a finalidade do uso dos dados pessoais, os riscos de fornecimento deles e, inclusive, a necessidade de se observar o remetente de forma que estes dados sejam fornecidos para o destinatário correto, assim como as medidas que podem ser adotadas para que este erro não ocorra.

Não pode ser esquecida a necessidade de registro da marca perante o Instituto Nacional de Propriedade Industrial, permitindo a aplicação dos dispositivos legais que permitem a proteção da marca e sanção àqueles que a utilizem indevidamente, como mencionado em capítulo anterior.

Dessa maneira, é possível evitar que exista uma eventual responsabilização incorreta recaída sobre a empresa por um ataque de *phishing*, ainda que a questão ainda possa ser discutida judicialmente.

CONCLUSÃO

Assim, em relação à problemática que este trabalho se propôs a discutir, obtém-se a conclusão de que a responsabilidade pelo *phishing* à sociedade empresária deve ser limitada e subsidiária, de modo que seja aplicada apenas caso não sejam instituídas medidas preventivas, para que seja obedecido o princípio de proteção ao consumidor sem que implique em dano desproporcional à instituição.

Essa prevenção deve ocorrer por meio de medidas de *compliance*, com os devidos meios técnicos empregados e, também, a instrução dos usuários acerca dos métodos para que se evite o ataque, identificando os conteúdos suspeitos e não acessando eventuais correspondências e *sites* maliciosos.

Isso porque a atribuição de responsabilidade integral à empresa, como já foi visto, afronta diretamente diversos princípios, como da função social da empresa, da preservação da empresa e do impacto social da crise da empresa, além dos demais que decorrem destes. Feridas estas determinações, os danos gerados não serão direcionados apenas àquele que realiza a atividade empresária, mas a toda a sociedade que é direta ou indiretamente afetada pelos resultados da instituição.

Essa responsabilidade deve ser primordialmente direcionada ao criminoso que realizou o *phishing* e, caso não sejam aplicadas as medidas acima mencionadas, ao usuário que não observou as instruções fornecidas e não tomou os devidos cuidados para evitar o ataque. Assim, é possível manter um equilíbrio entre as relações e evitar danos desproporcionais às empresas sem que sejam feridos os princípios do Código de Defesa do Consumidor.

BIBLIOGRAFIA

BRASIL. **Constituição** (1988). **Constituição** da República Federativa do Brasil. Brasília, DF: Senado **Federal**: Centro Gráfico, 1988. Acesso em 15 nov. 2021

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.**. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 15 nov. 2021

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 01 dez. 2021.

BRASIL. **Lei da Propriedade Industrial**. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 05 jan. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados**. Brasília, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 nov. 2021.

CADE. **Guia**: programas de compliance. Programas de Compliance. Disponível em: http://antigo.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf. Acesso em: 17 fev. 2022.

COELHO, Fabio Ulhôa. **Curso de Direito Comercial, Volume 1**. 16. ed. São Paulo: Saraiva, 2012.

CRUZ, André Santa. **Direito Empresarial**. São Paulo: Método, 2019.

DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 18. ed. São Paulo: Ltr, 2019.

DURÃES, Cintya Nishimura; RIBEIRO, Maria de Fátima. O COMPLIANCE NO BRASIL E A RESPONSABILIDADE EMPRESARIAL NO COMBATE À CORRUPÇÃO. **Revista Direito em Debate**, [S.L.], v. 29, n. 53, p. 69-78, 26 maio 2020. Editora Unijui. http://dx.doi.org/10.21527/2176-6622.2020.53.69-78.

EIRAS, Marcelo Coradassi. **Engenharia Social e Estelionato Eletrônico**. 2004. 40 f. Monografia (Doutorado) - Curso de Segurança de Informações na Internet, Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2004. Disponível em: https://docplayer.com.br/983029-Engenharia-social-e-estelionato-eletronico.html. Acesso em: 19 jan. 2021.

FINKELSTEIN, Maria Eugênia. Responsabilidade de instituições financeiras por fraude eletrônica. **Revista de Direito Bancário e do Mercado de Capitais**, São Paulo, v. 72, abr./jun. 2016.

KAPERSKY. **Dicas para a prevenção de phishing**. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips. Acesso em: 15 nov. 2021.

LIMA, Alvino. **Culpa e risco**. São Paulo: Revista dos Tribunais, 1998.

ROTH, Gabriela; NUNES, Samuel. A responsabilidade civil dos provedores por danos causados a terceiros: um estudo doutrinário e jurisprudencial do artigo 19 do Marco Civil da Internet. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Estudos Essenciais de Direito Digital**. Uberlândia: Laecc, 2019. p. 131-154.

FALEIROS JÚNIOR, José Luiz de Moura. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. In: LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Estudos Essenciais de Direito Digital**. Uberlândia: Laecc, 2019. p. 207-231.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. **Compliance digital e Responsabilidade Civil na Lei Geral de Proteção de Dados**. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson. Responsabilidade Civil e novas tecnologias. Ed. Foco, 2020, p. 263-297.

MITNICK, Kevin D.; SIMON, William L.. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education do Brasil, 2003. Tradução: Kátia Aparecida Roque.

NUNES, Rizzatto. **Curso de Direito do Consumidor**. 12. ed. São Paulo: Saraiva, 2018.

PRODEST. **Entenda o que é phishing e adote medidas para evitá-lo**. Disponível em: https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo. Acesso em: 15 nov. 2021.

OSTERMAN RESEARCH. **How to Reduce the Risk of Phishing and Ransomware**. Disponível em: https://resources.trendmicro.com/Osterman-Email-Security-WP.html. Acesso em: 06 jul. 2021.

ROSENTHAL, Maddie. **Must-Know Phishing Statistics: Updated 2022**. Disponível em: https://www.tessian.com/blog/phishing-statistics-2020/. Acesso em: 23 jan. 2022.

TARTUCE, Flávio. **Manual de Responsabilidade Civil**. Rio de Janeiro: Método, 2018.

TARTUCE, Flávio; NEVES, Daniel Amorim de Assumpção. **Manual de Direito do Consumidor**. 17. ed. São Paulo: Editora Forense, 2017

PAIVA, Mariza de Souza; COSTA, Samara Silva. COMPLIANCE DIGITAL E PROTEÇÃO DE DADOS: A LGPD E A RESPONSABILIDADE CIVIL DAS STARTUPS: inteligência artificial, startups, lawtechs e legaltechs. In: XI CONGRESSO RECAJ-UFMG, 11., 2020, Belo Horizonte. **INTELIGÊNCIA ARTIFICIAL, STARTUPS, LAWTECHS E LEGALTECHS.** Belo Horizonte: Conpendi, 2020. p. 54-60. Disponível em: http://site.conpedi.org.br/publicacoes/05sx3fe1/p1429102/et8w3R7G263Jo352.pdf. Acesso em: 11 fev. 2022.

PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2013.

PEREIRA, Emanuela de Araújo. **A fraude eletrônica à luz da Lei nº 14.155**. Disponível em: https://jus.com.br/artigos/91226/a-fraude-eletronica-a-luz-da-lei-n-14-155. Acesso em: 19 jan. 2022.

CHECK POINT RESEARCH**. Check Point Press Releases**. DHL Replaces Microsoft as Most Imitated Brand in Phishing Attempts in Q4 2021. Disponível em: https://www.checkpoint.com/press/2022/dhl-replaces-microsoft-as-most-imitated-brand-in-phishing-attempts-in-q4-2021/. Acesso em: 05 fev. 2022.

CHECK POINT RESEARCH. **Malware Family**: phishing. Phishing. Disponível em: https://threatpoint.checkpoint.com/ThreatPortal/threat?threatType=malwarefamily&threatId=6061. Acesso em: 05 fev. 2022.

R7. **Ataques por phishing no Brasil crescem 41% em 2021**. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/ataques-por-phishing-no-brasil-crescem-41-em-2021-12122021. Acesso em: 05 fev. 2022.

UBALDO, Flávia Safadi. **Lei Anticorrupção: a importância do programa de compliance no cenário atual**. In: PORTO, Vinícius; MARQUES, Jader (org.). O compliance como instrumento de prevenção e combate à corrupção. Porto Alegre: Livraria do Advogado, 2017

VENOSA, Silvio de Salvo. **Direito Civil - Obrigações e Responsabilidade Civil**. São Paulo: Atlas, 2018.

WOLKOFF, Alexander Porto Marinho. A Teoria do Risco e a Responsabilidade Civil Objetiva do Empreendedor. **Revista de Direito do Tribunal de Justiça do Estado do Rio de Janeiro**, Rio de Janeiro, n. 81, p. 113-135, out. 2009.

WRIGHT, Ryan; JOHNSON, Steven L.; KITCHENS, Brent. A Multi-Level Contextualized View of Phishing Susceptibility. **Ssrn.** out. 2010. Disponível em: https://ssrn.com/abstract=3622310. Acesso em: 22 jan. 2022.