ATAQUES POR PHISHING: UMA ANÁLISE JURÍDICA SOB O OLHAR DA RESPONSABILIDADE CIVIL EMPRESARIAL

PHISHING ATTACKS: A LEGAL ANALYSIS FROM THE PERSPECTIVE OF CORPORATE CIVIL LIABILITY

Rafaela Alves da Silva[1]
Thayna Carvalho Flor[2]
Marcos Henrique Vieira Farias[3]
Letícia Rosa Soares Temoteo[4]
Daiany Sousa Vieira Vidal[5]

RESUMO: Este estudo examina a responsabilidade civil empresarial em casos de ataques por *phishing,* possuindo como objetivo principal a observação da aplicação da responsabilidade objetiva das empresas prestadoras de serviços digitais. Propondo assim, uma análise criteriosa que considera os avanços legislativos e a complexidade dos elementos fáticos presentes nas fraudes digitais.

Palavras-chave: *Compliance***.** Empresas. *Phishing.* Proteção de dados. Responsabilidade civil.

ABSTRACT: This study examines corporate civil liability in cases of phishing attacks, with the primary objective of observing the application of strict liability to companies providing digital services. Thus, it proposes a thorough analysis that considers legislative advances and the complexity of the factual elements present in digital fraud.

Keywords: Civil liability. Companies. Compliance. Data protection*. Phishing.*

INTRODUÇÃO

Com a evolução da tecnologia e a digitalização das relações de consumo, verifica-se um aumento expressivo nas transações online, proporcionando eficiência e comodidade para clientes e fornecedores, contudo, essa evolução trouxe consigo um crescimento significativo de crimes digitais por meio de práticas fraudulentas que evidenciam a necessidade da proteção dos dados pessoais e financeiros dos sujeitos

[1] Estudante de Bacharelado em Direito na Faculdade Princesa do Oeste - FPO. E-mail: rafaela.alves@alu.fpo.edu.br.
[2] Estudante de Bacharelado em Direito na Faculdade Princesa do Oeste - FPO. E-mail: thayna.carvalho@alu.fpo.edu.br
[3] Estudante de Bacharelado em Direito na Faculdade Princesa do Oeste - FPO. E-mail: henrique.vieira@alu.fpo.edu.br
[4] Estudante de Bacharelado em Direito na Faculdade Princesa do Oeste - FPO. E-mail: leticia.rosa@alu.fpo.edu.br
[5] Doutoranda e mestra em Direito Público. Professora do curso de gradução em Direito na Faculdade Princesa do Oeste FPO – E-mail: daiany.vidal@fpo.edu.br.

dessa relação.

Nesse sentido, a atuação do ordenamento jurídico busca garantir a segurança do cliente e a responsabilização civil do fornecedor, ou empresa, sempre que ocorrer violação de informações, sejam elas de pessoas físicas ou jurídicas.

A responsabilidade civil das empresas diante desses ataques revela-se tema de grande relevância, tanto no âmbito jurídico, que envolve a proteção dos direitos dos consumidores, quanto no social, que trata da segurança das relações comerciais digitais.

Entre os crimes digitais mais recorrentes, destaca-se o phishing, termo originado em meados de 1990, do inglês "*phishing*", que significa "pesca", em analogia a "fisgar o alvo". Nesse delito, a vítima tem suas informações obtidas de forma enganosa, por meio de técnicas baseadas na engenharia social, que buscam induzir a confiança para posteriormente causar prejuízos.

A engenharia social consiste em manipular e persuadir pessoas a acreditar que o golpista é alguém de confiança ou tem autorização para agir, aproveitando-se da boa-fé, da falta de conhecimento ou da inocência da vítima para obter informações pessoais.

O usuário, portanto, é levado ao erro por fatores psicológicos e sociais, mais do que por falhas técnicas nos sistemas de segurança das empresas. Assim, os ataques exploram comunicações falsas com supostas instituições credenciadas, que resultam no vazamento de dados sensíveis.

Um exemplo clássico ocorre quando o destinatário recebe um e-mail, supostamente enviado pelo banco, que solicita a atualização imediata de dados sob a ameaça de bloqueio da conta, fazendo com que o usuário, por acreditar se tratar de comunicação legítima, forneça as informações confidenciais, como senhas, números de conta e dados de cartões de crédito.

O Brasil se destaca entre os países com maior número de golpes virtuais, especialmente por meio de aplicativos de mensagem e e-mails, o que demonstra o aumento preocupante das práticas de phishing e outras fraudes digitais, refletindo a vulnerabilidade dos usuários nas interações online e revelando fragilidades psicológicas e sociais que facilitam a ação dos criminosos, razão pela qual se faz necessária a ampliação da educação digital e a adoção de medidas preventivas para reduzir esses riscos.

As infrações cibernéticas se aproveitam da diversidade do público e da falta de conhecimento sobre esse tipo de ataque. Entre elas, há a fraude das faturas falsas de

operadoras telefônicas, no qual criminosos enviam boletos ou links fraudulentos, levando o cidadão a efetuar pagamentos indevidos e a fornecer informações financeiras sem perceber o risco envolvido.

Referidos casos evidenciam como esse tipo de infração ultrapassa o conceito habitual de subtração de informações sensíveis, configurando uma transgressão que envolve manipulação psicológica, bem como o contexto digital e social em que o polo passivo está inserido, ocasionando danos de natureza pessoal e patrimonial.

Diante desse cenário de complexidade e riscos ampliados, torna-se evidente a necessidade de uma intervenção normativa mais precisa. Nesse contexto, os avanços legislativos, especialmente a edição da Lei nº 14.155/2021, que supriu a lacuna quanto à tipificação penal do crime de phishing, ao acrescentar ao artigo 171 do Código Penal Brasileiro os §§ 2º-A e 2º-B, permitiram ao ordenamento jurídico disciplinar de forma mais adequada essa conduta, preenchendo as lacunas anteriormente existentes.

Ademais, tornaram-se igualmente evidentes as repercussões dessa infração no âmbito civil, especialmente no que se refere à responsabilidade das empresas que são alvo dos ataques e aos danos suportados pelas vítimas.

O presente trabalho tem como objetivo analisar o aumento expressivo das fraudes digitais e a importância de compreender a aplicação da legislação vigente nesses casos, com ênfase na responsabilidade objetiva fundamentada na teoria do risco-proveito e nas limitações decorrentes da culpa exclusiva da vítima ou de terceiros.

METODOLOGIA

A metodologia adotada neste estudo fundamenta-se na pesquisa bibliográfica e documental, com enfoque qualitativo e caráter descritivo analítico. Foram examinadas obras doutrinárias, artigos científicos e legislações que tratam da responsabilidade civil, da proteção de dados pessoais e das relações de consumo no ambiente digital, com especial atenção ao Código de Defesa do Consumidor e à Lei Geral de Proteção de Dados Pessoais. A escolha dessa metodologia justifica-se pela natureza teórica do objeto investigado, que demanda análise interpretativa das fontes normativas e doutrinárias para a compreensão das implicações jurídicas decorrentes das fraudes eletrônicas ora estudadas.

REFERENCIAL TEÓRICO

1. A Empresa

As empresas se estabelecem como estruturas que impulsionam o desenvolvimento comunitário e econômico, promovendo avanços tecnológicos, geração de emprego e enriquecimento social.

Segundo o doutrinador Fábio Ulhoa Coelho (2022), ela funciona não somente pelo interesse do empresário e dos funcionários, mas também da sua contribuição para a comunidade. Todos devem ser protegidos, ora que serão igualmente prejudicados em casos de conduta em desacordo com a legislação.

Apesar da Constituição Federal Brasileira de 1988 não trazer expressamente a função da empresa, entende-se, através de uma interpretação extensiva do texto, que esta deve cumprir com a sua função social. Por essa razão, menciona-se o princípio da função social da propriedade, previsto no art. 5° da referida norma, in verbis:

> Art. 5° Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> XXIII – a propriedade atenderá a sua função social;
> (Brasil, 1988)

De acordo com Gagliano (2012), a responsabilidade da instituição se concretiza ao compartilhar com o Estado a garantia de determinados deveres que devem ser assegurados à sociedade, corroborando o entendimento já consagrado na Constituição Federal de 1988, especialmente no artigo 170, que ressalta a importância da valorização do trabalho humano com dignidade e justiça social (BRASIL, 1988).

Nesse sentido, é possível observar que a função social da empresa não se refere somente às atividades que ela deve desempenhar, mas também ao comportamento que deve adotar perante as partes interessadas.

Por conseguinte, reforçando a responsabilidade das empresas no tratamento de dados pessoais, a Lei nº 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), representa um avanço relevante no direito brasileiro, ao regulamentar o tratamento de informações pessoais e reforçar direitos fundamentais, como a privacidade e a liberdade individual.

No entanto, conforme observa Saiuri (2022), a aplicação inadequada ou

descontextualizada dessas normas pode gerar consequências econômicas significativas para o empreendedorismo. Julgamentos sem critérios claros ou sem a devida análise do contexto das empresas podem resultar em condenações capazes de inviabilizar atividades empresariais, desestimular novos investimentos e tornar o ambiente de negócios menos propício à inovação e ao crescimento econômico.

É fato que há uma preocupação do empresário em relação às condenações engessadas em relação aos casos fraudulentos, ora que o prejudicado não é somente a vítima que foi o alvo do golpe, mas também a empresa que teve sua marca associada ao evento e que será impactada pelos prejuízos em virtude de descrédito social.

O legislador aduz, no art. 189 da Lei de Propriedade Industrial n° 9.279/96, que:

> 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;
> (...).
> (Brasil, 1996)

Dessa forma, resguarda-se ao empresário o direito de ingressar com ação judicial para responsabilizar aqueles que se utilizem indevidamente de sua marca para a prática de delitos cibernéticos. No entanto, para além da literalidade da lei, é imprescindível que a análise da responsabilidade das empresas seja realizada de maneira equilibrada, de modo a não prejudicar a vítima, mas considerando a estrutura, o porte e a capacidade organizacional de cada organização.

As particularidades de cada empresa influenciam diretamente a forma como ela pode cumprir suas obrigações legais e sociais. Nos casos de instituições financeiras, por exemplo, pesquisas da Deloitte Insights (2020) indicavam que menos de 10% dos investimentos realizados, estimados em alguns milhões de reais, eram destinados à segurança e à proteção dos dados dos clientes, evidenciando a relevância de se ponderar a responsabilidade em função da capacidade de cada instituição.

A Surfshark (2025) disponibiliza estatísticas globais de 2024 referentes a violação de dados, no estudo é informado que os números de contas violadas saltaram de 730 milhões, número registrado em 2023, para 5,5 bilhões em 2024, totalizando aproximadamente, 180 contas comprometidas a cada segundo.

No cenário atual, marcado pela obrigatoriedade legal e pela crescente competitividade no mercado, torna-se evidente que as organizações precisam investir cada vez mais na proteção de dados. Esse contexto também gera oportunidades de

lucro para empresas que desenvolvem soluções eficazes de segurança, elevando os preços dos serviços e tornando-os, muitas vezes, inacessíveis para empresas de pequeno porte.

Apesar disso, tal situação não exime as organizações da responsabilidade de adotar medidas de segurança adequadas e eficazes. Ao coletar dados de seus clientes, a empresa assume a obrigação legal e ética de proteger essas informações, prevenir vazamentos e garantir que seus clientes não se tornem vítimas de ataques virtuais, mesmo quando o custo para isso seja elevado.

RESULTADOS E DISCUSSÕES

1. A Responsabilidade Civil das Empresas

Ao tratar da responsabilidade civil das empresas nos ataques por phishing, é importante discutir a natureza jurídica dessa relação. De um lado, há a figura dos titulares dos dados atingidos, de outro, as sociedades empresárias.

De forma inicial, ainda que as empresas sejam impactadas pela utilização indevida da sua marca, a relação fraudulenta existente entre os agentes golpistas e as vítimas, são parte da relação de consumo original. Portanto, devem ser protegidas pelo Direito do Consumidor, considerando que as vítimas são destinatárias finais de um serviço ou produto atuante.

É necessário reconhecer as vítimas como clientes para que gozem das proteções jurídicas previstas nessa legislação, reconhecendo sua hipossuficiência, expondo o dever de segurança sobre as empresas que prestam serviços. Em regra, a responsabilidade objetiva torna desnecessária a demonstração de culpa do fornecedor quando da existência de eventuais danos.

Do ponto de vista da teoria do risco-proveito, entende-se que o agente que expõe ao risco outras pessoas em razão do desempenho da sua atividade comercial, com a possibilidade de obtenção de lucro, responde, independentemente de culpa, pelos prejuízos ocasionados por possíveis vícios ou defeitos oriundos dos seus produtos ou serviços. Para Tartuce e Neves (2025, p. 145), o Código de Defesa do Consumidor adota expressamente a referida teoria:

Na verdade, 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.

Diante dessas considerações, é importante destacar que, embora a legislação adote a responsabilidade objetiva, esta não deve ser aplicada de forma absoluta. Assim, nas hipóteses em que se reconheça a culpa exclusiva da vítima ou de terceiro, nos termos dos artigos 12, §3º, e 14, §3º, do referido diploma legal, o fornecedor não deve ser responsabilizado por prejuízos a que não tenha dado causa, evitando-se, desse modo, eventual injustiça (Brasil, 1990).

Esse entendimento revela-se essencial, pois afasta a perspectiva de que a empresa deve responder, independentemente de culpa, por todo e qualquer dano suportado pelos consumidores.

Diante disso, nos casos em que se comprove a adoção de condutas preventivas e diligentes pela sociedade empresária, com o objetivo de evitar ou mitigar ciberataques, é possível concluir que o evento lesivo, em geral, decorre da expectativa do próprio usuário, aliada à conduta ilícita de um terceiro, e não de uma falha estrutural ou técnica do fornecedor.

Nessa perspectiva, Rezende (2022) afirma que é possível responsabilizar o consumidor quando este deixa de adotar as cautelas necessárias que poderiam ter evitado o golpe. Assim, uma vez implementadas todas as medidas preventivas cabíveis à proteção dos dados dos consumidores, rompe-se o nexo de causalidade entre a conduta da empresa e o dano sofrido, afastando-se a sua responsabilização.

Dito isso, embora seja um ponto sensível atribuir culpa exclusiva à vítima, dada sua vulnerabilidade e o dever das empresas em garantir a segurança digital, é prudente expor que o ofendido terá de arcar com os próprios prejuízos se restar comprovado a negligência quanto às orientações educativas e os mecanismos de proteção divulgados pelas instituições empresariais.

Nessa hipótese, a responsabilidade das sociedades empresariais deixa de possuir caráter objetivo, passando a ser subjetiva e subsidiária, exigindo-se a demonstração de culpa quando da ocorrência de prejuízos decorrentes do desfalque. Desse modo, a atribuição de responsabilidade às instituições deve basear-se em uma análise criteriosa dos elementos fáticos do caso concreto, considerando-se não apenas as condutas do fornecedor, mas também as do consumidor.

Assim, no que pese a responsabilidade da sociedade empresária ser na

literalidade da Lei objetiva, é imprescindível verificar se houve a adoção de todas as medidas tecnicamente viáveis para a proteção do usuário, especialmente diante do crescente risco de fraudes digitais.

2. Compliance

O compliance consiste em um conjunto de medidas internas adotadas pelas empresas com o objetivo de assegurar a conformidade com a legislação e com padrões éticos de conduta. No contexto digital, esse conceito assume especial relevância diante da crescente ocorrência de fraudes eletrônicas e da necessidade de se estabelecer mecanismos eficazes de prevenção e resposta a essas práticas.

Ainda que os programas de compliance possuam uma abrangência multissetorial nas companhias em que são aplicados, o Direito Digital tem se destacado nesse cenário, impulsionado pelo avanço das relações humanas e empresariais nos ambientes virtuais e pela crescente preocupação com a proteção de dados sensíveis. Essa realidade deu origem ao chamado compliance digital, voltado especificamente à adoção de políticas e estratégias que assegurem a integridade das informações e o cumprimento das normas de proteção de dados.

Conforme destaca Cláudio Joel Brito Lóssio (2023), a boa governança possui caráter essencialmente preventivo, atuando como um instrumento capaz de evitar complicações futuras. A busca pela conformidade nas empresas, portanto, contribui para a proteção não apenas dos clientes, mas também dos colaboradores diretos e indiretos, tanto no que se refere à segurança das informações quanto à consolidação de uma cultura organizacional sólida e ética.

Além disso, o autor observa que, ao idealizar ou administrar um empreendimento, raramente se considera a possibilidade de situações extremas, como a violação ou o vazamento massivo de dados capaz de comprometer a reputação da empresa. Para evitar tais ocorrências, é indispensável uma gestão de riscos eficaz, pautada na análise de certezas, incertezas e probabilidades de perda, de modo a identificar e mitigar vulnerabilidades relacionadas à estrutura organizacional, às pessoas, aos produtos e aos serviços.

Essa gestão preventiva se alinha diretamente ao disposto no artigo 46 da Lei Geral de Proteção de Dados (LGPD), que impõe às empresas o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas (Brasil, 2018). Assim, o

compliance digital não se limita a um instrumento de prevenção, mas se revela também como um elemento de responsabilização, visto que a existência, ou a ausência, de programas de integridade pode influenciar a resposta jurídica em casos de vazamento de dados.

De acordo com o artigo 944 do Código Civil e o artigo 50, §2º, II, da LGPD, a efetividade das políticas de compliance pode, a depender das circunstâncias, agravar ou atenuar a responsabilização da empresa, permitindo inclusive a redução de penalidades quando demonstrado o comprometimento real com a cultura de proteção de dados (Brasil, 2018).

Diante disso, o foco do compliance deve recair sobre a educação dos usuários e a consolidação de uma cultura organizacional sólida, com orientações claras sobre riscos e sinais de alerta, simulações realistas, treinamentos periódicos e ações contínuas de conscientização. Além dessas medidas, destaca-se a importância do consentimento informado para o uso de dados pessoais e do registro da marca da empresa no Instituto Nacional da Propriedade Industrial (INPI), como forma de evitar fraudes e usurpações que possam comprometer a identidade e a reputação da organização no meio digital.

CONSIDERAÇÕES FINAIS

A partir dessa pesquisa, é possível verificar que a atuação empresarial diante do crescente número de ataques por phishing deve ultrapassar a habitual adoção de medidas técnicas, de modo que as organizações precisam reconhecer que a vulnerabilidade principal está no fator humano e devem investir em uma cultura organizacional baseada na prevenção, educação digital e transparência.

O compliance digital emerge como instrumento de proteção, assim como elemento essencial de mitigar a responsabilidade jurídica institucional, capaz de diminuir os riscos e reduzir a exposição jurídica.

Ainda que a legislação brasileira tenha avançado com tipificação penal e a imposição de boas práticas através da Lei Geral de Proteção de Dados (Brasil, 1988), é imprescindível que a análise da responsabilidade civil empresarial considere as peculiaridades de cada caso. Empresas que adotam medidas preventivas adequadas não devem ser facilmente responsabilizadas por falhas exclusivamente atribuíveis ao consumidor ou a terceiros fraudadores.

O caminho para a segurança digital passa pelo compartilhamento de

responsabilidades entre empresa, consumidor e o Estado. As organizações devem liderar esse processo, mas é necessário que haja atuação conjunta e equilibrada de todos estes agentes envolvidos para que seja possível desenvolver um ecossistema mais seguro, justo e resiliente.

REFERÊNCIAS

BRASIL. **Constituição Federativa da República do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 08 jun. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 08 jun. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1999. **Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 08 jun. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 08 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 jun. 2025.

BRASIL. Lei nº 9.276, de 14 de maio de 1996. **Regula direitos e obrigações à propriedade industrial**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em: 08 jun. 2025.

COFENSE. **Case Study**: Advanced Phishing Simulation Campaign. Virginia, EUA, 2022. Acesso em: 08 jun. 2025. Disponível em: https://cofense.com/resources/. Disponível em: Acesso em: 08 jun. 2025.

COELHO, Fábio Ulhoa. **Manual de Direito Comercial**. Av. Dr. Cardoso de Melo, 1855 - 13o andar - Vila Olímpia, CEP 04548-005, São Paulo, SP, Brasil: RT - Revista dos Tribunais, 2022. Acesso em: 08 jun. 2025.

FRAPORTI, Simone; REIS, Zaida C.; FERRARI, Fernanda L.; et al. **Teoria geral da empresa**. Porto Alegre: SAGAH, 2018. E-book. p.2. ISBN 9788595024434. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595024434/. Acesso em: 08 jun. 2025.

KASPERSKY. **Brasil é o país com mais ataques de phishing por WhatsApp no mundo em 2022**. Disponível em: https://www.kaspersky.com.br/about/press-releases/brasil-e-o-pais-com-mais-ataques-de-phishing-por-whatsapp-no-mundo-em-2022-aponta-kaspersky. Acesso em: 6 jun. 2025.

LÓSSIO, Claudio Joel B. **Proteção de dados e compliance digital.** 2. ed. São Paulo: Almedina, 2023. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/. Acesso em: 30 out. 2025.

NORTE FILHO, Antônio Ferreira do; BENTES, Cybelle Taveira; BEMERGUY DE SOUZA, Elias Emanuel; ROSSETTI, Matheus Bezerra. A prática de phishing: pandemia e impactos no ordenamento jurídico criminal brasileiro. **Contribuciones a Las Ciencias Sociales**, São José dos Pinhais, v. 18, n. 4, p. 01–12, jan. 2025. Disponível em: Acesso em: 8 jun. 2025.

OLIVEIRA, Helena Sayuri Kato Mendes de. **Responsabilidade civil e a possibilidade de aplicação de limitação e excludentes da responsabilidade civil diante de ataques às bases de dados de empresas privadas**: uma análise sob a luz da LGPD e do CDC. 2022. Disponível em: https://dspace.mackenzie.br/items/070cf847-7924-4e6c-9816-50a72324713c. Acesso em: 10 jun. 2025.

OLIVO, CLEBER KIEL; SANTIN, A. O.; OLIVEIRA, L. E. S. **Avaliação de Características para Detecção de Phishing de E-mail**. Pontifícia Universidade Católica do Paraná, Curitiba–PR, Brasil, 2010. Disponível em: https://scholar.google.com.br/scholar?hl=pt-BR&as_sdt=0%2C5&q=OLIVO%2C+Cl%C3%A9ber.*+Avalia%C3%A7%C3%A3o+de+caracter%C3%ADsticas+para+detec%C3%A7%C3%A3o+de+phishing+de+email.+2012.+126+f.+&btnG. Acesso em: 6 jun. 2025.

REZENDE, Giulia Gabriele. **O phishing e a responsabilidade empresarial**: aspectos sobre as medidas protetivas do empresário face ao prejuízo de seus usuários. 2022. Disponível em: https://repositorio.ufu.br/handle/123456789/34807. Acesso em 7 jun. 2025.

SURFSHARK. **Global data breach statistics**: a 2024 recap. Disponível em: https://surfshark.com/research/study/data-breach-recap-2024?srsltid=AfmBOoryKV1jkbohco g8YeiATgvzOPbWAqkj3qX6qtKZWgb8KeIJ9qlA. Acesso em: 8 jun. 2025.

TARTUCE, Flávio; NEVES, Daniel Amorim A. **Manual de Direito do Consumidor** - Vol. Único - 14ª Edição 2025. 14. ed. Rio de Janeiro: Método, 2025. E-book. p.145. ISBN 9788530996963. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530996963/. Acesso em: 08 jun. 2025.