Universidade Federal do Rio Grande do Sul
Faculdade de Direito
Mestrado em Ciências Jurídicas e Sociais

Daniele Verza Marcon

Seguro contra Riscos Cibernéticos:
desafios para delimitar a garantia e promover a cibersegurança na era digital

Porto Alegre
2023

Daniele Verza Marcon

Seguro contra Riscos Cibernéticos:
desafios para delimitar a garantia e promover a cibersegurança na era digital

Dissertação apresentada como requisito parcial à obtenção do título de mestra em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.
Orientador: Prof. Dr. Fabiano Menke

Porto Alegre
2023

CIP - Catalogação na Publicação

Marcon, Daniele Verza
Seguro contra Riscos Cibernéticos: desafios para delimitar a garantia e promover a cibersegurança na era digital / Daniele Verza Marcon. -- 2023.
201 f.
Orientador: Fabiano Menke.

Dissertação (Mestrado) -- Universidade Federal do Rio Grande do Sul, Faculdade de Direito, Programa de Pós-Graduação em Direito, Porto Alegre, BR-RS, 2023.

1. Riscos cibernéticos. 2. Cibersegurança. 3. Segurança da informação. 4. Proteção de dados. 5. Contrato de seguro. I. Menke, Fabiano, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Daniele Verza Marcon

Seguro contra Riscos Cibernéticos:
desafios para delimitar a garantia e promover a cibersegurança na era digital

Dissertação apresentada como requisito parcial à obtenção do título de mestra em Ciências Jurídicas e Sociais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul.
Orientador: Prof. Dr. Fabiano Menke

Aprovada em: Porto Alegre, 1 de agosto de 2023

BANCA EXAMINADORA:

Prof. Dr. Fabiano Menke [*orientador*]
Universidade Federal do Rio Grande do Sul

Prof. Dr. Bruno Nubens Barbosa Miragem
Universidade Federal do Rio Grande do Sul

Prof. Dr. Guilherme Damásio Goulart
CESUCA

Profa. Dra. Maria Cláudia Mércio Cachapuz
Universidade Federal do Rio Grande do Sul

AGRADECIMENTOS

Aos meus pais, agradeço pelo amor e carinho, pelo apoio que chega de longe em diferentes formas e por incentivarem, sempre, a minha educação. Ao meu irmão, Giovanni, por estar sempre ao meu lado, aos meus avôs e às pequenas Antonia e Bibiana, por tornarem o caminho mais leve com muita imaginação. Aos meus dindos, Fabiana e Guilherme, pelo exemplo acadêmico de longa data e, também, às minhas tias, Rosana e Valéria, por apoiarem e incentivarem voos que eu não me sentia – e por vezes ainda não me sinto – capaz de alçar, mas que tento mesmo assim.

Um agradecimento especial à madrinha das madrinhas, Dinda Marta, por ter me apresentado à primeira biblioteca e, junto com minha mãe, por ter me guiado pela literatura de ficção. Por vezes eu tentei escrever este trabalho como se fosse um romance e tive dúvida sobre a efetiva fronteira entre os perigos da realidade e a ficção científica, mas imagino que essa dúvida constante seja natural aos que se propõem a estudar os impactos da tecnologia.

Aos queridos colegas do Souto Correa Advogados, agradeço pelo suporte ao longo de todas as etapas do mestrado. Meu agradecimento especial aos queridos estagiários da Furriel, por todas as palestras que ouviram sobre o tema desta dissertação sempre que me apresentaram alguma dúvida inocente sobre proteção de dados, contratos ou responsabilidade civil nos últimos dois anos, e aos caríssimos colegas Anna Laura Dal Molin, Daniela Dalsotto, Erika Donin, Luis Peretti, Luiza Guindani, Maria Eduarda Piccinini, Rodrigo Cantali, Thiago Borba e Valentina Rossi, por acompanharem de perto o desafio e por nunca terem deixado de incentivar a empreitada que assumi. Devo agradecer também ao Paulo Dornelles, por sanar muitas das dúvidas de TI que eu precisei entender para escrever o trabalho, e à Lisiane Silva, pelos *insights* práticos sobre a contratação de seguro cibernético.

A todos os amigos que acompanharam essa trajetória, de perto ou de longe, e que de algum modo se fizeram presentes: muito obrigada. Faço uma menção especial às queridas Bibiana Vaz Poeta Roenick e Gabriela Mânica Passos, com quem tive a felicidade de compartilhar todas as angústias e conquistas envolvidas no desafio que é o curso de mestrado e que prestaram apoio incessante do início ao fim desta etapa.

Aos colegas, sou grata por todo o aprendizado proporcionado nos últimos dois anos. Aos grandes mestres com quem tive o privilégio de aprender, agradeço por todos os ensinamentos, oportunidades e provocações, dentro do possível implementadas ao longo da dissertação. Deixo um agradecimento especial ao professor Bruno Miragem, por ter instigado a curiosidade sobre o seguro contra riscos cibernéticos em um seminário de sua disciplina, a

ponto de eu adotar o tema como objeto da minha dissertação; e, em conjunto com o professor Guilherme Damásio Goulart, por todas as valiosíssimas contribuições na banca de qualificação e, novamente, na banca de defesa da dissertação.

À professora Maria Cláudia Mércio Cachapuz, orientadora de toda a graduação e hoje uma grande amiga: obrigada pela confiança, pela parceria acadêmica e por todos os conselhos. E, claro, ao meu querido orientador, o professor Fabiano Menke: obrigada pela paciência, pelos desafios compartilhados no grupo de pesquisa e no estágio docente, por todas as oportunidades de aprendizado que eu tive o privilégio de usufruir durante o mestrado e por ser um incentivador constante de todos os desafios que me propus a assumir nos últimos dois anos. A atuação ética, a seriedade e o compromisso com os alunos, com a faculdade e com a pesquisa que aprendi com vocês estará sempre comigo.

Por fim, à Faculdade de Direito da Universidade Federal do Rio Grande do Sul, minha casa nos últimos oito anos: é um orgulho concluir mais esta etapa no nosso querido Castelinho! Eu dedico este trabalho a todos que acreditam e que *fazem* a educação pública, gratuita e de qualidade.

"*I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again*."

Robert S. Muller

RESUMO

A transição do mundo analógico para o digital veio acompanhada de ameaças cibernéticas e ataques recorrentes, como *phishing*, *malware*, *ransomware* e negação de serviço. A cibersegurança reflete a preocupação com a proteção de pessoas, organizações e infraestruturas críticas contra riscos relacionados ao uso da internet e de computadores. Isso significa que ataques bem-sucedidos podem afetar a confidencialidade, integridade e disponibilidade de dados pessoais, segredos de negócio e informações protegidas por direitos autorais, além de inviabilizar serviços essenciais de saúde, transporte e energia, por exemplo. Os prejuízos decorrentes de um incidente de segurança podem facilmente ultrapassar milhões de dólares e os danos, especialmente relacionados ao vazamento de dados pessoais não substituíveis, podem atormentar vítimas pelo restante da vida. Essas consequências motivaram a promulgação de leis sobre a notificação de incidentes de segurança e proteção de dados pessoais nas duas últimas décadas. Por um lado, as leis permitiram que as pessoas afetadas por um incidente de segurança soubessem que seus dados foram comprometidos e tomassem medidas para evitar danos maiores, como fraudes de identidade. Por outro lado, impuseram custos significativos às organizações, que incluem investigação forense, notificação de todas as pessoas afetadas, pagamento de indenizações por danos decorrentes do incidente em ações individuais e coletivas e multas impostas por autoridades públicas. Esse cenário originou um mercado de seguros específico que busca cobrir tanto prejuízos suportados diretamente pelas organizações quanto por terceiros. O problema é que riscos cibernéticos são extremamente voláteis e evoluem em conjunto com a tecnologia. Isso significa que uma ameaça que hoje é considerada grave pode ser substituída em poucas semanas por outra ainda pior e que soluções para mitigar prejuízos podem ser rapidamente contornadas por novas táticas, a exemplo das duplas extorsões nos ataques ransomware. Em meio a tanta instabilidade, o que é necessário considerar para se contratar um seguro contra risco cibernético com garantia suficiente? Para responder a essa pergunta, o objetivo da pesquisa é compreender as nuances do contrato de seguro contra riscos cibernéticos e analisar como as particularidades do risco cibernético e da cibersegurança podem afetar a delimitação da garantia. A pesquisa tem como base o método dedutivo e a revisão bibliográfica e busca verificar se o seguro contra riscos cibernéticos poderia ser uma ferramenta de gestão de riscos e de incentivo à implementação de medidas preventivas de cibersegurança e de que forma isso pode ser alcançado. Devido à amplitude do tema, a pesquisa considerou três recortes importantes: a distinção entre os conceitos de cibersegurança e segurança da informação e a delimitação da garantia securitária a partir do primeiro conceito; foram analisados apenas contratos de seguro empresariais, regrados pelo Código Civil; e o estudo do contrato de seguro foi focado nas questões relacionadas à delimitação da garantia.

Palavras-chave: Riscos cibernéticos. Cibersegurança. Segurança da informação. Proteção de dados. Contrato de seguro.

ABSTRACT

The transition from the analogic to the digital world came accompanied by cyber threats and recuring attacks, like phishing, malware, ransomware, and service denial. Cybersecurity reflects the preoccupation with the protection of people, organizations and critical infrastructures against risks related to the use of internet and computers. This means that well-succeed attacks might affect confidentiality, integrity and availability of personal data, business secrets and information protected by copyrights, besides precluding essential services such as health, transport, and energy. The losses related to a security incident might easily surpass millions of dollars, and damages, especially regarding the breach of non-replaceable personal data, might torment the victims for the rest of their lives. Those consequences motivated the promulgation of laws regarding data breach notification and the protection of personal data in the last two decades. On the one hand, the laws allowed people affected by a security incident to know their data has been compromised and take measures to prevent further damages, such as identity theft. On the other hand, the laws imposed significant costs to organizations, including forensic investigation, the notification of all people affected, payment of indemnification for damages resulting from the incident in individual suits and class actions and fines imposed by public authorities. This scenario originated a specific market that aims at covering both the losses experienced directly by organizations and third parties. The problem is that cyber risks are extremely volatile and evolve alongside technology. This means that a threat considered major today might be replaced in a few weeks for another that is even worse, and that solutions to mitigate damages might be rapidly circumvented by new tactics, such as double extortion in ransomware attacks. Among so many instabilities, what should be considered for contracting a cyberinsurance with enough coverage? To answer that question, the objective of this research is to understand the nuances of an insurance contract against cyber risks and to analyze how the particularities of cyber risks and cybersecurity might affect the definition of the bond. The research is based on the deductive method and bibliographic review, and aims to verify if cyberinsurance could be a risk management tool to incentive the implementation of preventive measures for cybersecurity, and how this objective could be achieved. Due to the extension of the subject, the research considered three important cut-offs: the distinction between the concepts of cybersecurity and information security and the delimitation of the security bond according to the first concept; only business insurance contracts regulated by the Civil Code were analyzed; and the study of insurance contracts focused on issues related to the definition of the bond.

Keywords: Cyber risks. Cybersecurity. Information security. Data protection. Insurance contract.

LISTA DE ABREVIATURAS E SIGLAS

ABREVIATURA	SIGNIFICADO
AIG	*American International Group*
AIG Brasil	AIG Seguros Brasil S.A.
Allianz	Allianz Seguros S.A.
ANPD	Autoridade Nacional de Proteção de Dados
APDSI	Associação para a Promoção e Desenvolvimento da Sociedade da Informação
AXA	Axa Seguros S.A.
CDC	Código de Defesa do Consumidor
CNseg	Confederação Nacional das Seguradoras
DDoS	*Distributed Denial of Service* ou ataque de negação de serviço distribuído
ENISA	*European Unian Agency for Network and Information Security*
FBI	*Federal Bureau of Investigation*
FenSeg	Federação Nacional de Seguros Gerais
FTC	*Federal Trade Commission*
GDPR	*General Data Protection Regulation*
INFOSEC	*Information Security*
ISL	*Internet Security Liability*
LGPD	Lei Geral de Proteção de Dados
LMA	Lloyd's Market Association
MCI	Marco Civil da Internet
NIST	*National Institute for Standards and Technology*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
RaaS	*Ransomware as a Service*
SEC	*Securities and Exchange Commission*
SSIC	Secretaria de Segurança da Informação e Cibernética
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
Susep	Superintendência de Seguros Privados
TJSP	Tribunal de Justiça de São Paulo

Tokio Marine	Tokio Marine Seguradora S.A.
Zurich	Zurich American Insurance Co.
Zurich Brasil	Zurich Minas Brasil Seguros S.A.

SUMÁRIO

INTRODUÇÃO

No final de novembro de 2013, a rede de lojas de varejo norte-americana Target foi alvo de um ataque cibernético. Informações detalhadas de mais de 40 milhões de cartões de crédito e dados pessoais de mais de 70 milhões de clientes foram vazados e vendidos em sites de fraudes. O incidente foi um verdadeiro desastre. Além de uma queda de aproximadamente 46% nos lucros esperados para o período[1] (próximo ao Natal e à *Black Friday*), a Target amargou um prejuízo superior a US$ 300 milhões com o pagamento de reembolsos bancários, multas, monitoramento de crédito, honorários advocatícios para defesas em mais de 90 processos judiciais e acordos (somente essa última rubrica somou quase US$ 89 milhões)[2].

A origem? Uma tentativa bem-sucedida de *phishing*. *Hackers*[3] enviaram um e-mail para um funcionário da Fazio Mechanical, fornecedora da Target nos Estados Unidos. O funcionário abriu o e-mail, clicou no *link* e baixou um *malware* que não foi detectado pela versão gratuita de antivírus que a Fazio Mechanical utilizava na época. Essa falha permitiu que os *hackers* obtivessem as credenciais do fornecedor para entrarem nos sistemas da Target. Ou seja, não houve um ataque direto à Target. O problema é que, apesar de cuidar dos próprios sistemas, a Target não exigiu que os seus fornecedores adotassem medidas mínimas de segurança – como o uso de um antivírus adequado[4]. E isso bastou. Esse caso contribuiu para que 2013 ficasse

---

[1] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 3.

[2] NIEVES, Angela M. Cyber Insurance Today: Saving It before It Needs Saving. **Catholic University Journal of Law and Technology**, vol. 29, n. 1, 2020, p. 115.

[3] Ao longo do trabalho, optou-se por utilizar o termo "hacker" com relação às pessoas responsáveis por ataques cibernéticos, já que a palavra foi popularizada na mídia e tem sido adotada em diversas publicações acadêmicas. Não se descura, porém, que o termo técnico correto para o uso de conhecimentos de informática para finalidades ilícitas é "cracker". O glossário da sociedade da informação da APDSI define "cracker" ou "pirata informático" como a "[p]essoa que explora as falhas da segurança de um sistema com o intuito de violar a sua integridade, destruindo ou alterando a informação ali residente, ou ainda de copiar fraudulentamente os seus ficheiros" e indica que o "pirata informático (*cracker*) é um entusiasta da informática (*hacker*) que usa os seus conhecimentos para fins indevidos" (ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Glossário da sociedade da informação**. 4 ed. Lisboa, jun. 2019, p. 108). De acordo com esse mesmo glossário, "hacker" ou "entusiasta da informática" é a "[p]essoa com amplos conhecimentos de computadores e redes, que se introduz nos sistemas alheios com o fim de aprender sobre os mesmos, encontrar os seus pontos fracos, sem contudo querer causar prejuízos ou receber em troca algum benefício económico". Em nota, o glossário esclarece, porém, que "[e]xiste também quem considere este conceito no sentido oposto ao indicado, isto é, que o entusiasta da informática é o indivíduo que vai querer mesmo provocar prejuízos ou obter alguma vantagem ilícita da sua actividade; nesse sentido, o entusiasta da informática (*hacker*) torna-se sinónimo de pirata informático (*cracker*)" (*Ibidem*, p. 56).

[4] KASSNER, Michael. Anatomy of the Target data breach: Missed opportunities and lessons learned. **ZDNet**, 02.02.2015. Disponível em: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/?ref=hackernoon.com. Acesso em: 12 jan. 2023.

conhecido nos Estados Unidos como "*Year of the Mega Data Breach*" e "*Year of the Retailer Breach*"[5].

Um ano depois, em novembro de 2014, foi a vez da Sony Pictures Entertainment[6]. A empresa estava prestes a lançar o filme *The Interview*, uma comédia em que dois agentes da CIA são enviados para assassinar o líder da Coreia do Norte, Kim Jong-un. O grupo de *hackers* norte-coreanos intitulado "GOP" ou *Guardians of Peace* invadiu os sistemas da Sony em retaliação. A origem do ataque foi, novamente, o furto de credenciais de um dos administradores do sistema da Sony, obtidas por meio de *phishing.*

Após invadirem o sistema, os *hackers* inseriram um *malware* que apagou todas as informações armazenadas em 3.262 computadores pessoais e 837 servidores da Sony[7]. O apagão foi complementado pelo vazamento de 40 gigabytes de dados pessoais não encriptados, incluindo números de seguridade social, endereços residenciais, lista de salários e bônus de funcionários, informações de passaporte e vistos de atores e equipes envolvidas nos filmes produzidos pela Sony[8].

A particularidade do caso da Sony é que o incidente afetou não apenas consumidores e funcionários: os *hackers* divulgaram mais de 20 mil e-mails trocados por diretores da companhia, incluindo o presidente Steve Mosko e a executiva Amy Pascal. Além de informações sensíveis de negócio, os e-mails continham comentários pessoais envolvendo amigos, colegas e o próprio presidente Barack Obama. Acordos com ex-funcionários custaram à companhia mais de US$ 15 milhões – e essa é apenas uma pequena parte do prejuízo[9].

---

[5] MARTIN-VEGUE, Tony. Will the real "Year of the Data Breach" please stand up? **Hackernoon**, 04 jan. 2018. Disponível em: https://hackernoon.com/will-the-real-year-of-the-data-breach-please-stand-up-744ab6f63615. Acesso em 05 jan. 2023.

[6] Em abril de 2011, a Sony Inc., também foi protagonista de um incidente de segurança catastrófico que envolveu o vazamento de dados pessoais de cerca de 77 milhões de usuários do Playstation (BAKER, Liana B.; FINKLE, Jim. Sony PlayStation suffers massive data breach. **Reuters**, 26 abr. 2011. Disponível em: https://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110427. Acesso em: 12 jan. 2023). Em maio de 2011, a companhia divulgou um prejuízo estimado de 171 milhões de dólares com o incidente (SCHREIER, Jason. Sony Estimates $ 171 Million Loss From PSN Hack. **Wired**, 23 mai. 2011. Disponível em: https://www.wired.com/2011/05/sony-psn-hack-losses/. Acesso em: 12 jan. 2023).

[7] ELKIND, Peter. Sony Pictures: Inside the Hack of the Century. **Fortune**, 25 jun. 2015. Disponível em: https://fortune.com/2015/06/25/inside-sony-pictures-hack/. Acesso em: 12 jan. 2023.

[8] ZETTER, Kim. Sony Got Hacked Hard: What We Know and Don't Know So Far. **Wired**, 3 dez. 2014. Disponível em: https://www.wired.com/2014/12/sony-hack-what-we-know/. Acesso em: 12 jan. 2023. Os hackers teriam acessado mais de 100 terabytes de dados, incluindo roteiros e filmes ainda não lançados: "But more importantly for Sony's bottom line, the stolen data also includes the script for an unreleased pilot by Vince Gilligan, the creator of Breaking Bad as well as full copies of several Sony films, most of which have not been released in theaters yet. These include copies of the upcoming films Annie, Still Alice and Mr. Turner."

[9] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 150-152.

Intitulado "*The Hack of the Century*"[10], o caso da Sony contribuiu para que o ano de 2014 fosse coroado como "*Year of the Data Breach*"[11].

A história de vazamentos de dados não parou em 2014. Na verdade, o título "*Year of the Data Breach*" se parece mais com o título de Miss Universo do que com títulos do *Guiness Book*, pois já vinha sendo repassado ano a ano desde 2005. Talvez para fazer jus ao título, os anos seguintes foram ainda piores.

Em 2015, 3,2 milhões de usuários foram afetados pelo vazamento de dados do aplicativo Ashley Madison, desenvolvido para pessoas interessadas em manter casos extraconjugais. O aplicativo cobrava uma taxa de US$ 19 para deletar dados de usuários que optassem por encerrar a conta, mas, ainda assim, milhões de dados foram mantidos. Os prejuízos foram muito além do aspecto econômico: casamentos acabaram, algumas pessoas foram demitidas, outras foram vítimas de extorsão e algumas se suicidaram[12]. Esse e outros vazamentos renderam ao ano de 2015 o título de *Year of the Data Breach*.

Em 2016, a Yahoo divulgou que dois incidentes ocorridos em agosto de 2013 e dezembro de 2014 afetaram mais de 1,5 bilhões de dados[13]. Em 2018, a *Securities and Exchange Commission* dos Estados Unidos multou a plataforma em US$ 35 milhões pela omissão da informação ao mercado sobre o incidente – um valor baixo, considerando a quantidade de dados comprometidos. Note-se que o Yahoo não foi responsabilizado pelo vazamento dos dados ou pela falta de medidas adequadas de segurança, mas apenas por omitir fato relevante de seus investidores[14]. Em 2017, a plataforma divulgou atualizações sobre os vazamentos, indicando que todos os usuários com contas ativas em 2013 tiveram informações vazadas – são mais de 3 bilhões de contas[15]. O ano de 2016 também recebeu o título de *Year of the Data Breach*.

---

[10] ELKIND, Peter. Sony Pictures: Inside the Hack of the Century. **Fortune**, 25 jun. 2015. Disponível em: https://fortune.com/2015/06/25/inside-sony-pictures-hack/. Acesso em: 12 jan. 2023.

[11] MARTIN-VEGUE, Tony. Will the real "Year of the Data Breach" please stand up? **Hackernoon**, 04 jan. 2018. Disponível em: https://hackernoon.com/will-the-real-year-of-the-data-breach-please-stand-up-744ab6f63615. Acesso em 05 jan. 2023.

[12] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 146-147.

[13] FREEDMAN, Linn Foster. 2016 was the Year of the Data Breach. **Data Privacy and Cybersecurity Insider**, 29 dez. 2016. Disponível em: https://www.dataprivacyandsecurityinsider.com/2016/12/2016-was-the-year-of-the-data-breach/?ref=hackernoon.com. Acesso em: 12 jan. 2023.

[14] KASTRENAKES, Jacob. SEC issues $35 million fine over Yahoo failing to disclose data breach. **The Verge**, 24 abr. 2018. Disponível em: https://www.theverge.com/2018/4/24/17275994/yahoo-sec-fine-2014-data-breach-35-million. Acesso em: 12 jan. 2023.

[15] LARSON, Selena. Every single Yahoo account was hacked - 3 billion in all. **CNN Money**, 04 out. 2017. Disponível em: https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html?ref=hackernoon.com. Acesso em: 12 jan. 2023.

O ano de 2017 contou com ao menos três vazamentos catastróficos: Experian, Uber[16] e Equifax. O caso da Equifax, uma das três maiores agências de cadastro de consumidores dos Estados Unidos, é especialmente interessante. Cerca de 400 funcionários da Equifax utilizavam o software Apache Struts, de código aberto. Em março de 2017, a Equifax foi informada sobre a necessidade de atualização desse software, o que foi prontamente providenciado para 399 funcionários. Porém, o e-mail disparado pela equipe de segurança não foi enviado para um funcionário, que não atualizou o software. *Hackers* descobriram essa vulnerabilidade e tiveram acesso ao sistema da Equifax e a 145 milhões de dados, incluindo números de seguridade social que foram armazenados sem criptografia. Como observam Solove e Hartzog, a ironia do caso é que clientes que pagavam a Equifax para monitoramento de crédito passaram a receber o serviço gratuito pelo comprometimento de seus próprios dados[17]. Evidentemente, o ano de 2017 recebeu o título de *Year of the Data Breach*.

Os exemplos referidos até aqui são frequentemente encontrados na literatura sobre segurança de dados e exemplificam um dos motivos pelos quais os Estados Unidos ocupam o primeiro lugar em rankings de vazamento de dados. O histórico do Brasil é ainda tímido em comparação aos casos referidos acima, mas nem por isso deixa de ser preocupante.

Incidentes de segurança envolvendo dados pessoais foram multiplicados, em especial nos últimos três anos, diante da crescente digitalização de atividades que ainda resistiam à tecnologia e do trabalho remoto que ganhou espaço durante a pandemia de COVID-19. Talvez o maior incidente de segurança conhecido no Brasil seja o episódio ocorrido em dezembro de 2020, quando dados pessoais de 243 milhões de brasileiros ficaram expostos na internet por falhas no sistema de segurança do Ministério da Saúde (os dados incluíam nome completo, CPF, endereço e telefone de pessoas inscritas do Sistema Único de Saúde e planos de saúde particulares). Em janeiro de 2021, um novo vazamento de origem não confirmada afetou dados

---

[16] Hackers atacaram os sistemas da Uber em outubro de 2016, mas o incidente foi divulgado em novembro de 2017. Foram vazadas informações pessoais de 57 milhões de clientes no mundo todo, incluindo 600 mil informações sobre a habilitação de motoristas nos Estados Unidos, conforme informações disponibilizadas pela CEO da Uber à época (KHOSROWSHAHI, Dara. 2016 Data Security Incident, **Uber**, 21 nov. 2017. Disponível em: https://www.uber.com/newsroom/2016-data-incident/. Acesso em: 15 jan. 2023). A Uber admitiu o pagamento de US$ 100 milhões aos *hackers* para a exclusão de dados acessados indevidamente (FINKLE, Jim; SOMERVILLE, Heather. Uber's messy data breach collides with launch of SoftBank deal, **Reuters**, 22 nov. 2017. Disponível em: https://www.reuters.com/article/us-uber-cyberattack-idUSKBN1DM2F9. Acesso em: 15 jan. 2023). O relatório sobre seguros contra riscos cibernéticos da OCDE também indicou que a empresa pagou US$ 148 milhões em acordos com autoridades públicas referentes às multas impostas em decorrência do vazamento (OCDE. Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020, p. 17. Disponível em: www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf).

[17] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 93-95.

pessoais de 223 milhões de pessoas. Em ambos os casos, o número de registros afetados foi superior à população do país, pois incluíram dados de pessoas já falecidas[18].

Os eventos não se resumem ao vazamento de dados (violação de confidencialidade), alcançando também a integridade e (in)disponibilidade. O ataque cibernético que paralisou o Superior Tribunal de Justiça a partir do dia 3 de novembro de 2020 impediu acesso a milhões de processos pelas partes e pelos próprios Ministros, causando a suspensão de prazos por quase uma semana; o incidente foi reconhecido pela Corte como "o pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade"[19]. Em 19 de agosto de 2021, a Renner foi alvo de um ataque *ramsonware* e ficou dois dias com o *e-commerce* fora do ar. A varejista negou ter feito o pagamento dos US$ 20 milhões solicitados para o resgate de dados tornados indisponíveis[20].

A relevância social e econômica de incidentes de segurança e vazamentos de dados se inicia com a dependência de organizações públicas e privadas com relação à internet, à computação em nuvem e à digitalização. A tecnologia modificou profundamente a forma como dados são coletados, analisados e armazenados e a mesma facilidade para conectar sistemas e facilitar o fluxo de dados em nível internacional também permite espalhar, de forma sistêmica, ataques que antes eram direcionados apenas contra um único alvo. A *escalabilidade* proporcionada pela internet e a possibilidade de ataques remotos alteram substancialmente a dimensão de uma violação de dados.

A isso se soma o reconhecimento de um *dever de segurança*[21] cujo descumprimento acarreta consequências jurídicas. Toda entidade que coleta e armazena dados pessoais está (e

---

[18] ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil — e suas consequências. **Jota**, 28 jan. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 12 jan. 2023.

[19] SUPERIOR TRIBUNAL DE JUSTIÇA. Comunicado da Presidência do STJ, 9 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 13 jan. 2023.

[20] LOPES, André. Após ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos. **Exame**, 20 ago. 2021. Disponível em: https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/. Acesso em: 13 jan. 2023.

[21] Na lição de Eros Grau, o "*dever jurídico* consubstancia precisamente uma vinculação ou limitação imposta à vontade de quem por ele alcançado. Definido como tal pelo ordenamento jurídico, o dever há de ser compulsoriamente cumprido, sob pena de sanção jurídica — o seu não atendimento configura comportamento ilícito". O conceito difere da noção de "obrigação", que, em sentido estrito, "*consubstancia'* um vínculo em razão do qual uma pessoa (devedor) deve a outra (credor) o cumprimento de uma certa prestação. A obrigação consubstancia um *direito relativo,* na medida em que o crédito que dela decorre apenas pode ser exigido, pela pessoa ou pluralidade de pessoas dele titular, contra a pessoa ou pluralidade de pessoas na situação de devedor." (GRAU, Eros Roberto. Nota sobre a Distinção entre Obrigação, Dever e Ônus. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 77, 1982, p. 178-179). A compreensão da cibersegurança como um *dever jurídico* também pode ser sustentada a partir da função hermenêutica da boa-fé objetiva, a qual estão associados os deveres de proteção (MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. São Paulo: Saraiva, 2018, p. 426-430). O dever de proteção volta-se à integridade da esfera jurídica da parte de

sempre esteve) sujeita ao risco de um incidente de segurança, ainda que tais dados sejam mantidos exclusivamente em meios físicos. A concepção de "segurança da informação" engloba a proteção da *confidencialidade*, da *integridade* e da *disponibilidade* de informações, estejam elas armazenadas de forma digital ou não. Assim, excluídos os computadores da equação, o acesso não autorizado a fichas cadastrais, prontuários médicos ou quaisquer outros documentos físicos contendo dados pessoais ainda será um vazamento de dados[22].

Essa é a concepção adotada pelo artigo 6º, inciso VII, da LGPD, que trata do princípio da segurança, bem como pelos artigos 46 a 49, que tratam da segurança e do sigilo de dados. A lei brasileira exige a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão", independentemente do meio em que os dados estiverem armazenados[23]. O Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, editado em outubro de 2021 pela ANPD, igualmente contém recomendações para que documentos físicos contendo dados pessoais sejam guardados em gavetas, não sobre as mesas, e que pessoas envolvidas no tratamento assinem acordos de confidencialidade, o que pode evitar vazamento verbal de informações[24]. Porém, tais episódios tendem a ser pontuais e restritos.

O *dever de segurança* de dados pessoais foi introduzido de forma expressa e específica na legislação brasileira somente em agosto de 2018, com a LGPD – que entrou em vigor apenas em setembro de 2020, após idas e vindas e alguns Decretos. Antes disso, questões sobre segurança e sigilo de dados dependiam de interpretação, usualmente amparada no artigo 5º, incisos X e XII, da Constituição[25] e nos deveres de proteção derivados da boa-fé objetiva, ou

---

determinada relação e tem por função evitar prejuízos "que decorreriam da própria relação de obrigação considerada como um fato social tendencialmente produtor de danos em razão da especial aproximação ("contato social qualificado") que promove entre as partes" (MARTINS-COSTA, Judith. **Comentários ao novo Código Civil**: do inadimplemento das obrigações, vol. V. Tomo II. 2 ed. Rio de Janeiro: Forense, 2009, p. 89). O "contato social qualificado", neste caso, se dá pelo tratamento de dados e disponibilização de serviços para terceiros a partir de alguma atividade desenvolvida pela organização.

[22] DE GROOT, Juliana. The History of Data Breaches. **Data Insider**, 12 nov. 2018. Disponível em: https://digitalguardian.com/blog/history-data-breaches. Acesso em 05 jan. 2023.

[23] Princípios como necessidade, finalidade, adequação e prevenção igualmente revelam o intuito da LGPD de assegurar proteção efetiva aos dados pessoais, um direito reconhecido como fundamental apenas em 2022, quando foi inserido no artigo 5º, inciso LXXIX, da Constituição pela Emenda Constitucional nº 115.

[24] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, Brasília, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf.

[25] Sobre o assunto, é interessante conferir o texto publicado na década de 1990 pelo professor Tércio Sampaio Ferraz Jr., escrito no contexto da discussão sobre sigilo fiscal e posteriormente adotado pela jurisprudência do Supremo Tribunal Federal, com adaptações (FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993). As ideias desse texto foram analisadas novamente por Rafael Mafei Rabelo Queiroz e Paula Pedigoni Ponce e confrontadas com recentes decisões do STF e com a LGPD (QUEIROZ, Rafael

se restringiam à proteção do atributo de confidencialidade (sem tratar da integridade ou disponibilidade), conforme artigo 13 do Decreto nº 8.771/2016. Assim, pode-se dizer que o risco de um incidente de segurança era um mero figurante no palco de tantas outras ameaças. Um figurante, todavia, com o qual muitas organizações estavam dispostas a trabalhar.

A digitalização facilitou a coleta, o armazenamento e o processamento de volumes expressivos de dados – *Big Data* – e manter vastas bases de dados se tornou vantajoso: na era digital, informação é poder e dados podem ser transformados em dinheiro[26]. Além disso, organizações não eram obrigadas a divulgar incidentes de segurança e não havia delimitação clara sobre responsabilidade caso essa informação fosse ocultada. Sem publicidade e sem uma legislação preocupada com a proteção de dados pessoais, custos de uma violação de dados são menores. Essas observações se aplicam tanto ao Brasil quanto aos Estados Unidos.

Nos Estados Unidos, o cenário começou a mudar no início dos anos 2000, com a edição de leis obrigando a notificação de vítimas em caso de vazamento de dados – *data breach notification*. Em 2003, o estado da Califórnia editou a lei que serviu de modelo ao restante do país após um vazamento de dados da ChoicePoint, em fevereiro de 2005. Essa empresa fornecia relatórios com o histórico pessoal de candidatos para que organizações utilizassem em processos de contratação. Para isso, a ChoicePoint mantinha registros de todas as pessoas maiores de idade dos Estados Unidos, o que incluía nome, endereço, números de carteira de habilitação e seguridade social e histórico de crédito.

A questão é que as pessoas não sabiam que seus dados estavam sendo tratados pela ChoicePoint. Como a California era o único estado com obrigação legal de notificação, a ChoicePoint informou apenas 35 mil pessoas residentes naquele estado sobre o vazamento. Uma semana depois, entre os dias 16 e 17 de fevereiro de 2005, Procuradores Gerais de 38 estados americanos exigiram o mesmo tratamento às pessoas residentes em seus territórios[27], solicitação que acabou sendo cumprida pela ChoicePoint. Ao todo, aproximadamente 162 mil pessoas foram afetadas e ao menos 750 foram vítimas de fraudes de identidade por causa desse vazamento.

Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, n. 1, v. 1, p. 64-90, 2020).

[26] Ver mais em: ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

[27] SCALET, Sarah D. ChoicePoint Data Breach: The Plot Thickens. **CSO**, 01 mai. 2005. Disponível em: https://www.csoonline.com/article/2118146/choicepoint-data-breach--the-plot-thickens.html. Acesso em: 13 jan. 2023.

O caso ganhou a atenção da mídia e dos governos estaduais, não pela relevância do vazamento (que é mínima diante de casos como Target e Yahoo), mas pelo fato de ter sido um dos primeiros a ser publicizado. Como resultado, no final de 2006, 33 estados norte-americanos seguiram o exemplo da Califórnia e, em 2008, apenas seis estados ainda não possuíam lei específica sobre *data breach notification*[28]. E foi justamente esse modelo que inspirou o artigo 48 da LGPD, que trata da notificação em caso de incidente de segurança no Brasil, inaugurado apenas em 2018[29].

A possibilidade de publicização trouxe transparência às pessoas afetadas por um incidente de segurança – antes, elas provavelmente descobririam que tiveram seus dados vazados apenas quando fossem vítimas de alguma fraude de identidade. E, obviamente, trouxe mais custos. Ao notificar clientes e fornecedores, organizações passaram a enfrentar o risco (muitas vezes concretizado) de demandas individuais e coletivas buscando reparação de danos decorrentes do incidente. O gerenciamento da crise em sigilo deu lugar ao escrutínio público e, com ele, veio o desafio de recuperar a reputação perante o mercado e de arcar com penalidades administrativas impostas por autoridades públicas.

Com isso, o risco relacionado ao custo de uma violação de dados nos Estados Unidos deixou de ser irrelevante e as apólices de seguro se tornaram atrativas – uma virada significativa da década de 1990 para os anos 2000. As primeiras apólices cobriam principalmente prejuízos de terceiros decorrentes de violações de dados pessoais e evoluíram posteriormente para cobrir prejuízos suportados pelas próprias organizações em razão de violação de cibersegurança (que não se restringia a dados pessoais). Até meados de 2008, os prêmios de seguro contra riscos cibernéticos movimentaram aproximadamente US$ 500 milhões ao ano, mas tiveram um crescimento significativo a partir de 2012, com o aumento de ataques e a orientação da Securities and Exchange Commission (SEC) para que companhias listadas no mercado de valores mobiliários informassem seus perfis de risco cibernético e eventuais coberturas securitárias contratadas. Atualmente, seguros contra risco cibernético movimentam mais de US$ 5,5 bilhões ao ano em prêmios, aumento atribuído à frequência de ataques *ramsonware*[30].

---

[28] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 38-40.
[29] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469–483, 2018.
[30] JOHANSMEYER, Tom. The Cyber Insurance Market Needs More Money. **Harvard Business Review**, 10 mar. 2022. Disponível em: https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money. Acesso em: 16 jan. 2023.

O relatório anual divulgado pela IBM Security em parceria com o Ponemon Institute[31] apontou que o custo total médio de uma violação de dados entre março de 2021 e março de 2022 foi de US$ 4,35 milhões. Trata-se de um prejuízo 12,7% maior com relação ao ano de 2020, que apontou uma média de US$ 3,86 milhões, e o mais alto apurado desde a publicação do primeiro relatório, em 2016. A pesquisa considera dados de dezessete países e os Estados Unidos seguem em primeiro lugar com o maior custo total médio (US$ 9,44 milhões). O Brasil permaneceu abaixo da média geral, com um custo de US$ 1,38 milhão, ocupando a 16ª posição. Ainda assim, trata-se de um crescimento de 27,2% em relação ao relatório de 2021, quando o custo médio brasileiro ficou em US$ 1,08 milhão.

O cálculo da IBM considera prejuízos relacionados à perda de negócios, detecção e encaminhamento, notificação e resposta pós-violação. Em 2022, a maior parte do prejuízo envolveu a detecção e encaminhamento, o que inclui atividades forenses e investigativas, serviços de avaliação e auditoria, gerenciamento de crises e comunicados a executivos e conselhos. É a primeira vez em seis anos que esse custo supera a média dos prejuízos incorridos com a perda de negócios[32].

Outro ponto interessante é que o estudo considera violações envolvendo 2.200 a 102.000 registros, apontando um custo médio por registro de US$ 164 (novamente, o custo mais alto desde 2016)[33]. Essa apuração permite mensurar o prejuízo médio para organizações com bancos de dados menores – um parâmetro valioso, já que nem todos os incidentes terão a proporção dos casos da Target, Yahoo e Equifax – mas também indica uma limitação dos resultados aqui referenciados.

A IBM também reportou que as cinco principais causas de violação de dados em 2022 foram credenciais comprometidas, *phishing*, configuração incorreta da nuvem, vulnerabilidade em software de terceiros e usuário interno mal-intencionado. Essas causas são discutidas na contratação de um seguro contra risco cibernético e, a depender da forma como o ataque iniciar, a segurada poderá perder o direito à execução da garantia.

A adoção de mecanismos de inteligência artificial[34], criptografia, autenticação multifatorial, testes de vulnerabilidade e treinamentos internos permitiu a redução de prejuízos.

---

[31] IBM Security. **Relatório de custo da violação de dados de 2022**. São Paulo, jul. 2022. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 09 jan. 2023.

[32] IBM Security. **Relatório de custo da violação de dados de 2022**. São Paulo, jul. 2022, p. 12Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 09 jan. 2023.

[33] *Ibidem*, p. 9.

[34] Por exemplo, o Microsoft Sentinel é uma ferramenta disponibilizada pela Microsoft para usuários do serviço de nuvem da Azure que auxilia na detecção e resposta a ameaças de segurança com o apoio de inteligência artificial e algoritmos de *machine learning*. Ver mais em: https://learn.microsoft.com/pt-br/azure/sentinel/overview. Acesso em: 01 mai. 2023. Outros exemplos consolidados no mercado incluem a Sophos e a Fortinet, que fornecem

Por outro lado, o trabalho remoto, migração para a nuvem e complexidade de sistemas de segurança podem majorar os custos. Novamente, são fatores relevantes que podem influenciar não apenas a definição do valor da garantia, mas do próprio prêmio a ser pago à seguradora. Ainda assim, por maiores que sejam as precauções, basta uma única falha para dar início a um incidente (como no caso da Equifax). Não só isso: é provável que os ataques sejam vez mais frequentes (dentre as 550 empresas analisadas no relatório da IBM, 83% já sofreram mais de uma violação[35]), preocupação externada inclusive no relatório sobre os maiores riscos globais para o Fórum Econômico Mundial de 2023[36].

Esse cenário fez com que seguros contra riscos cibernéticos movimentassem, no Brasil, R$ 123 milhões entre janeiro e setembro de 2022, um crescimento de 75% com relação ao mesmo período do ano anterior[37]. Em 2021, a FenSeg já havia divulgado um aumento de 161% com relação a 2020[38], demonstrando a uma notória tendência de crescimento desse mercado para os próximos anos.

A edição de 2021 do Glossário do Seguro da CNSeg mencionou o seguro contra risco cibernético como um tipo de seguro de responsabilidade civil. A modalidade tem por objetivo cobrir danos diretos decorrentes de "ataques cibernéticos que geram perdas materiais, imateriais e de conteúdo informacional ou geram ressarcimento contra reclamações de terceiros por violação da privacidade, uso indevido de informações ou violação de direitos de propriedade intelectual"[39].

A cibersegurança, por outro lado, presta-se a controlar os riscos cibernéticos e reflete a preocupação com a proteção de pessoas, organizações e infraestruturas críticas contra ameaças

---

software para detecção de ameaças cibernéticas, auxiliando os controles dos departamentos de tecnologia da informação.

[35] IBM Security. **Relatório de custo da violação de dados de 2022**. São Paulo, jul. 2022, p. 5. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 09 jan. 2023.

[36] Conforme consta do relatório, "Alongside a rise in cybercrime, attempts to disrupt critical technology-enabled resources and services will become more common, with attacks anticipated against agriculture and water, financial systems, public security, transport, energy and domestic, space-based and undersea communication infrastructure. Technological risks are not solely limited to rogue actors. Sophisticated analysis of larger data sets will enable the misuse of personal information through legitimate legal mechanisms, weakening individual digital sovereignty and the right to privacy, even in well-regulated, democratic regimes." WORLD ECONOMIC FORUM. **The Global Risks Report 2023**. 18ª ed, Geneva, 2023, p. 8. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[37] PUENTE, Beatriz. Seguros de riscos cibernéticos têm crescimento de 75% nas contratações. **CNN Brasil**, 29 nov. 2022. Disponível em: https://www.cnnbrasil.com.br/nacional/seguros-de-riscos-ciberneticos-tem-crescimento-de-75-nas-contratacoes/. Acesso em: 13 jan. 2023.

[38] FEDERAÇÃO NACIONAL DE SEGUROS GERAIS. Ataques hackers movimentam venda de seguros contra risco cibernético, 22 out. 2021. Disponível em: https://fenseg.org.br/noticias/ataques-hackers-movimentam-venda-de-seguros-contra-risco-cibernetico.html. Acesso em: 18 ago. 2022.

[39] CONFEDERAÇÃO NACIONAL DAS SEGURADORAS. Glossário do Seguro, 2021, p. 77. Disponível em: https://cnseg.org.br/data/files/3A/45/72/CA/A253D710B2DC74C73A8AA8A8/NOVO_GLOSS%C3%81RIO%20(ONLINE).pdf. Acesso em: 13 jan. 2023.

relacionadas ao uso da internet e de recursos de computação[40]. O risco cibernético pode afetar informações, sistemas e redes utilizados por uma organização, incluindo a violação de dados pessoais de clientes, funcionários e prestadores de serviço e de informações confidenciais relacionadas ao negócio. O impacto não se restringe à violação da confidencialidade, afetando também a integridade e a disponibilidade de sistemas e serviços – o que pode gerar prejuízos operacionais, como a impossibilidade de realizar vendas via *e-commerce.*

Diversos fatores contribuem para dificultar a previsibilidade de incidentes e de suas consequências. O principal talvez seja pelo fato de que sistemas informáticos são utilizados por humanos. São humanos que podem comprometer a segurança, clicar em um link recebido via *phishing,* abrir espaço para *malware* e ignorar alertas de antivírus. Mas não só isso.

O risco cibernético é *amplo*, pois afeta tanto pessoas físicas com seus dispositivos pessoais quanto organizações públicas e privadas que utilizam a internet e sistemas de software. É *obscuro*, pois há poucos dados pretéritos para mensurar, com precisão, a dimensão de um incidente, especialmente em comparação com outros tipos de seguro, como o de automóveis. É *volátil*, pois envolve ameaças em constante mutação e desenvolvimento, característica compartilhada com a evolução tecnológica. E, principalmente, o risco cibernético é um risco *facilitado*: as pessoas se acostumaram a compartilhar mais dados pessoais por um desconto maior em alguma loja[41], a utilizar sistemas e dispositivos inseguros, a desabilitar atualizações automáticas (geralmente essenciais para contornar vulnerabilidades identificadas em determinado software), a utilizar aparelhos ou software obsoletos, a receber comunicações de fornecedores de produtos e serviços em formatos que facilitam tentativas de *phishing* e a se submeter a autenticações unilaterais, que não se aplicam às organizações que estão coletando os seus dados[42]. Quando governos se interessam mais em manter possibilidades de vigilância e espionagem do que em fomentar a segurança por *default*[43] e promovem políticas que focam mais em remédios do que em prevenções, favorece-se o risco.

Devido a essas particularidades, as consequências de um ataque cibernético são conhecidas somente depois que o estrago está feito. A evolução tecnológica dificulta análises

---

[40] SOMMERVILLE, Ian. **Engenharia de Software**. Tradução: Luiz Cláudio Queiroz. 10 ed. São Paulo: Pearson Education do Brasil, 2018, p. 383.

[41] Trata-se do que Daniel Solove chama de "paradoxo da privacidade". Ver mais em: SOLOVE, Daniel J. The Myth of the Privacy Paradox. **The George Washington Law Review**, v. 89, n. 1, p. 1–51, 2020.

[42] SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022, p. 180-182.

[43] Nesse sentido, pode-se mencionar as tentativas do FBI de obrigar empresas de tecnologia a instalar *backdoors* para permitir a quebra de criptografia de dispositivos. Ver mais em: SCHNEIER, Bruce. **Clique aqui para matar todo mundo**: segurança e sobrevivência em um mundo hiperconectado. Trad.: Eduardo Lima. Rio de Janeiro: Alta Books, 2020, p. 171.

de dados e o dimensionamento de riscos. Seguradoras também enfrentam dificuldades na formação de grupos equilibrados de segurados, pois todos os membros do grupo podem ser afetados por um incidente, ainda que estejam em regiões geográficas diferentes e atuem em segmentos de mercado distintos – particularidade que não ocorre sequer nas hipóteses de riscos ambientais catastróficos, em que seguradoras podem agrupar pessoas de diferentes regiões[44].

Por outro lado, pesquisas recentes constataram que o valor de mercado de empresas que anunciam vazamentos de dados tende a cair nos dias que se seguem ao anúncio, mas retoma a estabilidade no longo prazo[45]. Em 2015, Benjamin Dean chamou a atenção para o fato de que nem sempre prejuízos milionários são uma ferida profunda nas finanças de grandes corporações. No caso da Target, além de uma cobertura securitária parcial (de 36% sobre o valor total dos prejuízos[46]), deduções fiscais relacionadas aos gastos com o incidente de segurança fizeram com que a perda efetiva da empresa fosse de pouco mais de US$ 105 milhões, o equivalente a 0,1% das vendas em 2014. O caso da Sony, igualmente referido no início da introdução, resultou em um prejuízo correspondente a algo entre 0,9% e 2% do total de vendas projetadas para 2014, compensado em parte pela publicidade mundial gratuita para o filme *The Interview*, que custaria em torno de US$ 11 milhões[47]. Outro estudo publicado nos Estados Unidos identificou que mais de 25% dos americanos adultos já receberam notificações informando violações de dados, mas 89% deles continuaram utilizando os serviços das empresas que enviaram as notificações[48].

Ainda não há estudos abordando como organizações e consumidores brasileiros se comportam com relação a esses temas. Porém, tal como nos Estados Unidos, empresas brasileiras igualmente podem enquadrar, ainda que em parte, despesas incorridas com

---

[44] WOLFF, Josephine. **Cyberinsurance policy**: rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks. Cambridge: The MIT Press, 2022, p. 4.

[45] Trata-se de um prejuízo de curto prazo, pois o impacto negativo no preço das ações negociadas na bolsa, por exemplo, costuma ocorrer nos dias seguintes ao anúncio de um incidente de segurança; a longo prazo, o preço volta a se estabilizar. Nesse sentido: SCHNEIER, Bruce. Security Breaches Don't Affect Stock Price. **Schneier on Security**, 19 jan. 2018. Disponível em: https://www.schneier.com/blog/archives/2018/01/security_breach.html. Acesso em: 13 jan. 2023; ARCURI, Maria Cristina; BROGI, Marina; GANDOLFI, Gino. How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. **ITASEC**, Veneza, 2017. Disponível em: https://ceur-ws.org/Vol-1816/paper-18.pdf.

[46] FAURE, Michael; NIEUWESTEEG, Bernold. The Law and Economics of Cyber Risk Pooling. **New York University Journal of Law and Business.** New York, v. 14, n. 3, 2018, p. 934.

[47] DEAN, Benjamin. Why companies have little incentive to invest in cybersecurity. **The Conversation**, 04 mar. 2015. Disponível em: https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570. Acesso em: 16 jan. 2023.

[48] ABLON, Lillian *et. al.* Consumer attitudes toward data breach notifications and loss of personal information. **Rand Corporation**, n. 13, 2016, p. 26–27. Disponível em: https://www.rand.org/pubs/research_reports/RR1187.readonline.html; KOSSEFF, Jeff. Defining Cybersecurity Law. **Iowa Law Review**, v. 103, n. 985, mar. 2018, p. 1015.

vazamentos de dados como um custo operacional, para dedução no imposto de renda de pessoa jurídica[49].

Esses dados podem indicar uma combinação de fatores (coberturas securitárias, fidelidade de clientes, resposta do mercado e deduções tributárias) que pode permitir a rápida retomada da atividade empresarial após um ataque cibernético. Trata-se de uma notícia que, por um lado, é positiva, mas, por outro, pode fomentar o risco moral, isto é, a adoção de comportamentos indesejados pela parte que contrata um seguro. O risco moral abrange tanto o comportamento negligente, que facilita a ocorrência do sinistro diante da falta de cuidado, quanto o fraudulento, praticado para obter alguma vantagem indevida em razão da contratação da apólice[50].

A existência de fatores favoráveis à possível redução de prejuízos e a rápida recuperação após um ataque cibernético podem fazer com que empresas optem por não implementar medidas robustas de cibersegurança, o que favoreceria novos ataques[51]. Esse cenário representa um risco para terceiros: medidas robustas de cibersegurança protegem dados pessoais (informações que permitem identificar uma pessoa *natural*), serviços que podem integrar a infraestrutura crítica de um país e, claro, contribuem para o equilíbrio do grupo que contrata o seguro e o controle da taxa de sinistralidade.

Apesar de tantas particularidades, o seguro contra riscos cibernéticos não deixa de ser um contrato típico, já previsto e regulamentado no direito brasileiro. O artigo 757 do Código Civil dispõe que "pelo contrato de seguro, o segurador se obriga, mediante o pagamento do prêmio, a garantir interesse legítimo do segurado, relativo a pessoa ou a coisa, contra riscos predeterminados". A finalidade – e o elemento central – do contrato de seguro é transferir um risco predeterminado que paira sobre um interesse legítimo do segurado para a seguradora. Essa transferência se dá mediante o pagamento de um prêmio, pelo segurado, que terá direito à cobertura do seguro em caso de sinistro – isto é, à *garantia*[52].

---

[49] No documento disponibilizado pela Receita Federal para a declaração de imposto de renda de pessoa jurídica em 2022, consta que despesas com computadores são geralmente enquadradas como custo operacional. RECEITA FEDERAL. **Perguntas e respostas pessoa jurídica 2022**. Brasília, 31 dez. 2021, p. 215. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/ecf/PeRPJ2022v1.pdf.

[50] MIRAGEM, Bruno. PETERSEN, Luiza. **Direito dos Seguros**. Rio de Janeiro: Forense, 2022, p. 63.

[51] BAILEY, Liam M. D. Mitigating Moral Hazard in Cyber-Risk Insurance. **Journal of Law & Cyber Warfare**, v. 3, p. 1-42, 2014.

[52] PETERSEN, Luiza Moreira. **O risco no Contrato de Seguro**. São Paulo: Roncarati, 2018, p. 43.

No Brasil, a maioria das apólices oferecidas no ano de 2021 encontrava um limite de R$ 100 milhões, equivalente a aproximadamente US$ 20 milhões[53]. A princípio, esse limite seria suficiente para cobrir o custo médio de uma violação de dados no Brasil (US$ 1,38 milhão[54]) para empresas de médio porte. Porém, bastaria um ataque ransomware para atingir o limite da apólice (esse foi justamente o valor cobrado da Renner) e, a depender da quantidade de dados afetados e da estrutura dos sistemas utilizados por uma organização, as perdas podem se mostrar muito superiores ao limite do seguro, desafiando a própria utilidade da garantia e a função econômico-social esperada do contrato.

É justamente desse ponto que se extrai o problema de pesquisa da dissertação. Se riscos cibernéticos são tão voláteis e estão em constante mutação, acompanhando a evolução tecnológica, o que é necessário para se contratar um seguro com garantia suficiente?

Para responder a essa pergunta, diversos fatores ainda incipientes no direito brasileiro precisarão ser estudados. Essa particularidade permite adiantar, desde logo, que essa dissertação dificilmente fornecerá respostas assertivas sobre o assunto. Mais do que a análise de um imbróglio específico, este trabalho visa a oferecer proposições que possam contribuir para o desenvolvimento de apólices de seguro que atendam tanto interesses comerciais quanto de titulares de dados pessoais.

Surgem, nesse sentido, perguntas secundárias, que igualmente podem guiar o percurso até a conclusão do trabalho: (*i.*) qual o significado e a relevância dos conceitos de cibersegurança e segurança da informação? (*ii.*) quais são as principais ameaças cibernéticas que afetam organizações e titulares de dados pessoais? (*iii.*) que medidas podem ser adotadas

---

[53] FEDERAÇÃO NACIONAL DE SEGUROS GERAIS. Ataques hackers movimentam venda de seguros contra risco cibernético, 22 out. 2021. Disponível em: https://fenseg.org.br/noticias/ataques-hackers-movimentam-venda-de-seguros-contra-risco-cibernetico.html. Acesso em: 18 ago. 2022.

[54] Vale observar que os artigos 52, 53 e 54 da LGPD, que tratam das sanções administrativas, entraram em vigor apenas em 1º de agosto de 2021. A primeira penalidade imposta pela ANPD ocorreu em 05 de julho de 2023, em face da microempresa Telekall Infoservice. Conforme consta do Relatório de Instrução do Processo Administrativo Sancionador, a Telekall oferecia listagem de contatos de WhatsApp para disparo de mensagens e possuía um banco de dados de aproximadamente 130 milhões de pessoas, formado pela coleta de informações disponíveis na internet para posterior comercialização. A ANPD concluiu que a Telekall violou o artigo 7º da LGPD, ao tratar dados sem indicação de base legal autorizativa, e o artigo 41, por não ter nomeado Encarregado de Proteção de Dados. A ANPD decidiu pela imposição de advertência, para adoção de medidas corretivas consistentes na nomeação de Encarregado, e multa simples, arbitrada de acordo com os critérios estabelecidos na Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, em R$ 14.400,00 (BRASIL. **Autoridade Nacional de Proteção de Dados**. PAS nº 00261.000489/2022-62. Autuado: Telekall Infoservice. Brasília, 05 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em: 28 out. 2023). Nota-se que o valor referido no relatório da IBM ainda não reflete, no cômputo dos prejuízos decorrentes de uma violação de dados, as penalidades que poderão ser aplicadas pela ANPD. Muito embora o Apêndice II da Resolução nº 4/2023 estabeleça valores mínimos de penalidade relativamente baixos (de R$ 1.000,00 até R$ 4.000,00 para pessoa natural ou pessoa jurídica sem faturamento e de R$ 3.000,00 a R$ 12.000,00 para os demais infratores), há multas que podem atingir até R$ 50 milhões por infração, de modo que o custo de uma violação de dados no Brasil poderá ser modificado nos próximos anos.

para mitigar riscos e prejuízos relacionados à violação da cibersegurança? (*iv.*) que fatores devem ser considerados para a elaboração de garantias razoáveis e suficientes para que haja uma efetiva *transferência* do risco relacionado às falhas de cibersegurança que afetam interesses legítimos de segurados? (*v.*) o contrato de seguro contra riscos cibernéticos pode ser utilizado como uma ferramenta para fomentar a cibersegurança?

A pesquisa tem como base o método dedutivo e a revisão bibliográfica de trabalhos publicados no Brasil e no exterior. Não se trata propriamente de um trabalho de direito comparado, mas de um esforço de análise sobre como institutos desenvolvidos no direito interno de outros países podem contribuir para os debates e para o desenvolvimento do tema no Brasil.

O seguro contra riscos cibernéticos pode ser uma importante ferramenta de gestão de riscos e de incentivo à implementação de medidas preventivas de cibersegurança. Quanto mais medidas de prevenção forem adotadas, menores serão os riscos e maior será a chance de que a garantia seja suficiente para cobrir todos os prejuízos em caso de violação de dados. Do contrário – e aqui entra a relevância do risco moral e da antisseleção – incidentes catastróficos poderão resultar em coberturas insuficientes ou irrisórias. Vale lembrar que apenas a multa pela violação de dados da ANPD pode atingir R$ 50 milhões, isto é, metade do valor máximo das atuais apólices negociadas no Brasil.

O desenvolvimento dos capítulos terá por objetivo (*i.*) compreender os conceitos e a relação entre risco cibernético e cibersegurança; (*ii.*) analisar como o seguro contra riscos cibernéticos pode afetar ou contribuir para a prevenção de incidentes de segurança; (*iii.*) compreender que aspectos devem ser considerados para a contratação da apólice e para a delimitação da cobertura e dos riscos excluídos; e (*iv.*) analisar a intersecção entre risco cibernético, cibersegurança, mutualismo, risco moral e antisseleção no contrato de seguro.

Devido à amplitude do tema, foram estabelecidos três recortes.

Primeiro, a pesquisa considerará riscos relacionados à *cibersegurança*, e não apenas à *segurança da informação* prevista na LGPD. Isso porque riscos cibernéticos podem afetar direitos de propriedade intelectual e industrial, relações societárias e disponibilidade de serviços que não se limitam às discussões sobre dados pessoais. Ao reconhecer a amplitude do risco, contudo, não se pretende adentrar nos pormenores de cada uma dessas matérias correlatas – até porque, a responsabilização de administradores e diretores pela tomada de decisões não recomendadas ou contrárias à cibersegurança[55] poderia remeter a discussão às apólices de

[55] Por vezes, incidentes de segurança ocorrem pela decisão deliberada de administradores no sentido de não adotar medidas técnicas necessárias em razão de tratarem de um custo de curto prazo com benefícios verificáveis a longo

seguro D&O, por exemplo. A Parte I desta dissertação considera esse recorte e buscará delimitar os conceitos de cibersegurança e risco cibernético e abordar os principais fatores que podem contribuir para a sistematização desses riscos.

O segundo recorte de pesquisa tem relação com o direito dos seguros. Muitos são os desafios teóricos e práticos com relação ao seguro contra riscos cibernéticos. A dissertação abordará apenas as questões atinentes ao contrato de seguro empresarial, regrado pelo Código Civil, excluindo-se as relações de consumo. Dentro dessa temática, propõe-se um terceiro recorte, com foco na análise do *conteúdo* da formação da garantia – sem adentrar, ao menos por ora, na análise de *forma* e na regulamentação específica dos contratos de seguro. Nesse sentido, a Parte II da dissertação passará por dois pontos: a origem, evolução e premissas centrais do seguro contra riscos cibernéticos, com o apoio de estudos estrangeiros, em especial dos Estados Unidos, e os desafios para a formação da garantia, considerando os desafios para o princípio do mutualismo, o risco moral e a redação das cláusulas de delimitação e exclusão de cobertura.

Ao final, serão apresentadas as conclusões.

---

prazo. Bruce Schneier sugere que essa omissão deveria ser passível de responsabilização, já que pode comprometer não apenas a empresa, mas todos os seus clientes e fornecedores. Ver mais em: SCHNEIER, Bruce. **Clique aqui para matar todo mundo**: segurança e sobrevivência em um mundo hiperconectado. Trad.: Eduardo Lima. Rio de Janeiro: Alta Books, 2020, p. 109-110.

REFERÊNCIAS

ABLON, Lillian *et. al.* Consumer attitudes toward data breach notifications and loss of personal information. **Rand Corporation**, n. 13, 2016, p. 26–27. Disponível em: https://www.rand.org/pubs/research_reports/RR1187.readonline.html.

ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. The economics of privacy. **Journal of Economic Literature**, v. 54, n. 2, p. 442–492, 2016.

ALVARENGA, Darlan. Quais são as maiores empresas do Brasil em receita, lucro e valor de mercado? **G1**, 01 de abr. 2022. Disponível em: https://g1.globo.com/economia/noticia/2022/04/01/quais-sao-as-maiores-empresas-do-brasil-em-receita-lucro-e-valor-de-mercado.ghtml. Acesso em: 22 jan. 2023.

ALVIM, Pedro. **O Contrato de Seguro**. 3 ed. Rio de Janeiro: Forense, 2001.

ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil — e suas consequências. **Jota**, 28 jan. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em: 12 jan. 2023.

ARCURI, Maria Cristina; BROGI, Marina; GANDOLFI, Gino. How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns. **ITASEC**, Veneza, 2017. Disponível em: https://ceur-ws.org/Vol-1816/paper-18.pdf.

ARENDT, Hannah. **Origens do totalitarismo**. Tradução: Roberto Raposo. São Paulo: Companhia das Letras, 2012.

ARENDT, Hannah. **Responsabilidade e julgamento**. São Paulo: Companhia das Letras, 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro, 05 out. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. 3 ed. Rio de Janeiro, 24 out. 2019.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **Glossário da sociedade da informação**. 4 ed. Lisboa, jun. 2019. Disponível em: https://apdsi.pt/wp-content/uploads/2018/03/GLOSSA%CC%81RIO-DA-SOC-INFORMACAO_v2019-APDSI.pdf. Acesso em: 30 abr. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte, Brasília, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf.

BAILEY, Liam M. D. Mitigating Moral Hazard in Cyber-Risk Insurance. **Journal of Law & Cyber Warfare**, v. 3, p. 1-42, 2014.

BAJAK, Frank. Insurer AXA to Stop Paying for Ransomware Crime Payments in France, **Insurance Journal,** 09 mai. 2021. Disponível em: https://www.insurancejournal.com/news/international/2021/05/09/613255.htm. Acesso em: 05 jun. 2023.

BAKER, Liana B.; FINKLE, Jim. Sony PlayStation suffers massive data breach. **Reuters**, 26 abr. 2011. Disponível em: https://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110427. Acesso em: 12 jan. 2023.

BENTZ, Thomas H. Jr. Is Your Cyber Liability Insurance Any Good: a guide for banks to evaluate their cyber liability insurance coverage. **North Carolina Banking Institute**, 21, 2017, p. 39-54.

BONNER, Lance. Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. **Washington University Journal of Law & Policy**, v. 40, p. 257-278, 2012.

BREIDENBACH, Susan. The Policy of Protection. **Computerworld**, 03 jan. 2001. Disponível em: https://www.computerworld.com/article/2782654/the-policy-of-protection.html. Acesso em: 17 mai. 2023.

CACHAPUZ, Maria Cláudia Mércio. Privacidade, proteção de dados e autodeterminação informativa. **Revista Jurídica da Presidência**, Brasília v. 15 n. 107, out. 2013/jan. 2014, p. 823-848.

CANTALI, Rodrigo Ustárroz. O STJ e o dano moral coletivo: entre conduta e interesse tutelado, **Migalhas**, 11 fev. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/340156/o-stj-e-o-dano-moral-coletivo-entre-conduta-e-interesse-tutelado. Acesso em: 06 fev. 2023.

CAPPELLETTI, Mauro; GARTH, Bryan. **Acesso à Justiça**. Trad. Ellen Gracie Northfleet. Porto Alegre: Sergio Antonio Fabris Editor, 1988.

CARVALHO, Angelo Prata de; XAVIER, Vitor Boaventura. Seguro contra riscos cibernéticos: elementos dogmáticos para a construção de mecanismos securitários em face dos riscos oriundos das tecnologias da informação. In: TZIRULNIK, Ernesto (org.). **Direito do seguro contemporâneo:** edição comemorativa dos 20 anos do IBDS. Vol. 1. São Paulo: Contracorrente, 2021, p. 389–417.

CASEMIRO, Luciana; REIS, Luana. Cresce a oferta de proteção para riscos digitais: seguros avançam e passam a cobrir violação de dados de pessoas físicas e pequenas empresas. **O Globo**, 14 mai. 2023. Disponível em: https://infoglobo.pressreader.com/o-globo/20230514. Acesso em: 15 mai. 2023.

CEBULA, James J; POPECK, Mary E.; YOUNG, Lisa R. A Taxonomy of Operational Cyber Security Risks Versio 2. Pittsburgh, **Software Engineering Institute**, Carnegie Melon University. Disponível em: https://doi.org/10.1184/R1/6571784.v1.

COMPARATO, Fábio Konder. **O Seguro de Crédito**. São Paulo: RT, 1968.

COMPARATO, Fábio Konder. Obrigações de meios, de resultado e de garantia. **Doutrinas Essenciais de Direito Empresarial**, vol. 4. São Paulo, dez. 2010, p. 63-78.

CONFEDERAÇÃO NACIONAL DAS SEGURADORAS. Glossário do Seguro, 2021, p. 77. Disponível em: https://cnseg.org.br/data/files/3A/45/72/CA/A253D710B2DC74C73A8AA8A8/NOVO_GLOSS%C3%81RIO%20(ONLINE).pdf. Acesso em: 13 jan. 2023.

COUTO E SILVA, Clóvis V. **A obrigação como processo**. Rio de Janeiro: Editora FGV, 2006.

COVEWARE, Big Game Hunting is back despite decreasing Ransom Payment Amounts. Westport, 28 abr. 2023. Disponível em: https://www.coveware.com/blog/2023/4/28/big-game-hunting-is-back-despite-decreasing-ransom-payment-amounts. Acesso em: 05 jun. 2023.

CREEMERS, Rogier; TRIOLO, Paul; WEBSTER, Graham. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). **New America,** 29 jun. 2018. Disponível em: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Acesso em: 01 mai. 2023.

DE GROOT, Juliana. The History of Data Breaches. **Data Insider**, 12 nov. 2018. Disponível em: https://digitalguardian.com/blog/history-data-breaches. Acesso em 05 jan. 2023.

DEAN, Benjamin. Why companies have little incentive to invest in cybersecurity. **The Conversation**, 04 mar. 2015. Disponível em: https://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570. Acesso em: 16 jan. 2023.

DLA PIPER. Data Protection Laws of the World: China, 3 jan. 2023. Disponível em: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=CN&c2=. Acesso em: 20 mar. 2023.

DLA PIPER. Data Protection Laws of the World: Turkey. 12 jan. 2023. Disponível em: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=TR. Acesso em: 20 mar. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Revista dos Tribunais, 2021. *E-book*.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo *et al.* (coord.). **Tratado de proteção e dados pessoais**. Rio de Janeiro: Forense, 2021, p. 3-20.

DUDLEY, Renee. The extortion economy: how insurance companies are fueling a rise in ransomware attacks. **ProPublica**, 27 ago. 2019. Disponível em: https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks. Acesso em: 30 mai. 2023.

ELKIND, Peter. Sony Pictures: Inside the Hack of the Century. **Fortune**, 25 jun. 2015. Disponível em: https://fortune.com/2015/06/25/inside-sony-pictures-hack/. Acesso em: 12 jan. 2023.

ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. Heraklion, dez. 2013. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity. Acesso em: 29 out. 2023.

ENISA. Threat Landscape 2023: July 2022 to June 2022. Out. 2023, p. 140-160. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Acesso em: 30 out. 2023.

FAURE, Michael; NIEUWESTEEG, Bernold. The Law and Economics of Cyber Risk Pooling. **New York University Journal of Law and Business.** New York, v. 14, n. 3, 2018, p. 934.

FEDERAÇÃO NACIONAL DE SEGUROS GERAIS. Ataques hackers movimentam venda de seguros contra risco cibernético, 22 out. 2021. Disponível em: https://fenseg.org.br/noticias/ataques-hackers-movimentam-venda-de-seguros-contra-risco-cibernetico.html. Acesso em: 18 ago. 2022.

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993.

FINKLE, Jim; SOMERVILLE, Heather. Uber's messy data breach collides with launch of SoftBank deal, **Reuters**, 22 nov. 2017. Disponível em: https://www.reuters.com/article/us-uber-cyberattack-idUSKBN1DM2F9. Acesso em: 15 jan. 2023.

FORREST, Conner. Dyn DDoS attack: 5 takeaways on what we know and why it matters, **TechRepublic**, 24 out. 2016. Disponível em: https://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/. Acesso em: 19 jan. 2023.

FREEDMAN, Linn Foster. 2016 was the Year of the Data Breach. **Data Privacy and Cybersecurity Insider**, 29 dez. 2016. Disponível em: https://www.dataprivacyandsecurityinsider.com/2016/12/2016-was-the-year-of-the-data-breach/?ref=hackernoon.com. Acesso em: 12 jan. 2023.

FUSTER, Gloria González. **The Emergence of Personal Data Protection as a Fundamental Right of the EU**. Brussels: Springer, 2014.

GRAU, Eros Roberto. Nota sobre a distinção entre obrigação, dever e ônus. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 77, p. 177–183, 1982.

GREENBERG, Andy. The Untold Story of NotPetya, the Most DevastatingCyberattack in History. **Wired**, 22 ago. 2018. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Acesso em: 26 mai. 2023.

GRIFFIN, Riley; CHIGLINSKY, Katherine; VOREACOS, David. Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question. **Insurance Journal**, 3 dez. 2019. Disponível em: https://www.insurancejournal.com/news/national/2019/12/03/550039.htm. Acesso em: 27 mai. 2023.

HA, Young. N.Y. Court: Zurich Not Obligated to Defend Sony Units in Data Breach Litigation. **Insurance Journal**, 17 mar. 2014. Disponível em:

https://www.insurancejournal.com/news/east/2014/03/17/323551.htm. Acesso em: 20 mai. 2023.

HALTON, Clay; KELLY, Robert C.; MUNICHIELLO, Katrina. The Truth About Y2K: What Did and Didn't Happen in the Year 2000, **Investopedia**, 13 set. 2021. Disponível em: https://www.investopedia.com/terms/y/y2k.asp. Acesso em: 17 mai. 2023.

HARDCASTLE, Jessica Lyons. Ritz cracker giant settles bust-up with insurer over $100m+ NotPetya cleanup. **The Register**, 2 nov. 2022. Disponível em: https://www.theregister.com/2022/11/02/mondelez_zurich_notpetya_settlement/. Acesso em: 26 mai. 2023.

HILL, Kashmir. How Target figured out a teen girl was pregnant before her father did. **Forbes**, 16 fev. 2012. Disponível em: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=5f55a9026668. Acesso em: 12 set. 2021.

HOFFMANN-RIEM, Wolfgang. A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação. Tradução: RIBEIRO, Pedro Henrique. São Paulo: **Revista de Direito Civil Contemporâneo**, v. 23, abr./jun., 2020.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: desafios para o direito. FUHRMANN, Italo (trad.). 1 ed. Rio de Janeiro: Forense, 2021.

IBM Security. Relatório de custo da violação de dados de 2022. São Paulo, jul. 2022. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 09 jan. 2023.

INSURANCE INFORMATION INSTITUTE. Spotlight on: Catastrophes – Insurance issues. Disponível em: https://www.iii.org/article/spotlight-on-catastrophes-insurance-issues. Acesso em: 29 abr. 2022.

JOHANSMEYER, Tom. The Cyber Insurance Market Needs More Money. **Harvard Business Review**, 10 mar. 2022. Disponível em: https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money. Acesso em: 16 jan. 2023.

KASSNER, Michael. Anatomy of the Target data breach: Missed opportunities and lessons learned. **ZDNet**, 02.02.2015. Disponível em: https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/?ref=hackernoon.com. Acesso em: 12 jan. 2023.

KASTRENAKES, Jacob. SEC issues $35 million fine over Yahoo failing to disclose data breach. **The Verge**, 24 abr. 2018. Disponível em: https://www.theverge.com/2018/4/24/17275994/yahoo-sec-fine-2014-data-breach-35-million. Acesso em: 12 jan. 2023.

KHOSROWSHAHI, Dara. 2016 Data Security Incident, **Uber**, 21 nov. 2017. Disponível em: https://www.uber.com/newsroom/2016-data-incident/. Acesso em: 15 jan. 2023.

KOSSEFF, Jeff. Defining Cybersecurity Law. **Iowa Law Review**, v. 103, n. 985, p. 985-1031. Mar. 2018. Disponível em: https://ilr.law.uiowa.edu/assets/Uploads/ILR-103-3-Kosseff.pdf.

LAFER, Celso. **Hannah Arendt**: pensamento, persuasão e poder. 3 ed. Rio de Janeiro/São Paulo: Paz e Terra, 2018.

LAI, Charlie; MEDVINSKY, Gennady; NEUMAN, B. Clifford. Endorsements, Licensing, and Insurance for Distributed System Services, **2nd ACM Conference on Computer and Communications Security (CCS)**, 1994. Disponível em: https://dl.acm.org/doi/pdf/10.1145/191177.191215.

LARSON, Selena. Every single Yahoo account was hacked - 3 billion in all. **CNN Money**, 04 out. 2017. Disponível em: https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html?ref=hackernoon.com. Acesso em: 12 jan. 2023.

LAZARUS, David. The guy who stole my identity 15 years ago just resurfaced in my life. **Los Angeles Times**, 08 ago. 2017. Disponível em: https://www.latimes.com/business/lazarus/la-fi-lazarus-identity-theft-20170808-story.html. Acesso em: 10 jan. 2023.

LEEUW, Karl de; BERGSTRA, Jan. **The History of Information Security:** a comprehensive handbook. Amsterdam: Elsevier, 2007.

LESSIG, Lawrence. **Code**. New York: Basic Books, 2006.

LINEBAUGH, Kate; KNUTSON, Ryan. Ransomware, a Pipeline and a Gas Shortage. **The Journal**, 13 mai. 2021. Disponível em: https://www.wsj.com/podcasts/the-journal/ransomware-a-pipeline-and-a-gas-shortage/ba1e55ad-29b3-468d-98ad-92b9f1a58003?mod=WSJ_JournalPodCaption. Acesso em: 05 fev. 2023.

LLOYDS MARKET ASSOCIATION. Cyber War and Cyber Operation Exclusion Clauses. 25 nov. 2021. Disponível em: https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx. Acesso em: 20 mai. 2023.

LLOYDS. Global ransomware attack could cost businesses almost $200bn, new study finds. 29 jan. 2019. Disponível em: https://www.lloyds.com/about-lloyds/media-centre/press-releases/global-ransomware-attack. Acesso em: 27 mai. 2023.

LLOYDS. Market bulletin: State backed cyber-attack exclusions. 16 ago. 2022. Disponível em: https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf. Acesso em: 20 mai. 2023.

LOPES, André. Após ataque hacker, Renner nega que pagou US$ 20 milhões aos criminosos. **Exame**, 20 ago. 2021. Disponível em: https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/. Acesso em: 13 jan. 2023.

MACHT, Joshua. Safe Haase. **Inc**., 15 set. 1997. Disponível em: https://www.inc.com/magazine/19970915/1427.html. Acesso em: 17 mai. 2023.

MAJUCA, Ruperto P.; YURCIK, William; KESAN, Jay P. The Evolution of Cyberinsurance. arXiv: **Criptography and Security**, jan. 2006. Disponível em: https://doi.org/10.48550/arXiv.cs/0601020.

MARTINS, Maria Inês de Oliveira. Defendendo o caminho mais trilhado, na demarcação entre o regime da avaliação inicial do risco e o do seu agravamento subsequente. In: TZIRULNIK, Ernesto (org.). **Direito do seguro contemporâneo:** edição comemorativa dos 20 anos do IBDS. Vol. 1. São Paulo: Contracorrente, 2021, p. 517-546.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para a sua aplicação. São Paulo: Saraiva, 2018.

MARTINS-COSTA, Judith. **Comentários ao novo Código Civil**: do inadimplemento das obrigações, vol. V. Tomo II. 2 ed. Rio de Janeiro: Forense, 2009.

MARTINS-COSTA, Judith. Os avatares do abuso do direito e o rumo indicado pela boa-fé. Canela, set. 2006. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4673590/mod_resource/content/0/Judith%20Martins-Costa%20-%20Os%20avatares%20do%20Abuso%20do%20direito%20e%20o%20rumo%20indicado%20pela%20Boa-F%C3%A9.pdf. Acesso em: 29 out. 2023.

MARTINS-COSTA, Judith; XAVIER, Rafael Branco. A cláusula de *ensuing loss* nos seguros *all risks*. In: TZIRULNIK, Ernesto (org.). **Direito do seguro contemporâneo:** edição comemorativa dos 20 anos do IBDS. Vol. 2. São Paulo: Contracorrente, 2021, p. 13-44.

MARTIN-VEGUE, Tony. Will the real "Year of the Data Breach" please stand up? **Hackernoon**, 04 jan. 2018. Disponível em: https://hackernoon.com/will-the-real-year-of-the-data-breach-please-stand-up-744ab6f63615. Acesso em 05 jan. 2023.

MATWYSHYN, Andrea. Hacking speech: informational speech and the first amendment. **Northwestern University School of Law**, v. 107, n. 2, p. 795-846, 2013. Disponível em: https://northwesternlawreview.org/issues/hacking-speech-informational-speech-and-the-first-amendment/.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (org.). **Technology and Privacy**: The New Landscape. Cambridge: The MIT Press, 1997. p. 219–241.

MCMILLAN, Robert; LINEBAUGH, Kate. Why a Ransomware Group Is Pretending to Be a Real Company, **The Journal**, 28 out. 2021. Disponível em: https://www.wsj.com/podcasts/the-journal/why-a-ransomware-group-is-pretending-to-be-a-real-company/da6d1d8e-8e36-40b6-9773-a5cf83ae6823?mod=WSJ_JournalPodCaption. Acesso em: 05 fev. 2023.

MELLO, Marcos Bernardes de. **Teoria do Fato Jurídico**: plano da validade. 16 ed. São Paulo: SaraivaJur, 2022.

MENDES, Laura Schertel. O fortalecimento da agência da União Europeia para a Segurança das Redes e da Informação: comentário ao Regulamento (EU) n. 526/2013. **Revista de Direito do Consumidor**, São Paulo, v. 90, p. 295 – 332, nov./dez. 2013.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469–483, 2018.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar F.; SARLET, Ingo. W.; COELHO, Alexandre Z. P. (coord.). **Direito, Inovação e Tecnologia**. São Paulo: Saraiva, 2015, p. 205-230.

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acesso em: 21 jan. 2023.

MENKE, Fabiano; GOULART, Guilherme Damásio. Segurança da informação e vazamento de dados. *In*: DONEDA, Danilo *et al*. (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 339-359.

MIRAGEM, Bruno. O Direito dos Seguros no Sistema Jurídico Brasileiro: uma introdução. In: MIRAGEM, Bruno; CARLINI, Angélica (org.). **Direito dos Seguros**: fundamentos de direito civil, direito empresarial e direito do consumidor. São Paulo: Revista dos Tribunais, 2015. *E-book*.

MIRAGEM, Bruno. PETERSEN, Luiza. **Direito dos Seguros**. Rio de Janeiro: Forense, 2022.

MUELLER, Robert S. Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies. **The Federal Bureau of Investigation**. Mar. 2012. Disponível em: https://archives.fbi.gov/archives/news/speeches//combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies. Acesso em: 28 ago. 2022.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. São Paulo, **Revista do Advogado**, ano XXXIX, n. 144, nov. 2019, p. 47-53.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS. **Report on Cyberinsurance Market**. Kansas, 18 out. 2022. Disponível em: https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf. Acesso em: 20 ago. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Computer Security Resource Center**: Glossary. Disponível em: https://csrc.nist.gov/glossary. Acesso em: 04 jan. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Cybersecurity Framework (CSF) 2.0. Disponível em: https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters. Acesso em: 30 out. 2023.

NEWMAN, Lily Hay. A New Pacemaker Hack Puts Malware Directly on the Device. **Wired**, 9 ago. 2018. Disponível em: https://www.wired.com/story/pacemaker-hack-malware-black-hat/. Acesso em: 20 ago. 2023.

NIEVES, Angela M. Cyber Insurance today: saving it before it needs saving. **Catholic University Journal of Law and Technology**, vol. 29, n. 1, p. 111-144, 2020.

NURSE, Jason R.C *et al.* The data that drives cyber insurance: a study into the underwriting and claims processes. **2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)**. Dublin, 2020. DOI: https://doi.org/10.1109/CyberSA49311.2020.9139703

OCDE. Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020. Disponível em: www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf.

ORLAND, Kyle. Sony to pay up to $17.75 million in 2011 PSN hacking settlement. **Arstechnica**, 24 jul. 2014. Disponível em: https://arstechnica.com/gaming/2014/07/sony-to-pay-up-to-17-75-million-in-2011-psn-hacking-settlement/. Acesso em: 21 mai. 2023.

PALHARES, Felipe. *Cookie*s: contornos atuais. In: PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2020. *E-book.*

PAPADOPOULOS, Panagiotis; KOURTELLIS, Nicolas; MARKATOS, Evangelos P. *Cookie* synchronization: Everything you always wanted to know but were afraid to ask. **WWW '19: The World Wide Web Conference**, p. 1432–1442, 2019.

PETERS, Gareth W.; SHEVCHENKO, Pavel V.; COHEN, Ruben D. Understanding Cyber-Risk and Cyber-Insurance. **Macquarie University Faculty of Business & Economics Research Paper**, jan. 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3200166.

PETERSEN, Luiza Moreira. **O risco no Contrato de Seguro**. São Paulo: Roncarati, 2018.

PETERSON, Andrea. Data exposed in breaches can follow people forever. The protections offered in their wake don't. **The Washington Post**. Jun. 2015. Disponível em: https://www.washingtonpost.com/news/the-switch/wp/2015/06/15/data-exposed-in-breaches-can-follow-people-forever-the-protections-offered-in-their-wake-dont/. Acesso em 19 nov. 2022.

PIRES, Catarina Monteiro. Limites dos esforços e dispêndios exigíveis ao devedor para cumprir. **Revista da Ordem dos Advogados**, Lisboa, p. 105–136, 2016. Disponível em: http://www.catarinamonteiropires.com/Archive/Docs/f755007429055.pdf.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado**: direito das obrigações. Tomo XLV. Atualização: Bruno Miragem. São Paulo: Revista dos Tribunais, 2012.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado**: Parte Especial: validade, nulidade, anulabilidade. Tomo IV. Atualizadores: Marcos Bernardes de Mello e Marcos Ehrdardt Jr. São Paulo: Revista dos Tribunais, 2013.

PUENTE, Beatriz. Seguros de riscos cibernéticos têm crescimento de 75% nas contratações. **CNN Brasil**, 29 nov. 2022. Disponível em: https://www.cnnbrasil.com.br/nacional/seguros-de-riscos-ciberneticos-tem-crescimento-de-75-nas-contratacoes/. Acesso em: 13 jan. 2023.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, n. 1, v. 1, p. 64-90, 2020.

RAWLINGS, Philip. Cyber Risk: insuring the digital age. **British Insurance Law Association Journal**, v. 128, 2015. Queen Mary School of Law Legal Studies Research Paper n. 189/2015, Disponível em: https://ssrn.com/abstract=2551421.

REED, Toni Scott. Cybercrime and technology losses: claims and potential insurance coverage for modern cyber risks. **Tort Trial & Insurance Practice Law Journal**, v. 54, n. 1, p. 153-210, 2019.

REGO, Margarida Lima; SILVA, Rute Carvalho da. Os seguros de riscos catastróficos. In: GOMES, Carla Amado (coord.). **Direito(s) das catástrofes naturais**. Lisboa: Almedina, 2012, p. 269-322. Disponível em: http://hdl.handle.net/10362/15125.

RICKEN, Keith. The Missing Piece: Buyer Interest. **Risk & Insurance**, 01 dez. 2001. Disponível em: https://www.thefreelibrary.com/The+Missing+Piece%3A+Buyer+Interest%3B+Despite+some+high-profile+hacker...-a080897971. Acesso em: 18 mai. 2023.

RODRIGUES JUNIOR, Otávio Luiz. Do príncipe Bismarck à princesa Carolina de Mônaco: vida privada de pessoas célebres e as liberdades comunicativas no Direito Civil. In: CASSETTARI, Christiano (coord.). **10 anos de vigência do Código Civil brasileiro de 2002**. São Paulo: Saraiva, 2013, p. 111-125.

ROMANOSKY, Sasha, et al. Content analysis of cyber insurance policies: how do carriers price cyber risk? **Journal of Cybersecurity**, 2019, v. 5, n. 1, p. 1-19. Disponível em: https://doi.org/10.1093/cybsec/tyz002.

SABBAT, Arthur Pereira. Defesa Cibernética e Segurança Cibernética: Diferenças e Semelhanças. **LinkedIn**, 17 dez. 2018. Disponível em: https://www.linkedin.com/pulse/defesa-cibern%C3%A9tica-e-seguran%C3%A7a-diferen%C3%A7as-semelhan%C3%A7as-sabbat. Acesso em: 19 jan. 2023.

SALOMÃO FILHO, Calixto. Regulação econômica e novo Código Civil: o contrato de seguro. **Anais do III Fórum de Direito do Seguro José Sollero Filho**. São Paulo, IBDS, 2003, p. 271.

SANTOS, Gilmara. Busca por seguro cibernético cresce no país, mas análise das apólices fica mais burocrática. **InfoMoney**, 06 mar. 2023. Disponível em: https://www.infomoney.com.br/minhas-financas/busca-por-seguro-cibernetico-cresce-no-pais-mas-analise-das-apolices-fica-mais-burocratica/. Acesso em: 25 mai. 2023.

SARAMAGO, José. **O homem duplicado**. 2 ed. São Paulo: Companhia das Letras, 2017.

SCALET, Sarah D. ChoicePoint Data Breach: The Plot Thickens. **CSO**, 01 mai. 2005. Disponível em: https://www.csoonline.com/article/2118146/choicepoint-data-breach--the-plot-thickens.html. Acesso em: 13 jan. 2023.

SCHEUERMANN, James E. Cyber risks, systemic risks and cyber insurance. **Penn State Law Review**, v. 122, n. 3, 2018, p. 614 – 644.

SCHNEIER, Bruce. **Clique aqui para matar todo mundo**: segurança e sobrevivência em um mundo hiperconectado. Trad.: Eduardo Lima. Rio de Janeiro: Alta Books, 2020.

SCHNEIER, Bruce. Security Breaches Don't Affect Stock Price. **Schneier on Security**, 19 jan. 2018. Disponível em: https://www.schneier.com/blog/archives/2018/01/security_breach.html. Acesso em: 13 jan. 2023.

SCHREIER, Jason. Sony Estimates $ 171 Million Loss From PSN Hack. **Wired**, 23 mai. 2011. Disponível em: https://www.wired.com/2011/05/sony-psn-hack-losses/. Acesso em: 12 jan. 2023).

SCHWAB, Klaus. **La cuarta revolución industrial**. Barcelona: Debate, 2017.

SIMITIS, Spiros. Revisiting Sensitive Data. **Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)**, Estrasburgo, nov. 1999, p. 5. Disponível em: https://rm.coe.int/09000016806845af.

SOLOVE, Daniel J. Data is what data does: regulating use, harm, and risk instead of sensitive data. **Northwestern University Law Review**, v. 118, jan. 2023, no prelo. Disponível em: https://ssrn.com/abstract=4322198.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. **The George Washington Law Review**, v. 89, n. 1, p. 1–51, 2020. Disponível em: https://doi.org/10.2139/ssrn.3536265.

SOLOVE, Daniel J.; CITRON, Danielle Keats. Risk and anxiety: a theory of data-breach harms. **Texas Law Review**, v. 96, n. 4, p. 737-786, 2018. Disponível em: https://texaslawreview.org/risk-and-anxiety/.

SOLOVE, Daniel J; HARTZOG, Woodrow. **Breached!** Why data security fails and how to improve it. New York: Oxford University Press, 2022.

SOMMERVILLE, Ian. **Engenharia de Software**. Tradução: Luiz Cláudio Queiroz. 10 ed. São Paulo: Pearson Education do Brasil, 2018.

SPIECKER GEN DÖHMANN, Indra. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. In: DONEDA, Danilo *et al.* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 97–113.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. Painel de Inteligência do Mercado de Seguros. Disponível em: https://www2.susep.gov.br/safe/menuestatistica/pims.html. Acesso em: 07 mai. 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Comunicado da Presidência do STJ**, 9 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 13 jan. 2023.

TALESH, Shauhin A. Data Breach, Privacy, and Cyber Insurance: how insurance companies act as 'Compliance Managers' for businesses. **Law & Social Inquiry**, vol. 43, n. 2, 2018. Disponível em: https://ssrn.com/abstract=2974233.

TARUFFO, Michele. La tutela collettiva nell'ordinamento italiano: lineamenti generali. *In*: GRINOVER, Ada Pellegrini; BENJAMIN, Antonio Herman; WAMBIER, Teresa Arruda Alvim; VIGORITI, Vincenzo (org.). **Processo Coletivo**. São Paulo: Revista dos Tribunais, 2014. *E-book*.

THAW, David. The Efficacy of Cybersecurity Regulation. **Georgia State University Law Review**, v. 3, n. 2, p. 287-374, jun. 2014. Disponível em: https://readingroom.law.gsu.edu/gsulr/vol30/iss2/1.

TOWNSEND, Kevin. Lloyd's of London Introduces New War Exclusion Insurance Clauses. **Security Week**, 22 ago. 2022. Disponível em: https://www.securityweek.com/lloyds-london-introduces-new-war-exclusion-insurance-clauses/. Acesso em: 20 mai. 2023.

TOWNSEND, Kevin. Zurich Rejects Mondelez' $100 Million NotPetya Insurance Claim Citing 'Act of War'. **SecurityWeek**, 14 jan. 2019. Disponível em: https://www.securityweek.com/zurich-rejects-mondelez-100-million-notpetya-insurance-claim-citing-act-war/. Acesso em: 26 mai. 2023.

TZIRULNIK, Ernesto. **Seguro de Riscos de Engenharia**: instrumento do desenvolvimento. 2014. 189 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

TZIRULNIK, Ernesto; CAVALCANTI, Flávio de Queiroz; PIMENTEL, Ayrton. **O contrato de seguro**: de acordo com o novo Código Civil brasileiro. 2 ed. São Paulo: Revista dos Tribunais, 2003.

VAUGHAN, Emmet J.; VAUGHAN, Therese M. **Fundamentals of risk and insurance**. 11 ed. Hoboken: John Wiley & Sons, 2014.

VÉLIZ, Carissa. **Privacidade é poder:** porque e como você deveria retomar o controle de seus dados; tradução Samuel Oliveira; Ricardo Campos (prefácio). 1 ed. São Paulo: Contracorrente, 2021.

VOLZ, Dustin; YOUNG, Sarah. White House blames Russia for 'reckless' NotPetya cyber attack. **Reuters**, Washington/London, 15 fev. 2015. Disponível em: https://www.reuters.com/article/us-britain-russia-cyber-usa-idUSKCN1FZ2UJ. Acesso em: 26 mai. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, n. 5, p. 193-220, dec. 1890.

WELLS, Andrea. What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now, **Insurance Journal**, 01 mar. 2018. Disponível em: https://www.insurancejournal.com/news/national/2018/03/01/481886.htm. Acesso em: 16 mai. 2023.

WOLFF, Josephine. **Cyberinsurance policy**: rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks. Cambridge: The MIT Press, 2022.

WORLD ECONOMIC FORUM. The Global Risks Report 2023. 18ª ed, Geneva, 2023, p. 8. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

ZETTER, Kim. Sony Got Hacked Hard: What We Know and Don't Know So Far. **Wired**, 3 dez. 2014. Disponível em: https://www.wired.com/2014/12/sony-hack-what-we-know/. Acesso em: 12 jan. 2023.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

Processos judiciais e administrativos consultados:

BRASIL. **Autoridade Nacional de Proteção de Dados**. PAS nº 00261.000489/2022-62. Autuado: Telekall Infoservice. Brasília, 05 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em: 28 out. 2023.

BRASIL. **Superior Tribunal de Justiça**. Agravo em Recurso Especial nº 2.130.619/SP. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Relator: Ministro Francisco Falcão, 07 mar. 2023.

BRASIL. **Superior Tribunal de Justiça**. Inteiro teor das súmulas, 16 nov. 2022, p. 1065. Disponível em: https://www.stj.jus.br/docs_internet/jurisprudencia/tematica/download/SU/Sumulas/SumulasSTJ.pdf.

BRASIL. **Superior Tribunal de Justiça**. Informativo de Jurisprudência nº 791. Brasília, 18 out. 2023. Disponível em: https://www.stj.jus.br/publicacaoinstitucional/index.php/Informjuris20/article/view/12965/13069. Acesso em: 29 out. 2023.

BRASIL. **Superior Tribunal de Justiça**. Recurso Especial nº 2077278/SP. Recorrente: Daniela Ferreira Ramos. Recorrido: BV Financeira AS Crédito Financiamento e Investimento. Relatora: Ministra Nancy Andrighi, 03 out. 2023.

BRASIL. **Tribunal de Justiça de São Paulo**. Apelação Cível nº 1003671-31.2021.8.26.0405. Apelante: Marcelo Monteiro. Apelado: Eletropaulo Metropolitana Eletricidade De São Paulo S/A. Relator: Desembargador Plinio Novaes de Andrade Júnior, 29 nov. 2022.

BRASIL. **Tribunal de Justiça de São Paulo**. Apelação Cível nº 1006041-80.2021.8.26.0405. Apelante: Cheila Gomes de Siqueira Xereguin. Apelada: Enel Brasil S/A. Relatora: Desembargadora Silvia Rocha, 2 fev. 2022.

BRASIL. **Tribunal de Justiça de São Paulo**. Apelação Cível nº 1007827-41.2021.8.26.0606. Recorrentes/Recorridos: Banco do Brasil S/A e Davi Kawashima. Relator: Desembargador Vicentini Barroso, 05 set. 2022.

BRASIL. **Tribunal de Justiça de São Paulo**. Apelação Cível nº 1010354-98.2016.8.26.0554. Apelante: Companhia de seguros Aliança. Apelado: José Ramos de Lira. Relator: Desembargador Antonio Rigolin, 23 fev. 2022

ESTADOS UNIDOS DA AMÉRICA. **Circuit Court of Illinois**. Caso nº 2018 L011008. Autora: Mondelez International, Inc. Ré: Zurich American Insurance Company. Petição Inicial da Mondelez. 10 de outubro de 2018. Disponível em: https://pt.scribd.com/document/397265756/Mondelez-Zurich#.

ESTADOS UNIDOS DA AMÉRICA. **Superior Court of New Jersey**. Caso nº UNN-L-2662-18. Autoras: Merck & Co. e International Indemnity, Ltd. Rés: ACE American Insurance Company *et. al.* Juiz: Thomas J. Walsh. 13 jan. 2022. Disponível em: https://s3.documentcloud.org/documents/21183337/merck-v-ace-american.pdf.

ESTADOS UNIDOS DA AMÉRICA. **Supreme Court of Idaho**. Autores: Arthur E. Rosenau e Freda S. Ronesau. Ré: Idaho Mutual Benefit Association. Relator: Justice Dunlap. 17 jan. 1944. Disponível em: https://casetext.com/case/rosenau-v-ida-mut-benefit-assn.

ESTADOS UNIDOS DA AMÉRICA. **Supreme Court of South Carolina**. Recorrente: Kenneth Huggins, Jr. Recorridos: Citibank, N.A., Capital One Services, Inc., e Premier Bankcard, Inc. Relator: Joseph F. Anderson, Jr. Columbia, 13 de maio de 2003. Disponível em: https://law.justia.com/cases/south-carolina/supreme-court/2003/25691.html.

ESTADOS UNIDOS DA AMÉRICA. **Supreme Judicial Court of Massachusetts**. Autora: Marcela Stankus. Ré: New York Life Insurance Company. Relator: Justice Ronan. 29 out. 1942. Disponível em: https://casetext.com/case/stankus-v-new-york-life-ins-co.

ESTADOS UNIDOS DA AMÉRICA. **United States District Court of California**. Caso nº CV 13-3728 GAF (JCx). Autora: Hartford Casualty Insurance Company. Réus: Corcino & Associates e Stanford Hospital and Clinics. Juiz: Gary Allen Feess. Los Angeles, 7 de outubro de 2013. Disponível em: https://www.courtlistener.com/docket/4150126/hartford-casualty-insurance-company-v-corcino-associates/.

ESTADOS UNIDOS DA AMÉRICA. **United States District Court of Florida**. Caso nº 8:16-cv-2453-MSS-JSS. Autora: Innovak International, Inc. Ré: Hanover Insurance Company. Juíza: Mary S. Scriven. Tampa, 17 de novembro de 2017. Disponível em: https://casetext.com/case/innovak-intl-inc-v-hanover-ins-co.

ESTADOS UNIDOS DA AMÉRICA. **United States District Court of New York.** Caso nº 651982/2011. Autora: Zurich American Insurance Company. Réus: Sony Corporation of America e outros. Juiz: Jeffrey K. Oing. Nova York, 21 de fevereiro de 2014. Disponível em: https://techriskreportboutique.perkinscoieblogs.com/wp-

content/uploads/sites/26/2019/05/ZURICH-AMERICAN-INSURANCE-COMPANY-Plaintiff-v-SONY-CORPORATION-OF-AMERICA-Sony-C.pdf.

Leis e regulamentos consultados:

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resolucaon4CDANPD24.02.2023.pdf.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

BRASIL. **Decreto nº 3.505, de 13 de junho de 2000**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm. Acesso em: 01 mai. 2023

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm.

BRASIL. **Lei nº 13.260, de 16 de março de 2016**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9609.htm.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 01 mai. 2023.

BRASIL. **PNCiber – Apresentação do Projeto**. Brasília, 17 mai. 2023. Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf. Acesso em: 01 jun. 2023.

RECEITA FEDERAL. Perguntas e respostas pessoa jurídica 2022. **Brasília**, 31 dez. 2021. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/ecf/PeRPJ2022v1.pdf.

SECURITIES AND EXCHANGE COMMISSION. **CF Disclosure Guidance**: Topic No. 2 Cybersecurity. 13 out. 2011. Disponível em: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Acesso em: 20 mai. 2023.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Circular nº 579, de 13 de novembro de 2018**. Disponível em: https://www.in.gov.br/web/dou/-/circular-n-579-de-13-de-novembro-de-2018-50481886. Acesso em: 07 fev. 2023.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Circular nº 621, de 12 de fevereiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/circular-susep-n-621-de-12-de-fevereiro-de-2021-303756056. Acesso em: 15 mai. 2023.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Circular nº 637, de 27 de julho de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/circular-susep-n-637-de-27-de-julho-de-2021-334825686. Acesso em: 07 fev. 2023.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Circular nº 638, de 27 de julho de 2021**. Disponível em: https://www.in.gov.br/web/dou/-/circular-susep-n-638-de-27-de-julho-de-2021-335760591. Acesso em: 07 fev. 2023.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **Circular Susep nº 438, de 15 de junho de 2012**. Disponível em: https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/10290.

UNIÃO EUROPEIA. **Diretiva 2002/58/CE, de 12 de julho de 2002.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002L0058.

UNIÃO EUROPEIA. **Diretiva 2009/136/CE, de 25 de novembro de 2009**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32009L0136.

UNIÃO EUROPEIA. **Diretiva 95/46/CE, de 24 de outubro de 1995**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

UNIÃO EUROPEIA. **General Data Protection Regulation**, 04 mai. 2016. Disponível em: https://gdpr-info.eu/.

UNIÃO EUROPEIA. **Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

***Apólices de seguro consultadas (https://www2.susep.gov.br/safe/menumercado/REP2/Produto.aspx/Consultar)*:**

AIG SEGUROS BRASIL S.A. Cláusula Particular de Proteção por Interrupção de Rede. Processo Susep nº 15414.900466/2015-15, 26 fev. 2022.

AIG SEGUROS BRASIL S.A. Condições Gerais: Seguro de Proteção de Dados e Responsabilidade Cibernética. Processo Susep nº 15414.901341/2014-13, 26 fev. 2022.

AIG SEGUROS BRASIL S.A. Condições Gerais: Seguro de Responsabilidade Civil. Processo Susep nº. 15414.900484/2013-27, 15 set. 2022.

AIG SEGUROS BRASIL S.A. Condições Gerais: Seguro de Responsabilidade Civil. Processo Susep nº. 15414.900484/2013-27, 07 jun. 2013.

AIG SEGUROS BRASIL S.A. Condições Gerais: Seguro de Responsabilidade Civil. Processo Susep nº. 15414.900484/2013-27, 08 out. 2014.

ALLIANZ SEGUROS S.A. Apólice de Responsabilidade Civil por Ataques Cibernéticos. Processo Susep nº 15414.900593/2017-78, 01 mai. 2019.

ALLIANZ SEGUROS S.A. Condições Gerais: Responsabilidade Civil Geral. Processo Susep nº 15414.900730/2013-41, 06 set. 2013.

ALLIANZ SEGUROS S.A. Condições Gerais: Responsabilidade Civil Geral. Processo Susep nº 15414.900730/2013-41, 11 jan. 2020.

ALLIANZ SEGUROS S.A. Condições Gerais: Responsabilidade Civil Geral. Processo Susep nº 15414.900730/2013-41, 10 mai. 2022.

AXA SEGUROS S.A. Condições Gerais: Seguro de Responsabilidade Civil Geral. Processo Susep nº 15414.901611/2014-96, 15 out. 2014.

AXA SEGUROS S.A. Condições Gerais: Seguro de Responsabilidade Civil Geral. Processo Susep nº 15414.901611/2014-96, 20 fev. 2019.

AXA SEGUROS S.A. Seguro de Responsabilidade Cibernética e Proteção de Dados. Processo Susep nº 15414.615443/2022-29, 23 jun. 2022.

AXA SEGUROS S.A. Seguro de Responsabilidade Cibernética e Proteção de Dados a base de Reclamações com Notificação. Processo Susep nº 15414.603184/2023-74, 03 fev. 2023.

AXA SEGUROS S.A. Seguro de Responsabilidade Profissional, Cibernética e Proteção de Dados. Processo Susep nº 15414.615441/2022-30, 23 jun. 2022.

TOKIO MARINE SEGURADORA S.A. Seguro de Responsabilidade Civil Geral. Processo Susep n.º 15414.901076/2013-92, 03 set. 2013.

TOKIO MARINE SEGURADORA S.A. Seguro de Responsabilidade e Proteção Cibernética. Processo Susep nº 15414.900628/2018-50, 03 dez. 2022.

TOKIO MARINE SEGURADORA S.A. Seguro de Responsabilidade e Proteção Cibernética. Processo Susep nº 15414.900628/2018-50, 01 fev. 2023.

TOKIO MARINE SEGURADORA S.A. Seguro de Responsabilidade e Proteção Cibernética. Processo Susep nº 15414.900628/2018-50, 03 mar. 2023.

ZURICH MINAS BRASIL SEGUROS S.A. Condições Contratuais: Responsabilidade Civil Geral. Processo Susep nº 15414.900932/2013-92, 27 dez. 2016.

ZURICH MINAS BRASIL SEGUROS S.A. Condições Contratuais: Responsabilidade Civil Geral. Processo Susep nº 15414.901306/2015-85, 23 fev. 2023.

ZURICH MINAS BRASIL SEGUROS S.A. Zurich Cyber Solution: Apólice de Responsabilidade Civil por Violação de Segurança e Privacidade. Processo Susep nº 15414.900493/2016-61, 11 nov. 2022.