I ENCONTRO NACIONAL DE DIREITO DO FUTURO

INSTITUIÇÕES JURÍDICAS, INOVAÇÕES DE MERCADO E TECNOLOGIA

I59
Instituições jurídicas, inovações de mercado e tecnologia [Recurso eletrônico on-line] organização I Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores Vinicius de Negreiros Calado, Roney Jose Lemos Rodrigues de Souza e Clarice Marinho Martins – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2024.

Inclui bibliografia
ISBN: 978-85-5505-938-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os desafios do humanismo na era digital.
1. Direito do Futuro. 2. Humanismo. 3. Era digital. I. I Encontro Nacional de Direito do Futuro (1:2024 : Belo Horizonte, MG).

CDU: 34

Dom Helder
ESCOLA SUPERIOR

I ENCONTRO NACIONAL DE DIREITO DO FUTURO

INSTITUIÇÕES JURÍDICAS, INOVAÇÕES DE MERCADO E TECNOLOGIA

Apresentação

O Encontro Nacional de Direito do Futuro, realizado nos dias 20 e 21 de junho de 2024 em formato híbrido, constitui-se, já em sua primeira edição, como um dos maiores eventos científicos de Direito do Brasil. O evento gerou números impressionantes: 374 pesquisas aprovadas, que foram produzidas por 502 pesquisadores. Além do Distrito Federal, 19 estados da federação brasileira estiveram representados, quais sejam, Amazonas, Amapá, Bahia, Ceará, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Paraíba, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos 29 grupos de trabalho do evento, que geraram uma coletânea de igual número de livros que ora são apresentados à comunidade científica nacional, contou com a valiosa colaboração de 69 professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre as perspectivas dos principais ramos do Direito.

Tamanho sucesso não seria possível sem o apoio institucional de entidades como o Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), a Universidade do Estado do Amazonas (UEA), o Mestrado Profissional em Direito e Inovação da Universidade Católica de Pernambuco (PPGDI/UNICAP), o Programa RECAJ-UFMG – Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a Comissão de Direito e Inteligência Artificial da Ordem dos Advogados do Brasil – Seção Minas Gerais, o Grupo de Pesquisa em Direito, Políticas Públicas e Tecnologia Digital da Faculdade de Direito de Franca e as entidades estudantis da UFMG: o Centro Acadêmico Afonso Pena (CAAP) e o Centro Acadêmico de Ciências do Estado (CACE).

Os painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional. A abertura foi realizada pelo professor Edgar Gastón Jacobs Flores Filho e pela professora Lorena Muniz de Castro e Lage, que discorreram sobre o tema “Educação jurídica do futuro”. O professor Caio Lara conduziu o debate. No segundo e derradeiro dia, no painel “O Judiciário e a Advocacia do futuro”, participaram o juiz Rodrigo Martins Faria,

os servidores do TJMG Priscila Sousa e Guilherme Chiodi, além da advogada e professora Camila Soares. O debate contou com a mediação da professora Helen Cristina de Almeida Silva. Houve, ainda, no encerramento, a emocionante apresentação da pesquisa intitulada "Construindo um ambiente de saúde acessível: abordagens para respeitar os direitos dos pacientes surdos no futuro", que foi realizada pelo graduando Gabriel Otávio Rocha Benfica em Linguagem Brasileira de Sinais (LIBRAS). Ele foi auxiliado por seus intérpretes Beatriz Diniz e Daniel Nonato.

A coletânea produzida a partir do evento e que agora é tornada pública tem um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Além disso, busca-se formar novos pesquisadores nas mais diversas áreas do Direito, considerando a participação expressiva de estudantes de graduação nas atividades.

A Escola Superior Dom Helder Câmara, promotora desse evento que entra definitivamente no calendário científico nacional, é ligada à Rede Internacional de Educação dos Jesuítas, da Companhia de Jesus – Ordem Religiosa da Igreja Católica, fundada por Santo Inácio de Loyola em 1540. Atualmente, tal rede tem aproximadamente três milhões de estudantes, com 2.700 escolas, 850 colégios e 209 universidades presentes em todos os continentes. Mantida pela Fundação Movimento Direito e Cidadania e criada em 1998, a Dom Helder dá continuidade a uma prática ético-social, por meio de atividades de promoção humana, da defesa dos direitos fundamentais, da construção feliz e esperançosa de uma cultura da paz e da justiça.

A Dom Helder mantém um consolidado Programa de Pós-graduação Stricto Sensu em Direito Ambiental e Sustentabilidade, que é referência no país, com entradas nos níveis de mestrado, doutorado e pós-doutorado. Mantém revistas científicas, como a Veredas do Direito (Qualis A1), focada em Direito Ambiental, e a Dom Helder Revista de Direito, que recentemente recebeu o conceito Qualis A3.

Expressamos nossos agradecimentos a todos os pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 29 de julho de 2024.

Prof. Dr. Paulo Umberto Stumpf – Reitor da ESDHC

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação da ESDHC

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa da ESDHC

ESCORE DE RISCOS DE CIBERSEGURANÇA NOS SEGUROS DE RESPONSABILIDADE CIVIL PARA RISCOS CIBERNÉTICOS: PRECIFICAÇÃO E DELIMITAÇÃO DA GARANTIA

CYBERSECURITY RISK SCORE IN CIVIL LIABILITY INSURANCE FOR CYBER RISKS: PRICING AND DELIMITATION OF THE GUARANTEE

Kesya Luciana Do Nascimento Silva Vasco [1]
Roney José Lemos Rodrigues de Souza
Vinicius de Negreiros Calado

Resumo

O estudo do tema aborda o exponencial número de ataques cibernéticos ocorridos, expondo a dificuldade que as operadoras que comercializam o seguro de responsabilidade civil contra riscos cibernéticos, enfrentam em valorar as apólices e delimitar uma garantia mínima que abarque os prejuízos sofridos decorrentes de um incidente de segurança, isso devido a ausência de um mapeamento dos incidentes que possam fomentar os cálculos atuariais do seguro através das estatísticas de sinistralidade e de probabilidade propondo a criação de um escore de riscos considerando as peculiaridades do seguro de responsabilidade civil contra riscos cibernéticos.

Palavras-chave: Gerenciamento de risco, Cibersegurança, Seguro de responsabilidade civil, Riscos cibernéticos

Abstract/Resumen/Résumé

The study of the topic addresses the exponential number of cyber attacks that have occurred, exposing the difficulty that operators who sell civil liability insurance against cyber risks face in valuing policies and delimiting a minimum guarantee that covers losses suffered resulting from an incident of security, this is due to the absence of a mapping of incidents that can support actuarial insurance calculations through accident and probability statistics, proposing the creation of a risk score considering the peculiarities of civil liability insurance against cyber risks.

Keywords/Palabras-claves/Mots-clés: Risk management, Cybersecurity, Liability insurance, Cyber risks

[1] Mestranda em Direito e Inovação pela Unicap. Especialização em Compliance e ESG pela Unicap. Especialista em Processo Civil Contemporâneo, pela UFPE. Graduada em Direito pela Faculdade Maurício de Nassau.

1. INTRODUÇÃO

A crescente transformação digital e a rápida evolução tecnológica enfrentada nos últimos anos trouxeram consigo novos desafios para o mercado segurador, particularmente no que diz respeito ao seguro de responsabilidade civil por riscos cibernéticos. A dificuldade de padronização no valor da Apólice e na delimitação da garantia mínima desses seguros é exacerbada pela falta de definição clara e classificação dos riscos cibernéticos. Este artigo tem como objetivo abordar essa problemática, analisando, classificando e padronizando os riscos cibernéticos, a fim de auxiliar as operadoras de seguros na precificação e delimitação da garantia mínima do seguro de responsabilidade civil por riscos cibernéticos.

2. O MERCADO SEGURADOR E OS INCIDENTES DE ATAQUES CIBERNÉTICOS

De acordo com dados da Associação Brasileira de empresas de Software (ABES) obtidos través do relatório da Trend Micro[1], o ano de 20023 fechou com um novo recorde de 161 bilhões de ameaças bloqueadas, em todo o mundo, o que representa um crescimento de 10% em relação a 2022, quando ocorreram 146 bilhões de ataques.

Neste cenário há que se destacar os Estados Unidos, que ocupa o topo do ranking de e o Brasil que vem logo na sequência com no registro da maioria dos casos de ataques. Toda essa celeuma fez com que as empresas apressassem os passos na busca pela maturidade em segurança da informação, de modo que a implantação de planos de cibersegurança passassem a considerar questões técnicas que possam prever incidentes de modo a mitigar os danos.

Nesse sentido, o mercado segurador preocupado com o crescente número de casos de ataques cibernéticos tem encontrado um cenário fértil ao propor uma garantia securitária para que empresas tenham uma garantia mínima de que estão acobertadas se sofrerem um incidente de vazamento de dados, por exemplo.

Destarte, analisando a visão de BELLE (2023) sobre a cibersegurança como um "conjunto de normas, práticas e processos que permitem proteger sistemas críticos, informações particularmente importantes e, sobretudo, pessoas de potenciais riscos e ameaças cibernéticas" conclui-se que além da adoção de práticas de segurança cibernética é imprescindível que as

[1] A informação foi extraída da TREND MICRO 2023 MIDYEAR CYBERSECURITY THREAT REPORT, da Trend Micro de Agosto de 2023, empresa líder mundial em soluções de cibersegurança, disponível em:<< https://www.trendmicro.com/pt_br/about/threat-research.html>> e apresentada pela ABES (Associação Brasileira de Empresas de Software).

empresas tenham o mínimo de garantia securitária para viabilizar a manutenção de seus negócios.

Assim, é importante destacar que a proteção de dados é apenas uma das camadas que envolvem o conceito e a abordagem de Cibersegurança que inclui também a segurança das informações e a segurança de sistemas financeiros, além de segurança de infraestruturas críticas e de infraestruturas democrática (BELLE, 2023)

A era da disrupção digital, ou a chama Indústria 4.0 alavancada pela Pandemia da Covid-19 em 2020, trouxe consigo inúmeras formas operacionais de ataques cibernéticos sendo uma delas visivelmente identificada pela utilização em potência da Internet das coisas (IoT - *internet of things*), que viabiliza o acesso de diversos dispositivos dentro de um mesmo ambiente corporativo virtual, fruto da modalidade de trabalho *home office*, bem como a digitalização em larga escala de documentos para armazenamento na nuvem, a automatização de processos internos entre outros (GARCIA, 2021).

Neste ambiente, há que se considerar que o Brasil representa uma pequena parcela, mas não menos preocupante, diante dos casos notoriamente conhecidos mundialmente de grandes *players* que sofreram com ataques causando-lhes prejuízos de considerável monta. Com toda essa evolução a preocupação com o número de casos sobre incidentes de segurança tirou as empresas brasileiras da zona de conforto na busca por implementação de práticas de segurança que viabilizassem uma maior confiabilidade a seus clientes sobre a proteção de seus dados.

Após edição da Lei Geral de Proteção de Dados (LGPD) no Brasil as empresas que tratam dados pessoais e/ou sensíveis foram obrigadas a melhorar seus sistemas de governança da informação e privacidade de dados. A LGPD, juntamente com normativas internacionais como o GDPR (*General Data Protection Regulation*), estabelece diretrizes importantes para a proteção de dados, mas também impõe desafios adicionais para o mercado segurador, que precisa adaptar suas práticas para estar em conformidade com essas leis (PALHARES, 2021).

Nesse contexto, o mercado segurador tem se mostrado cada vez mais preocupado com a gama de incidentes de ataques cibernéticos, uma preocupação que se intensificou com a transformação digital. A proliferação de ataques como *phishing* (tentativas de fraude para obter ilegalmente informações como senhas bancárias, dados de cartão de crédito), *malware* (software maldoso que pode causar um o colapso no sistema corrompendo arquivos importantes ou sobrecarregando seus recursos), *ransomware* (software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo) e negação de serviços tem levado as empresas a buscarem seguros de responsabilidade civil contra riscos cibernéticos. No

entanto, a ausência de uma correta definição e classificação desses riscos tem dificultado a precificação adequada e a delimitação da garantia mínima necessária.

O tema ganha grande força através do último Fórum Econômico Mundial de 2023, cujo Relatório de Riscos Globais 2023 trouxe dados da última Pesquisa Global de Percepção de Riscos (GRPS) que dividiu a classe de riscos globais em duas categorias, as que representam ameaças a curto prazo (dois anos) e que seus impactos já estão sendo evidenciados nas crises atuais e as que ao longo da próxima década representará impactos significativos. Os riscos atrelados a Crime cibernético generalizado e insegurança cibernética ocupam a oitava posição nas duas categorias.

Ainda segundo o relatório supracitado, os riscos cibernéticos podem ultrapassar a intenção de atores meramente desonestos, uma vez que as obtenções de informações pessoais através de sistemas legais podem enfraquecer a soberania digital individual e o direito à privacidade, mesmo em ambientes bem regulamentados e democratizados trazendo consequências altíssimas não apenas para as instituições que realizam o tratamento dos dados, tampouco apenas para os titulares dos dados, mas para toda uma nação.

A implantação de boas práticas de Governança Corporativa nas empresas que visem a mitigação dos riscos de ataques de segurança amplia o dever de diligência dos administradores na prevenção e no enfrentamento de questões relacionadas a cibersegurança, quer na promoção interna de Políticas de Segurança da Informação, quer na adoção de um seguro de responsabilidade civil que garanta a manutenção do negócio em caso de ataques (LUPION; HACKMAN, 2023).

Dentre as práticas de segurança cibernéticas a serem adotadas pelos administradores das empresas porque não pensar em “ferramentas securitárias de tutela” (CARVALHO, 2021)? Ocorre que em virtude dos escassos registros oficiais de incidentes de segurança em um determinado banco de dados que viabilize a criação de um mapeamento dos riscos e prejuízos há ainda lacunas que precisam ser analisadas para robustecer a tutela securitária e viabilizar a construção de um Limite Máximo de Garantia que mais se aproxime dos efeitos que um ataque pode causar as empresas.

3. DESAFIOS NA PRECIFICAÇÃO E DELIMITAÇÃO DE GARANTIAS

A precificação do seguro de responsabilidade civil por riscos cibernéticos enfrenta diversos desafios, dentre os quais se destaca a dificuldade de delimitar os riscos cibernéticos. Esta dificuldade se deve à constante mutação dos tipos de ataques, que acompanham a evolução

tecnológica, e à falta de registros históricos abrangentes de incidentes. Essa ausência de dados dificulta a elaboração de cálculos atuariais precisos e a definição de limites de cobertura adequados.

Outra questão que merece destaque é a que ante a ausência de uma padronização dos riscos de ataques cibernéticos muitas apólices de seguro acabam sendo precificadas de forma equivocada apresentando valores de Limite Máximo de Garantia inferiores ao real prejuízo enfrentado pelas empresas, sobre esse tema aponta Carlini:

> Delimitar riscos é atividade fundamental para os contratos de seguro porque apenas dessa forma é possível pesquisar estatísticas de sinistralidade e efetuar cálculos de probabilidade. Os fundos mutuais que sustentam a atividade de seguro são organizados com estudos de estatísticas (passado) para construção de probabilidades (futuro), de forma que os cálculos atuariais estejam sempre sustentados pelo histórico de sinistralidade acrescido de margem de segurança (CARLINI, 2022).

Pela IBM Security, em parceria com o Ponemon Institute, o custo total médio de um incidente de violação de dados entre março de 2021 e março de 2022 foi de US$ 4,35 milhões, ou seja, um prejuízo calculado em 12.7% a mais que o mesmo período do ano de 2020. O Instituto considera nesse cálculo os custos relacionados à perda de negócios, detecção e encaminhamento, notificação e resposta pós-violação (MARCON, 2023).

Diante do aumento expressivo dos casos a procura por seguros contra riscos cibernéticos no pais movimentou a casa dos R$ 123 milhões entre janeiro e setembro de 2022, ou seja, um aumento de 161%, segundo dados da FenSeg, em relação ao ano de 2020.

O seguro contra ataques cibernéticos apresenta-se como ferramenta de gerenciamento de riscos da qual visa a cobertura de perdas e responsabilidades de terceiros em virtude de um incidente de segurança no ambiente digital Entretanto a delimitação dos riscos e o mapeamento de seus efeitos impactam diretamente na precificação de um LMG mais aproximado de seus prejuízos.

Assim, a ausência de registros de ataques pretéritos não só dificulta a atuação mais eficaz para a mitigação dos riscos cibernéticos, bem como anula a intenção das operadoras de seguro de mensurar os impactos que um ataque pode ocasionar a uma empresa. Além do que outros fatores devem ser considerados como premissa a essa dificuldade de delimitação, tais como a constante mutação dos tipos de ataques que acompanham evolução tecnológica, e a facilidade com que as pessoas compartilham seus dados no ambiente digital.

Diante da problemática ora abordada, quanto a ausência da correta delimitação dos riscos cibernéticos para a precificação e oferta de garantia mínima do seguro de responsabilidade civil contra riscos cibernéticos como uma das medidas de *cybersegurança* constitui o problema de pesquisa abordado neste trabalho.

4. PROPOSTA DE PESQUISA

O estudo propõe que seja realizada uma pesquisa com a metodologia qualitativa exploratória, utilizando a análise documental de registros de incidentes cibernéticos ocorridos entre 2020 e 2023, com o objetivo de mapear, avaliar e classificar os riscos cibernéticos envolvidos. Adicionalmente, propõe-se que sejam analisadas decisões administrativas do órgão fiscalizador de proteção de dados, bem como a jurisprudência e a legislação aplicável ao tema.

O objetivo é o mapeamento e classificação dos riscos cibernéticos para auxiliar na precificação. Este mapeamento deve considerar os impactos financeiros e reputacionais dos ataques, assim como a frequência e a gravidade dos incidentes. A construção de um banco de dados robusto com registros detalhados dos incidentes permitirá a elaboração de um score de riscos, baseado na ABNT ISO 27001, facilitando a definição de limites de cobertura adequados.

Contudo, não se pode olvidar que a análise das práticas adotadas por algumas operadoras de seguro para mitigar os riscos de ataques cibernéticos é crucial, sendo o estudo das medidas de segurança implementadas e dos controles adotados uma forma de fornecer insights valiosos para a construção do score de riscos cibernéticos e para a proposição de estratégias de mitigação eficazes.

Portanto, a troca de informações e a colaboração entre as operadoras também são instrumentos eficazes para a melhoria contínua das práticas de gestão de riscos.

5. RESULTADOS ESPERADOS E CONTRIBUIÇÕES DO ESTUDO

Espera-se que o estudo contribua para a padronização da precificação do seguro de responsabilidade civil por riscos cibernéticos, bem como para a delimitação adequada das garantias mínimas. A proposta de identificação e classificação dos riscos cibernéticos poderá ser utilizada como uma ferramenta prática pelas operadoras de seguros, auxiliando na mitigação dos riscos e na proteção das empresas contra os impactos financeiros e reputacionais dos ataques cibernéticos.

6. CONCLUSÕES

A rápida evolução tecnológica e a transformação digital intensificaram a necessidade de seguros de responsabilidade civil por riscos cibernéticos.

No entanto, a falta de padronização na precificação e delimitação das garantias mínimas tem se mostrado um desafio significativo para as operadoras de seguros.

Este estudo propõe uma pesquisa com abordagem sistemática para mapear, analisar e classificar os riscos cibernéticos, com o objetivo de auxiliar na precificação e delimitação das garantias dos seguros.

A construção de um banco de dados robusto e a análise das práticas de mitigação adotadas pelas operadoras são passos fundamentais para alcançar esse objetivo, contribuindo para a proteção do mercado segurador e das empresas contra os impactos dos ataques cibernéticos.

REFERÊNCIAS

ABES (Associação Brasileira de Empresas de Software). **2023 fecha com 161 bilhões de ataques cibernéticos, em mais um recorde, segundo relatório da Trend Micro**. 2024, Disponível em: <https://abes.com.br/2023-fecha-com-161-bilhoes-de-ataques-ciberneticos-em-mais-um-recorde-segundo-relatorio-da-trend-micro/#:~:text=Relat%C3%B3rio%20da%20Trend%20Micro%2C%20l%C3%ADder,ocorreram%20146%20bilh%C3%B5es%20de%20ataques>. Acesso em 22 de maio de 2024.

ABNT Disponível em: <<https://www.cetam.am.gov.br/wp-content/uploads/2022/02/09_ABNT_NBR_15287-2011_Projeto-de-Pesquisa-1.pdf>> Acesso em 21 fev. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018.

BELLI, Luca. [et al.]. **Cibersegurança [recurso eletrônico] uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano.**– Rio de Janeiro: FGV Direito Rio, 2023.

CARLINI, Angélica. **Nova regulação dos seguros de responsabilidade civil no Brasil e os seguros para riscos cibernéticos**. Revista IBERC, Belo Horizonte, v. 5, n. 2,p. 1-17,maio/ago. 2022. Disponível em: <<https://revistaiberc.emnuvens.com.br/iberc/article/view/225/171>> Acesso em 21 de fevereiro de 2024.

CARVALHO, Ângelo Prata de. XAVIER, Vitor Boaventura. **Seguros contra Riscos Cibernéticos: Elementos Dogmáticos para a Construção de Mecanismos Securitários em Face dos Riscos Oriundos das Tecnologias de Informação**. In: TZIRULNIK, Ernesto;

BLANCO, Ana Maria; CAVALCANTI, Carolina; XAVIER, Vítor Boaventura. Direito do Seguro Contemporâneo. Edição Comemorativa dos 20 Anos do Instituto Brasileiro de Direito de Seguro –IBDS. São Paulo: Editora Contracorrente, 2021.

Empresa Brasileira de Comunicação – EBC. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/ataques-hackers-movimentam-venda-de-seguros-contra-risco-cibernetico> Acesso em 21 de fevereiro de 2024.

FENSEG. Busca por seguro cibernético cresce no país, mas análise das apólices fica mais burocrática. 2023. Disponível em: << https://fenseg.org.br/noticias/busca-por-seguro-cibernetico-cresce-no-pais-mas-analise-das-apolices-fica-mais-burocratica>> Acesso em 21 de fev. de 2024.

GARCIA, Solimar. **Gestão 4.0: disrupção e pandemia**. São Paulo : Blucher, 2021. Disponível em: <<https://www2.cjf.jus.br/pergamumweb/vinculos/0000d1/0000d182.pdf>> Acesso em 21 de fevereiro de 2024.

LUPION, Ricardo; HACKMANN, Evaldo Osório. **Cibersegurança e dever de diligência do administrador**. REVISTA JURÍDICA LUSO-BRASILEIRA, Ano 9 (2023), nº 2.

MARCON, Daniele Verza. **Seguro Contra riscos cibernéticos: Desafios para Delimitar a garantia e promover a cibesegurança na era digital**. Dissertação de Mestrado. Universidade Federal de Rio Grande do Sul. Faculdade de Direito. Programa de Pós Graduação em Direito. Porto Alegre. 2023. Disponível em: << https://lume.ufrgs.br/handle/10183/267969>> Acesso em 21 de fevereiro de 2024.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance Digital e LGPD**. Coleção Compliance. v. V. São Paulo: Thomsom Reuters Brasil, 2021.

The Global Risks Report 2023. 18ª ed, Geneva, 2023, p. 8. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf>> Acesso em 21 fev. 2024.