PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ

ESCOLA DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

SUZANA ROSOSKI DE OLIVEIRA

CIBERSEGURANÇA COMO ELEMENTO DE DILIGÊNCIA DOS ADMINISTRADORES EM SOCIEDADES ANÔNIMAS

CURITIBA

2024

SUZANA ROSOSKI DE OLIVEIRA

CIBERSEGURANÇA COMO ELEMENTO DE DILIGÊNCIA DOS ADMINISTRADORES EM SOCIEDADES ANÔNIMAS

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Econômico e Desenvolvimento e na linha de pesquisa em Estado, Economia e Desenvolvimento, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Eduardo Oliveira Agustinho.

CURITIBA

2024

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Edilene de Oliveira dos Santos CRB 9 / 1636

O48c 2024

Oliveira, Suzana Rososki de
Cibersergurança como elemento de diligência dos administradores em sociedades anônimas / Suzana Rososki de Oliveira ; orientador: Eduardo Oliveira Agustinho. -- 2024
121 f. ; il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2024
Bibliografia: f. 109-121

1. Sociedades comerciais. 2. Inovações tecnológicas. 3. Computadores – Medidas de segurança. 4. Diligência. 5. Administradores de empresa. I. Agustinho, Eduardo Oliveira. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título

Doris 3. ed. – 342.225

TERMO DE APROVAÇÃO

SUZANA ROSOSKI DE OLIVEIRA

CIBERSEGURANÇA COMO ELEMENTO DE DILIGÊNCIA DOS ADMINISTRADORES EM SOCIEDADES ANÔNIMAS

Dissertação apresentada ao programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial para a aprovação no Mestrado em Direito.

COMISSÃO EXAMINADORA

_____

Professor Dr. Eduardo Oliveira Agustinho
Orientador PPGD – PUCPR

_____

Professor Dr. Oksandro Osdival Gonçalves
Membro PPGD – PUCPR

_____

Professor Dr. Giovani Saavedra
Membro externo – UPM

_____

Professor Dr. Luís Alexandre Carta Winter
Membro PPGD – PUCPR - Suplente

Curitiba/PR, 20 de março de 2024.

“A distância é curta quando se tem um bom motivo.”

(Jane Austen, “Orgulho e Preconceito”, 1813)

Uma homenagem à Catharina Rosowski

AGRADECIMENTOS

Agradeço ao meu orientador pela gentileza, ensinamentos, sabedoria e confiança durante os anos de desenvolvimento acadêmico e pessoal. Obrigada pela dedicação à orientação, entusiasmo, verdade em suas palavras e incentivos. As lições que aprendi serão carregadas sempre comigo.

À Pontifícia Universidade Católica do Paraná, por ser a instituição que me acolheu desde a graduação, época em que poucos eram os recursos financeiros, mas que, outrora, por meio das oportunidades concedidas, demonstrou não existir pontos limitantes ou impeditivos para que eu pudesse continuar. Afirmo com segurança que as conquistas posteriores se originaram após a graduação em direito na PUCPR.

Assim, estendo meus agradecimentos aos professores, pelo amor à profissão de lecionar, assim como por todo o engajamento e incentivo no desenvolvimento de pesquisas. Aos meus colegas de curso, pelo período de compartilhamento de emoções, vidas, momentos de desespero e alegrias.

À CAPES e ao CNPQ pelo incentivo e fomento à pesquisa científica, essenciais ao desenvolvimento social.

Agradeço também à minha família que, mesmo em meio a dificuldades, sempre buscaram forças para me ajudar na medida de suas possibilidades. Obrigada por demonstrarem que não há limites para a realização dos nossos sonhos. Por trazerem como características principais a força e a resiliência. Os frutos desta árvore também são seus, Roseli, Suzi, Marili, Neri, Rosa, Wesley e Vanessa!

À família que me recebeu, por todas as mensagens de incentivo, carinho e preocupação, agradeço e mantenho-as no coração, Laene, Sergio e Eduardo!

À minha avó, Catharina, que escolheu partir para o plano espiritual em agosto de 2022, por todo amor, fé, cuidado, ensinamentos e demonstração da força que uma família de origem matriarcal possui.

Aos meus amigos por todo apoio, risadas e incentivo.

Ao meu esposo, Sergio, por toda paciência, afeto, companheirismo e motivação. Obrigada por ser meu maior entusiasta e encorajador. Por comprar meus sonhos e objetivos, assim como partilhar sonhos e conquistas em conjunto.

Por fim, à Nossa Senhora Aparecida que, com seu manto sagrado, intercede por proteção e ilumina nossos caminhos.

“Dentre todos os fatores técnicos da mobilidade, um papel particularmente importante foi desempenhado pelo transporte da informação — o tipo de comunicação que não envolve o movimento de corpos físicos ou só o faz secundária e marginalmente. Desenvolveram-se de forma consistente meios técnicos que também permitiram à informação viajar independente dos seus portadores físicos — e independente também dos objetos sobre os quais informava: meios que libertaram os “significantes” do controle dos “significados”. A separação dos movimentos da informação em relação aos movimentos dos seus portadores e objetos permitiu por sua vez a diferenciação de suas velocidades.”

Globalização: as consequências humanas,
Zygmunt Bauman, 1999.

RESUMO

Há uma nova forma de sociedade na contemporaneidade, efeito da penetrabilidade da tecnologia em todas as esferas da vida humana. Como consequência, existe uma dependência de recursos tecnológicos e o incessante surgimento de novas modalidades de riscos, como os ataques por *ransomware.* A problemática da pesquisa circunscreve-se na possibilidade de reconhecimento de ações de cibersegurança como novos padrões de conduta esperados diante do dever de diligência dos administradores das sociedades anônimas de capital aberto, focalizando sociedades anônimas de capital aberto em razão da extensão de possíveis eixos afetados, somados com a sujeição à CVM. A hipótese desta dissertação reside no entendimento de que se trata de um problema que cabe ao dever de diligência. As variáveis, no entanto, inserem-se em: a. Na inexistência de relação entre consequências de ciberataques e tomada de decisão pelos administradores; b. Não cabimento de apurações ou responsabilizações de administradores pela ocorrência de incidente de ciberataque. Em geral, objetiva-se evidenciar o surgimento de uma nova conduta esperada frente ao dever de diligência dos administradores. De forma específica, almeja-se demonstrar o *modus operandi* dos ataques, apresentar *cases*, identificar boas práticas que possam ser utilizadas e, por fim, trazer cenários de responsabilidade existentes, assim como respectivas ações cabíveis face o administrador da S/A. Empregou-se, para tanto, o método hipotético-dedutivo de viés sociológico e jurídico, cotejando aos referenciais teóricos de tecnologia da informação e comunicação e aos de direito empresarial. A pesquisa foi dividida em três capítulos. O primeiro aborda aspectos da sociedade tecnológica, tipologias de ciberataques e a relação do tema com a proteção da privacidade e de dados pessoais. O segundo contempla a visualização de casos de enfrentamento de ataques por *ransomware*, com a apresentação de medidas de prevenção e combate aplicáveis. Por fim, o terceiro aborda configurações basilares ao cumprimento do dever de diligência, uma leitura das modalidades de responsabilização, dividindo por culpa, dolo, violação de lei ou estatuto e, ao final, medidas de responsabilização aplicáveis, seja em âmbito cível ou administrativo. Em conclusão, entende-se que medidas preventivas a ciberataques devem ser parte indissociável no cumprimento do dever de diligência dos administradores de sociedades anônimas abertas, considerando indubitável a presença dessa categoria de risco no contexto social, ao fácil acesso à estândares de mercado aplicáveis, corroborando para a adequada tomada de decisões. Considera-se, também, a presença de tendências normativas relacionadas, como a Lei Geral de Proteção de Dados e, ademais, que qualquer ausência ou razoabilidade de decisão oportuna e cabível demonstram falta para com os deveres de se informar, qualificar, fiscalizar, intervir, enfim, de participar e de bem administrar, evitando erros grotescos, configurações estas que são básicas quanto ao dever de diligência, podendo agravar situações de crise por ataque *ransomware*, expondo a empresa, a sociedade e o mercado a riscos, os quais poderão ser apurados pela Companhia ou pela Comissão de Valores Mobiliários.

Palavras-chave: Sociedade Tecnológica; Cibersegurança; Dever de Diligência; Administradores; Sociedades empresárias.

ABSTRACT

There is a new form of society in contemporary times, an effect of the penetrability of technology in all spheres of human life. Therefore, there is a dependence on technological resources and the incessant emergence of new types of risks, such as ransomware attacks. The research problem is limited to the possibility of recognizing cybersecurity actions as new standards of conduct expected in view of the duty of diligence of administrators of publicly traded corporations, focusing on publicly traded corporations due to the extent of possible affected axes, added to the subjection to the CVM. The hypothesis of this dissertation lies in the understanding that this is a problem that falls under the duty of diligence. The variables, however, are included in: a. In the absence of a relationship between the consequences of cyberattacks and decision-making by administrators; B. It is not appropriate to carry out investigations or hold administrators responsible for the occurrence of a cyber-attack incident. In general, the objective is to highlight the emergence of a new expected conduct in relation to the administrators' duty of diligence. Specifically, the aim is to demonstrate the modus operandi of attacks, present cases, identify good practices that can be used and, finally, present existing liability scenarios, as well as respective appropriate actions vis-à-vis the S/A administrator. To this end, the hypothetical-deductive method of sociological and legal bias was used, comparing the theoretical references of information and communication technology and those of business law. The research was divided into three chapters. The first addresses aspects of technological society, types of cyberattacks and the relationship between the topic and the protection of privacy and personal data. The second includes the visualization of cases of combating ransomware attacks, with the presentation of applicable prevention and combat measures. Finally, the third addresses basic configurations for fulfilling the duty of diligence, a reading of the modalities of liability, dividing by fault, intent, violation of law or statute and, at the end, applicable liability measures, whether in civil or administrative scope. In conclusion, it is understood that preventive measures against cyberattacks must be an inseparable part of fulfilling the duty of diligence of administrators of public limited companies, considering the presence of this risk category in the social context as undoubted, easy access to applicable market standards, corroborating for adequate decision-making. It is also considered the presence of related normative trends, such as the General Data Protection Law and, furthermore, that any absence or reasonableness of a timely and appropriate decision demonstrates a lack of compliance with the duties of informing, qualifying, monitoring, intervening , finally, to participate and manage well, avoiding grotesque errors, configurations that are basic in terms of due diligence, and can aggravate crisis situations due to ransomware attacks, exposing the company, society and the market to risks, which could be determined by the Company or the Securities and Exchange Commission.

Key-words: Technological Society; Cybersecurity; Duty of Care; Administrators; Business Corporations

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
CC	Código Civil
CCPA	*California Consumer Privacy Act*
CF88	Constituição da República Federativa do Brasil de 1988
COBIT	*Control Objectives for Information and related Technology*
Covid-19	Vírus “SARS-CoV-2” (ou “Coronavírus”)
CVM	Comissão de Valores Mobiliários
DPO	*Data Protection Officer*
GDPR	*General Data Protection Regulation*
EDBP	*European Data Protection Board*
EC	Emenda Constitucional
GAFI	Grupo de Atuação Financeira
IA	Inteligência Artificial
IBGC	Instituto Brasileiro de Governança Corporativa
IBGE	Instituto Brasileiro de Geografia e Estatística
IdC	Internet das Coisas (do IOT – Internet of things)
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018)
LSA	Lei das Sociedades Anônimas
MCI	Marco Civil da Internet (Lei n.º 12.965/2014)
NIST	*National Institute of Standards and Technology*

OT	*Operational Technology*
P2P	*Peer-to-Peer*
PAS	Processo Administrativo Sancionador
PROCON	Órgão Proteção e Defesa do Consumidor
RGPD	Regulamento Geral de Proteção de Dados (Diretiva UE 679/2016)
TI	Tecnologia da Informação
TICs	Tecnologias da Informação e Comunicação
S/A	Sociedade Anônima
SEC	*Securities and Exchange Commission*
SI	Segurança da informação
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

Na contemporaneidade, nossa economia é muito atrelada à tecnologia, como consequência, existem pontos de risco e atenção que passam despercebidos por algumas corporações. Eis o mote que move esta pesquisa.

A atuação profissional focada na gestão de riscos e *compliance*, somada ao monitoramento do mercado e mídias, permitiu-nos observar o tendente aumento na incidência de casos envolvendo grandes corporações e ciberataques, sobretudo ataques na modalidade de sequestro – por meio de criptografia de sistemas – com pedidos de resgate em criptomoedas (denominados de *ransomware*).

Em reflexão à vivência profissional, os usos dos valores recebidos a título de resgate podem, inclusive, atrelar-se a outras categorias de delitos, como os relacionados a guerras virtuais ou o financiamento de organizações terroristas. Em conjunto, os tópicos comumente noticiados abarcam a esfera de surgimento de crises, dificuldade de restabelecimento de operações e sistemas, danos sofridos, como, por exemplo, os possíveis riscos de reputação negativa, perdas financeiras inestimadas ou responsabilidades legais sobre dados pessoais expostos.

Por outro lado, invariavelmente, o objetivo dos cibercriminosos consiste na elaboração de ataques que causem impactos negativos severos a uma organização, de modo a demonstrar dependência e submissão aos cibercriminosos para a retomada das operações e dados. Eles almejam a percepção de dependência de recursos de tecnologia em operações basilares, induzindo aos tomadores de decisão da organização à realização do pagamento do resgate pretendido como a única e melhor ação a ser adotada.

Ponderando sobre a situação, consideramos que vivemos em uma sociedade dependente de tecnologia – conforme evidenciado pelo estudo de Adam Greenfield (2006) –, parte de um fenômeno denominado como *Paradigma Everyware*, em que todas as esferas da sociedade possuem recursos tecnológicos nelas imbuídos.

Não forçosamente, verificamos que o ambiente de ensino utiliza e demanda das tecnologias de informação e comunicação para a realização de pesquisas e compartilhamento de informações.

Da mesma forma, os ambientes laborais são interligados por redes corporativas ou industriais, de modo a otimizar o tempo de processamento e partilha de informações e operações essenciais à manutenção e perenidade operativa da organização.

Em cenários industriais, vemos recursos como a "*internet* das coisas", "aprendizagem de máquina", "inteligência artificial" e "big data" como presentes na automatização e compreensão das máquinas utilizadas como parte das linhas de produção e distribuição de bens.

As interações sociais hoje também são fomentadas por tecnologias, sobretudo pelos aplicativos de redes sociais, que permitem que pessoas de diversos lugares e fusos possam se comunicar em tempo quase real. Assim ocorrem também algumas atividades de lazer por meio de recursos tecnológicos, a título de exemplo, empresas de *streaming* e de jogos digitais.

Nesta toada, como vislumbrado por Manuel Castells (2016), há uma nova forma de sociedade constituída, oriunda de mudanças de paradigmas sociais, econômicos, culturais e tecnológicos, na qual ocorre a penetrabilidade da tecnologia em todas as esferas da vida humana. Com efeito, há uma consequente dependência de recursos tecnológicos pela sociedade.

Perfazendo uma somatória de fatores, salientamos o surgimento de novas modalidades de riscos como os ciberataques, que se utilizam da dependência tecnológica como insumo para o aumento dos ataques, como dito anteriormente.

No ambiente corporativo, os efeitos de um ataque podem ser agravados quando se observa a interrupção das operações de produção e distribuição de bens, a administração dos negócios e a exposição de dados pessoais tratados. Assim sendo, existem riscos acerca da perenidade das organizações, sobre a estabilidade de determinado mercado e aos respectivos públicos relacionados, que podem ser clientes, investidores, trabalhadores, fornecedores, ou, ainda, agentes indiretamente vinculados à entidade empresarial.

Junto a isso, refletimos sobre os impactos negativos causados no contexto de sociedades de capital aberto, reguladas pela Comissão de Valores Mobiliários, que, a depender da severidade de um ataque, falta de transparência ou ausência de postura adequada ao tratamento da crise, tendem a ensejar uma crise ao próprio eixo mobiliário, como na incidência de efeito manada na venda de ações, na perda

de confiança sobre determinado mercado listado em bolsa, na geração de crise a fornecedores e investidores também listados, desencadeando uma reação em cascata.

Perguntamo-nos, portanto, se a cibersegurança ou, em outros termos, a adoção de ações preventivas a ciberataques devem ser parte de novos padrões de conduta esperados do dever de diligência dos administradores das sociedades anônimas de capital aberto.

O recorte compreende a extensão de públicos possivelmente afetados por um incidente de tecnologia, pela sujeição de companhias à Comissão de Valores Mobiliários, que *per si* já dispõe de algumas medidas de comunicação e tratamento normatizadas e exigidas.

Objetivamos, nessa direção, evidenciar o surgimento desse ponto de atenção como um novo padrão de conduta esperado ao dever de diligência dos administradores, restando como inegociável quando da assunção da posição de administração de uma companhia. De forma específica, buscamos demonstrar o *modus operandi* dos ataques, apresentando *cases* de organizações por capitais que vivenciaram ataques por *ransomware*; identificando boas práticas que possam ser utilizadas para a tomada eficiente de decisões nas organizações; analisando cenários de responsabilidade existentes e invocáveis nas respectivas ações de responsabilidade diante o administrador da sociedade anônima.

Empregamos, aqui, o método hipotético-dedutivo de viés sociológico e jurídico, conjugando perspectivas sobre tecnologia da informação e comunicação atreladas ao direito empresarial, com procedimento histórico e comparativo.

A hipótese desta pesquisa parte da constatação de que decisões e medidas adequadas à prevenção ou tratamento de crises relacionadas a ciberataques devem ser parte indissociável quanto ao cumprimento do dever de diligência.

A *contrário sensu*, vemos como possíveis variáveis: a. o afastamento entre as consequências de um ciberataque e as ações decisórias por parte dos administradores; b. o descabimento de ações de responsabilização dos órgãos de administração de uma companhia aberta pela ocorrência de ciberataques e consequentes crises instauradas.

Para demonstrar o percurso analítico e a conclusão da pesquisa, o trabalho está dividido em três capítulos. O primeiro abordará os diversos aspectos da

sociedade tecnológica, as tipologias de ciberataques existentes e seu modo de realização, ao final, cotejando uma possível relação com a temática da proteção da privacidade e de dados pessoais, respaldados por legislação própria, como a Lei Geral de Proteção de Dados brasileira.

O segundo capítulo relatará o estudo de casos recentes de enfrentamento de ataques por *ransomware*; quais as ações foram adotadas pelas entidades; a apresentação de medidas de prevenção e combate aplicáveis para os casos analisados, assim como para demais organizações, as quais poderão ser vistas como boas práticas de entendimento e aplicação em segurança da informação, aqui mencionado em sentido amplo.

Por fim, o terceiro abordará especificamente as configurações basilares para o cumprimento do dever de diligência. Perfazendo, em decorrência, a demonstração das modalidades de responsabilização existentes, divididas preliminarmente por culpa, dolo, violação de lei ou estatuto. Ademais, discutimos medidas de responsabilização aplicáveis, seja em âmbito cível ou administrativo, e as consequentes sanções aplicáveis para tanto.

2 DESAFIOS NAS ESTRUTURAS EMPRESARIAIS ATRELADOS AO USO DA TECNOLOGIA E DADOS PESSOAIS

No prefácio da obra *Sociedade em Rede* (2016), de Castells, Fernando Henrique Cardoso trata da investigação científica desta nova “modalidade” de sociedade como um “paradigma tecnológico”, gerador de um “novo modo de desenvolvimento”: qual seja, o desenvolvimento humano com suporte de recursos tecnológicos. Há uma ruptura de contextos entre o início e o final do século XX, caracterizada pela atuação de “redes interligadas”, mas sem, contudo, substituir o modo econômico predominantemente capitalista[1].

Com base nessa percepção, esta pesquisa aborda novos cenários de riscos e consequente surgimento de responsabilidades, oriundas de uma sociedade tecnológica em suas diversas teorias relacionadas[2345678910], como a descrita por Castells, qual seja, informacional.

Culminando certa relevância em atividades voltadas exclusivamente a novas tecnologias no cenário econômico mundial, somando-se à vivência social e empresarial, em dependência de recursos tecnológicos e de informações resolutas em dados, considerados essenciais para a perenidade de organizações.

Como fonte de reflexão inicial deste tópico, é importante exemplificar como são nítidas as mudanças existentes no ambiente econômico, empresarial e social do século passado (XX) para o presente (XXI). Nesta pesquisa, é imperioso começar

---

[1] CARDOSO, Fernando Henrique. Prefácio. *In*: CASTELLS, Manuel. **A Sociedade em Rede**. Trad. Roneide Venancio Majer. 17. ed. São Paulo: Paz eTerra. 2016. p. 57 e 58.
[2] CASTELLS, Manuel. **A Sociedade em Rede**. Trad. Roneide Venancio Majer. 17. ed. São Paulo: Paz eTerra. 2016.
[3] Paradigm everyware, *Cf.*: GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. Berkeley: New Riders, 2006.
[4] Disciplina, vigilância e controle, *Cf.*: RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
[5] Disciplina, vigilância e controle, *Cf.*: DELEUZE, Gilles. Conversações. Trad. Pelbart, Peter Pál. São Paulo: Ed. 34, 1992.
[6] Disciplina, vigilância e controle, *Cf.*: FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.
[7] Civilidade Tecnológica, *Cf.*: JONAS, Hans. **O princípio responsabilidade**: Ensaio de uma ética para a civilização tecnológica. Trad. Marijane Lisboa e Luiz Barros Montez. Rio de Janeiro: Editora Contraponto, PUCRJ. 2006.
[8] Cultura Algorítmica, *Cf.*: STRIPHAS, Ted. Algorithmic culture. **European Journal of Cultural Studies**, v. 18, n. 4-5, 2015, p. 395-412.
[9] ELLUL, Jacques. **The Technological Society**. New York, Vintage Books, 1964.
[10] SCHUURMAN, Egbert. **Reflections on the Technological Society**. Ontario: Wedge Publishing Foundation, 1983.

pela abordagem dos conceitos de empresário e empresa, que não se confundem: a empresa é a atividade econômica organizada e desenvolvida profissionalmente pelo empresário. Esse, como mencionado, é aquele definido pelo Art. 966 do Código Civil Brasileiro, de 2002, o qual diz: "Considera-se empresário quem exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços".

Partindo dessa breve definição legal do conceito de empresário, incumbe extrair algumas características necessárias, definidas por: a. economicidade; b. profissionalidade; c. assunção e gestão de riscos; d. posição direcionadora ao mercado.

A economicidade, por sua vez, advém do desenvolvimento de atividade econômica pelo empresário – sujeito de direitos que gerencia a empresa –, cujo objetivo consiste na geração de lucro ou riqueza[11]. Para que haja a presença da característica da economicidade, é importante que os órgãos da empresa tenham noções sobre os meios de produção empregados[12] para a geração de bens ou serviços, assim como conhecimento sobre a estrutura da organização.

Para além, há de se considerar o profissionalismo durante o exercício da atividade empresarial. Aqui, englobam-se os conceitos de pessoalidade (o agente), habitualidade no exercício (repetição da atividade empresarial) e monopólio de informações, ou seja, deter todo o conhecimento e informação necessária acerca do objeto da atividade exercida pela empresa, em relação aos insumos, maquinários, forma de criação ou prestação de serviço e outros.

A assunção de riscos consiste na definição do apetite[13] tolerável[14] de

---

[11] MENDONÇA, Saulo Bichara. Função Social da Empresa – Análise Pragmática. **Revista de Estudos Jurídicos da UNESP**, v. 16, n. 23, 2012.

[12] Saulo traz em sua composição o surgimento das corporações por meio da produção artesanal, na qual se constituíam centros de consumo e trocas, sendo esse o ponto basilar de entendimento de produção como fonte de lucro ou riqueza. *Cf.* ASCARELLI, Tullio. Origem do Direito Comercial. Trad. Fabio Konder Comparato. *In*: **Revista de Direito Mercantil, Industrial, Econômico e Financeiro**. n. 114. São Paulo: Malheiros Editores, 1996.

[13] "*O apetite ao risco está associado ao nível de risco que a organização está disposta a aceitar na busca e na realização de sua missão. Ele deve ser estabelecido pelo conselho de administração (CA) (ou pelos sócios, caso a organização não possua conselho), levando em conta o melhor interesse da organização, e serve como ponto de referência para a fixação de estratégias e para a escolha dos objetivos relacionados a essas estratégias.*" *Cf.* INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos**: evolução em governança e estratégia. São Paulo, SP: IBGC, 2017. p. 15.

[14] "*A tolerância ao risco pode ser vista como a variação aceitável em torno dos limites estabelecidos. Dentro dos riscos e exposições aceitáveis, os limites de tolerância são 'gatilhos' para atuação do conselho de administração. Indicadores de riscos e indicadores da efetividade dos hedges devem ser*

problemas a serem “aceitos”, por ser característica inerente de toda atividade empresarial. É inegável que ele poderá decidir o grau tolerável, mas deverá ter ciência de que haverá a existência de riscos, mesmo que de nível baixo.

No aspecto prático e real, de acordo com Marcelo Sacramone[15], somando ao conceito trazido por Rubens Requião[16], que o empresário, portanto, é aquele com poder para determinar o caminho de uma empresa e seu objeto de atividade; junto a isso, deve ser aquele que suporta os prejuízos da atividade ou aufere lucros pelos seus respectivos resultados.

Nesse sentido, esportes como a Fórmula Um (F1) e suas respectivas equipes participantes passaram por uma mudança de cenário envolvendo patrocínios, antes caracterizados, por exemplo, por empresas[17][18][19] de cigarro[20], como a Marlboro, Camel e John Player Special, para empresas do ramo de tecnologia[21], como a Oracle, Google Chrome e Cognizant.

Em sentido similar, em estudo publicado pela *Forbes*, em junho de 2023,

---

acompanhados pelo conselho de administração” *Cf.* ROSS, Stephen A.; WESTERFIELD, Randolph W.; JAFFE, Jeffrey. **Administração Financeira**. Porto Alegre: Grupo AMGH, 2015, p. 924.

[15] SACRAMONE, Marcelo B. **Manual de Direito Empresarial**. São Paulo: Editora Saraiva, 2023. E-book. p. 27.

[16] REQUIÃO, Rubens. **Curso de direito comercial**. 33. ed. São Paulo: Saraiva, 2014. p. 75.

[17] Cabe mencionar a escolha por se utilizar o termo ‘empresa’ de modo indiferenciado na pesquisa, não se optando por realizar as classificações da teoria do direito comercial. A justifica para tanto se dá pela amplitude de objetivos e alcances acerca da empresa, assim como ao vislumbrar o fácil entendimento durante a leitura por não operantes do direito.

[18] É importante destacar a diferença conceitual entre empresa e sociedade empresária. Nas lições de Coelho (2013, p. 127), entende-se por empresa aquela com a possibilidade de exploração por pessoa física ou jurídica. No caso do exercício, por pessoa física, tem-se o denominado empresário individual. No aspecto da explorada por pessoa jurídica, a sociedade empresária. Neste posto, ressalta-se que, por ser uma pessoa jurídica explorando determinada atividade, não se pode chamar os respectivos sócios da sociedade empresária como empresários. A empresa, portanto, subsome-se como “sendo atividade, cuja marca essencial é a obtenção de lucros com o oferecimento ao mercado de bens ou serviços, gerador estes, mediante a organização dos fatores de produção (força de trabalho, matéria-prima, capital e tecnologia)” (Coelho, 2013, p. 32-33). *Cf.* COELHO, Fábio Ulhoa. **Curso de Direito Comercial**. Volume 1: direito de empresa. 17. ed. São Paulo: Saraiva, 2013.

[19] Destacando a sociedade empresária, cabe apresentar o escopo de sua constituição como sendo a união de habilidades, capital e serviços, almejando maior sucesso na atingimento do lucro, ponto este inato à atividade empresarial. Através de tais uniões, tem-se a sociedade empresária, que explora a empresa, ou seja, a atividade empresarial. *Cf.* GOMES, Fábio Bellote. **Manual de Direito Empresarial**. 4. ed. São Paulo: Revista dos Tribunais, 2013. p. 39 a 41. Ainda, na visão de Verçosa, refere-se a uma interação bem definida e regulada, com objetivos, interesses e ações especificados e de tamanho adequado ao almejado. *Cf.* VERÇOSA, Haroldo Malheiros Duclerc. **Curso de Direito Comercial**. Volume 1. 2. ed. São Paulo: Malheiros, 2008. p. 159.

[20] ABREU, José Luis. Grandes patrocinadores. **Autosport**, 20 de março de 2024.

[21] VENTUROLI, Emanuele. Os 275 acordos de patrocínio da Fórmula 1 de 2023. **RTR Sports Marketing**, 24 fev. 2023.

nomeado como *Ranking Global 2000*[22], apresentou empresas de tecnologia, como a *Alphabet* (sociedade controladora da Google), *Microsoft*, *Apple*, *Samsung Eletronics* como empresas participantes do rol de maiores empresas do Mundo, em conjunto com aquelas do ramo bancário, de investimentos, de petróleo e agricultura.

Diante disso, há também a presença de novas profissões[23] relevantes para ações de incentivo ao consumo e movimentação da economia, como *social medias*, *influencers*, agentes de *marketing* digital, gestores de tráfego pago, profissionais de tecnologia e segurança da informação em sentido amplo.

Os exemplos acima citados são reflexos de uma nova sociedade de consumo[24] e da economia movida por dados (*Data Driven)*, essenciais para a movimentação da economia, dependente e atraída por produtos tecnológicos, como equipamentos celulares, computadores e demais mecanismos "inteligentes", tornando-as usuárias frequentes de redes sociais por meio de mecanismos de publicidade direcionada ao consumidor[25].

Tais fatores indicam que a tecnologia e os dados fazem parte dos mais variados plexos empresariais e sociais, razão pela qual o movimento econômico hoje é, também, tecnológico[26].

Considerando fatores de dependência do uso de recursos tecnológicos e dados[27] para a realização de operações comerciais, também verificamos o uso de tecnologia na adoção de ações preventivas, objetivando a perenidade de uma organização empresarial no contexto atual. Para tal propósito, há a presença de externalidades[28] sobre o desenvolvimento de atividade inovativa, adequada à sociedade de consumo (atrativa), estável, lucrativa e de confiança para com seus

---

[22] MURPHY, Andrea; TUCKER, Hank. Forbes Global 2000: Quais são as maiores empresas do mundo em 2023. **Forbes**, 9 jun. 2023.
[23] BECK, Milton. **Emerging Jobs Report Brazil**. LinkedIn, 2020. 1 apresentação, 25 banners.
[24] BAUMAN, Zygmunt. **Vida para consumo**. Rio de Janeiro: Zahar, 2008.
[25] Guilherme Misugi entende que vivemos em uma sociedade de hiperconsumo, ocasionada por estímulos que vão para além das necessidades de sobrevivência, expondo a fragilidade humana em seus aspectos sensoriais, culturais e socioantropológicos, carecendo de medidas de proteção ao consumidor em sua amplitude. *Cf.* MISUGI, Guilherme. **Tutela Jurídica das Novas Práticas Mercadológicas**: manipulação do comportamento do consumidor. Curitiba: Juruá, 2018. p. 75; 100.
[26] NOVAS TECNOLOGIAS: tendências e o que esperar para o futuro. **CNN BRASIL**, 10 abr. 2023.
[27] GOMES, Irene. CABRAL, Umberlância. 84,9% das indústrias de médio grande porte utilizaram tecnologia digital avançada. **Agência IBGE notícias** 28 set. 2023.
[28] GICO JR, Ivo T. Introdução à Análise Econômica do Direito. *In*: KLEIN, Vinicius; RIBEIRO, Marcia Carla Pereira (Coord.). **O que é análise econômica do direito**: uma introdução. Belo Horizonte: Editora Fórum, 2011.

diversos *stakeholders*[29].

Castells entende que a revolução da tecnologia da informação penetrou em todas as esferas da sociedade[30], é através de tal constatação que a pesquisa fora desenvolvida, retratando questões sobre a dependência de recursos tecnológicos e dados em estruturas empresariais e sociais e consequentes novos fatores de atenção pelos administradores de sociedades anônimas. Para além das obras de Castells, serão abordados outros conceitos acerca de uma sociedade voltada a recursos tecnológicos, informacionais e de comunicação, mas sem, contudo, aprofundá-las.

Acrescentar-se, portanto, o reflexo do paradigma *everyware* e a definição de computação ubíqua de Greenfield (2006), tratado como essencial para a compreensão do cenário invisível da tecnologia na sociedade, base teórica aprofundada no subtópico específico.

Como mencionado, não se exclui a existência de outras classificações similares. No entanto, não serão objeto de aprofundamento na presente pesquisa, são algumas delas: 1) a sociedade da disciplina, vigilância e controle, tratadas por Michel Foucault[31], Stefano Rodotá[32] e de Gilles Deleuze[33], em um mundo contemporâneo; 2) o entendimento sobre a vivência humana em uma cultura algorítmica, com Ted Stiphas[34], e sociedade tecnológica de Jacques Ellul[35] e Egbert Schuurman[36], para a compreensão da nova economia tecnológica envolta sobre o tratamento e utilização de dados, também como parte das linhas de fomento de *big data*; 3) em um viés voltado à atuação ética e responsável das tecnologias em sociedade, cita-se a pesquisa de Hans Jonas[37], que focaliza uma visão filosófica sobre como pessoas e empresas devem agir diante da construção de novas tecnologias.

Considerando novas modalidades de influência e incentivo ao consumo,

---

[29] “Àquele que possui interesse.”. *Cf.* Stake: interesse. Holders: aqueles que possuem.
[30] CASTELLS, *op. cit.*, p. 64.
[31] FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.
[32] RODOTÀ, *op. cit.*, p. 36.
[33] DELEUZE, *op. cit.*
[34] STRIPHAS, Ted. Algorithmic culture. **European Journal of Cultural Studies**, v. 18, n. 4-5, 2015. p. 395-412.
[35] ELLUL, *op. cit.*
[36] SCHUURMAN, *op. cit.*
[37] JONAS, *op. cit.*

também é relevante considerar as reflexões de Zygmunt Bauman[38], em especial, sua abordagem sobre a vida para o consumo e o consumo líquido.

Por fim, quanto ao referencial teórico basilar para uma visualização do cenário proposto na pesquisa, fundamental é a abordagem que trata da sociedade de risco idealizada por Ulrich Beck[39], considerando as incertezas oriundas de inovações tecnológicas e aceleração social, ensejando novos cenários de riscos globais, destacada com mais profundidade no subtópico seguinte.

A soma de tais conceitos gera um resultado comum: as tecnologias de informação e comunicação causam impactos positivos e negativos na sociedade, sobretudo à sociedade dos anos 2000.

A partir dos diferentes conceitos trazidos, em relação aos possíveis cenários resultantes da relação de dependência social às tecnologias da informação e comunicação, o segundo subtópico abordará algumas categorias de risco, classificados tecnicamente por incidentes de tecnologia; no terceiro subtópico, o surgimento e relevância quanto à adoção de medidas de proteção de dados pessoais, bem como às legislações diretamente relacionadas e a constituição federal.

No segundo capítulo, junto às problemáticas teorizadas neste tópico, evidencia-se cenários reais e recentes de crises empresariais geradas por incidentes de cibersegurança, através de *cases* e da existência de padronização nos ataques.

Ao final, no último capítulo, manifesta-se pela presença de novos e evidentes cenários de atenção de administradores de sociedades empresárias, os quais devem demandar uma adoção de novas medidas de tratamento precoce diante de possíveis situações de crise, a fim de reduzir riscos de continuidade da organização empresária por eles administrada. Como resultado, portanto, espera-se um novo fator para atendimento do dever de diligência dos administradores de sociedades anônimas.

2.1 DEPENDÊNCIA DO USO DA TECNOLOGIA E DADOS

Há uma coexistência “invisível” de tecnologias da informação e comunicação

[38] BAUMAN, op. cit.
[39] BECK, Ulrich. Sociedade de risco: Rumo a outra modernidade,2. ed. São Paulo: Editora 34, 2011.

(TICs) na vida social. Percepção inicialmente cunhada por Greenfield, denominando esse fenômeno social como o “paradigma *everyware*[40]”, que significa, em tradução literal, “todo dispositivo”.

Esse paradigma é resultante da existência da computação ubíqua, ou seja, tecnologia presente em todos os cenários da vivência humana, não somente em referência a equipamentos computacionais por si só, mas, sim, à presença da tecnologia em tudo, principalmente em função dos novos meios de produção, distribuição, comércio e consequente utilização e descarte. Nesse sentido, direta ou indiretamente, o ser humano e todas as outras coisas estão integradas em rede.

Sobre a rede, coaduna-se a possibilidade de conexão, coleta e troca de informações entre as diversas partes pertencentes da rede e em variados momentos. Tal percepção trazida por Greenfield é parte de um conjunto de pesquisas sobre tecnologias, em específico, as informacionais e comunicacionais, para com a sociedade atual[41].

Por conseguinte, através dessas pesquisas, não é forçoso constatar que tecnologias da informação e comunicação estão diretamente ligadas em nosso contexto social, como teorizado por Greenfield, Castells, Byung-chul Han[42], Rodotá, Jonas, Claus Schwab[43] e outros que esta pesquisa não objetiva apresentar.

Um dos conceitos norteadores deste trabalho é o da sociedade informacional[44], movida por dados e dependente de recursos tecnológicos para a realização de suas mais variadas ações, como interações sociais, atuação laboral, desenvolvimento e inovação. Consideramos a ideia de sociedade informacional com Castells, diante de sua amplitude. Para ele, a nova modalidade de economia (informacional, global e em rede) foi inserida em um cenário global no século XX. Para tanto, o autor define como informacional em razão da dependência humana em gerar, processar e aplicar a informação de forma eficiente nos contextos da produção e concorrência, resultando em informações oriundas do conhecimento[45].

O uso das tecnologias também é global face à extensão de atividades

---

[40] GREENFIELD, *op. cit*., p. 10-17.
[41] *Ibid.*, p. 33.
[42] HAN, Byung-chul. **NO ENXAME**: Perspectivas do Digital. Trad. Lucas Machado. Petrópolis, Rio de Janeiro: Editora Vozes, 2018.
[43] SCHWAB, Claus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2018.
[44] CASTELLS, *op. cit.*, p. 64-66.
[45] *Ibid*., p. 135.

produtivas, do consumo, da circulação e das próprias matérias-primas, as quais ultrapassam barreiras territoriais, gerando amplitude operacional em escala mundial. Exemplifica-se com o caso de produção de veículos automotores, cuja produção de componentes é feita em países distintos e, posteriormente, enviados para um país onde há indústria de montagem; ao final, os veículos são exportados para outros países para venda.

Como anteriormente mencionado, vivemos em uma sociedade em rede, motivada pela interação entre redes empresariais, fomentando a produção e a competitividade[46].

Sem esgotar as demais linhas de pesquisa de Han, traz-se sua interessante visão, a qual aduz que a sociedade atual vive em um mundo do "*homo digitalis*"[47]. Definida pela entrada e permanência de massas em ambientes digitais como uma forma de ser conhecido como "alguém no mundo", mesmo que de forma anônima; o agente que não vive (faz uso) em ambientes digitais é percebido como um ninguém.

Vê-se então que o fator de dependência tecnológica pode ser gerado por uma movimentação de massas, na busca de pertencimento a determinado grupo, acarretando o aumento na utilização de TIC em contextos de trabalho e lazer.

Seguindo a mesma linha de pensamento, Han diz que as divisões entre ambientes de trabalho, lazer e descanso foram suprimidas com a nova realidade digital. Isto considerando que o aparato digital se tornou o próprio "trabalho móvel", resultando num sistema em que as pessoas não mais podem "escapar do trabalho", através de um fenômeno intitulado pelo autor de "coação da comunicação"[48].

Para evidenciar a dependência das TIC, objetiva-se neste capítulo apresentar temas diretamente influenciados por tecnologias em uma "nova" estrutura social, as quais, como consequência, podem ser negativamente impactadas com eventos de tecnologia.

Para tanto, foca-se principalmente em invasões na modalidade *ransomware* – conforme o recorte da pesquisa, assim como na falha ou interrupção de tais tecnologias. Demais incidentes serão apenas classificados.

Cabe dizer que as TICs são definidas por um conglomerado de tecnologias

---

[46] *Ibid*.
[47] Han entende por "massas" toda a movimentação social para pertencer a um meio/núcleo digital. *Cf.* HAN, Byung-chul. **NO ENXAME**: Perspectivas do Digital. Trad. Lucas Machado. Petrópolis, Rio de Janeiro: Editora Vozes, 2018.
[48] *Ibid.*, p. 65.

capazes de produzir, acessar, transmitir informações e comunicados entre pessoas e sistemas, independente de distâncias geográficas[49]. A título exemplificativo, comunicações à distância, através de mensagens, *e-mails* ou reuniões *online* são fatores presentes no desenvolvimento social, gerando ambientes colaborativos, negociais e de ensino. Diante da mudança e evolução das metodologias de comunicação, há dependência de tais recursos para a manutenção de ações já solidificadas no mercado.

Quanto ao ambiente laboral e educacional, cita-se a obra organizada por Antônio Carlos Efing e Cinthia Obladen de Almendra Freitas, conforme os autores, a "valorização monetária do conhecimento, sua capacidade de propagação, e relativização espacial e temporal" são características de uma sociedade da informação, fatores estes viabilizadores de uma evolução tecnológica[50]. Entende-se que a educação e o trabalho são dependentes de recursos tecnológicos em razão da utilização de equipamentos computacionais para a realização de atividades básicas, como comunicação, apresentações, pesquisas e gestão de rotinas empresariais.

No cenário fabril não é destoante, considerando o uso de maquinários para operação, produção e distribuição de bens, materiais, serviços, a presença de técnicas de *machine learning*[51] e o uso de redes de tecnologia operacional[52] (Redes OT) em rotinas industriais, objetivando agilidade, confiança e segurança em seus processos.

Há uma interessante percepção trazida por Han[53], que expressa o fenômeno do trabalho acelerado na sociedade mesmo que não mais dependente das máquinas da era industrial, mas por conta da modalidade de exploração do trabalho na fase digital. Presente em virtude da mobilidade e viabilidade da transformação de qualquer local ou aparato eletrônico como um "local de trabalho", e, como

---

[49] OLIVEIRA, Fátima Bayma de. **Tecnologia da Informação e da Comunicação**: desafios e propostas estratégicas para o desenvolvimento dos negócios. 1. ed. São Paulo: Editora Pearson Prentice Hall, 2006. p. 146.

[50] EFING, Antônio Carlos. FREITAS, Cinthia Obladen de Almendra. **Direito e Questões Tecnológicas**: aplicados no desenvolvimento social. Vol. 2. Curitiba: Juruá, 2012. p. 109.

[51] Machine Learning é o meio empregado para o aprendizado da máquina, visando suas diversas utilizações. Estima-se que, entre 2013 e 2017, mais de 200 bilhões de libras esterlinas circularam em função da *big data. Cf.* INFORMATION COMMISSIONER'S OFFICE (ICO). **Big data, artificial intelligence, Machine Learning and data protection**.

[52] É o uso de recursos tecnológicos, como *hardwares* e *softwares*, inclusive de inteligência artificial, para controlar equipamentos industriais. *Cf.* RAJAMÃKI, Ari. **Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center**. Master's thesis (Master's Degree) – Programme in Information Technology, Cyber Security, 2021.

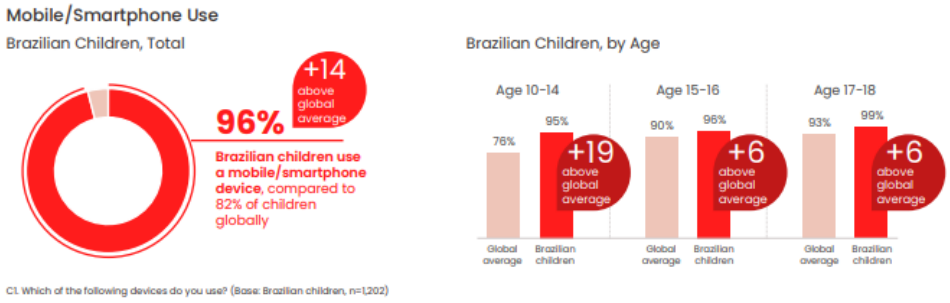
[53] HAN, *op. cit.*, p. 64 e 65.

consequência, tornando todo o tempo como um tempo apto ao labor. Isso ocorre por conta da quebra das barreiras em relação à existência de um local de trabalho separado de locais de descanso, como as casas.

No que tange ao entretenimento, não há de se olvidar sobre a presença das mídias sociais, equipamentos celulares, televisores, computadores, *tablets* e livros digitais, disponíveis em eletrônicos como o *kindle*, produto comercializado pela empresa *Amazon*, que objetiva a leitura "confortável" de livros digitais, prometendo a experiência similar a leitura de um material físico[54].

Um dos públicos que mais consome vias de entretenimento digitais, ou seja, através de plataformas, são os públicos de crianças e adolescentes. Em pesquisa realizada pela Mcafee[55], estima-se que 96% das crianças brasileiras usam algum dispositivo móvel em suas rotinas.

Figura 1 – Dados sobre uso de equipamentos móveis por crianças e adolescentes no Brasil



Fonte: MCAFEE, 2022.

No cenário da saúde, existe o fator bem-estar e a saúde dos indivíduos na sociedade tecnológica, bem como das próprias instituições que prestam serviços ao ramo e as respectivas autoridades do governo em atuação de tutela de direitos e garantias fundamentais atrelados.

Quanto ao bem-estar e à saúde, existem pesquisas recentes[56][57] indicando que a dependência da tecnologia acarreta prejuízos ao desenvolvimento cerebral de crianças e adolescentes, gera o afastamento das relações afetivas familiares,

[54] PORTO, Walter. Venda de ebooks salta 83% em 2020 e revela força dos livros digitais na pandemia. **Folha de São Paulo**, 1 jul. 2021.
[55] MCAFEE. **Life Behind the screens of Parents, Tweens and Teens**, 2022.
[56] MARQUES, Christopher da Costa; SOUZA, Weilan Carvalho; SOUZA, Julio Cesar Pinto de. A dependência da tecnologia na saúde mental dos adolescentes / The dependence of technology in the mental health of adolescents. **Brazilian Journal of Health Review**, v. 4, n. 5, 2021. p. 23082-23083.
[57] NEUMANN, Débora Martins Consteila; MISSEL, Rafaela Jarros. Família Digital: A Influência da Tecnologia nas Relações Entre Pais e Filhos Adolescentes. **Pensando Famílias**, v. 23, n. 2, 2019.

motivado pelo isolamento social, aumento de níveis de estresse e ansiedade pela falha ou impossibilidade de uso de *internet* em um curto período.

Sobre as entidades governamentais e empresárias do ramo da saúde, é inegável que os ambientes hospitalares são altamente tecnológicos, pois demandam equipamentos de análise, monitoramento e tratamento para a realização de cuidado clínico adequado. Assim sendo, pode-se descrever a dependência da integridade dos dispositivos, tornando relevantes medidas de contenção de danos causados por ataques, que podem ensejar situações de crise[58].

No que diz respeito à mobilidade, tem-se o uso de aplicativos para viagens com motoristas independentes e autônomos, como o aplicativo *Uber*, que facilitou a rotina de seus usuários, mas, ao mesmo tempo, gerou dependência, sobretudo dos motoristas que tiram sua renda e sobrevivência através do trabalho com esses aplicativos[59]. Para além desses, há a dependência daqueles que auxiliam ao aspecto geográfico, como o GPS, em funcionamento a partir do *Google maps* e o *Waze*, que direcionam a locomoção de pessoas aos seus destinos, mas também tendem a gerar dependência[60].

À temática do consumo e dependência tecnológica, em uma breve exposição, reúne-se a discussão sobre a nova modalidade de consumo. Conforme abordado por Bauman[61], voltada aos interesses emocionais passageiros, que acarretam um consumo excessivo, e, para atender tal demanda, há um significativo aumento no lançamento de novos produtos para estimular compradores.

Aos aspectos de privacidade e segurança de informações pessoais, Dânton Oliveira traz como problemática o fato de a *big data*, componente essencial em tempos de *data driven economy*[62], assim como as tecnologias da comunicação e informação, gerar riscos à privacidade e proteção de dados pessoais, considerando

---

[58] Nesse sentido, cita-se o caso de ciberataque ao hospital em Idaho (EUA), que teve suas operações impactadas negativamente após a ocorrência de incidente de ataque. *Cf.* LYNGAAS, Sean. Ciberataque força hospital dos EUA a enviar ambulâncias para outros lugares. **CNN Brasil**, 1 jun. 2023.

[59] GUIMARÃES, Fernanda. Cerca de 11,4 milhões de brasileiros dependem de aplicativos para ter uma renda. **CNN Brasil**, 12 abr. 2021.

[60] KLEINA, Nilton. Erro no waze deixa trânsito de São Paulo (ainda mais) congestionado). **Tecmundo**, 25 out. 2017.

[61] BAUMAN, *op. cit.*, p. 21.

[62] CIURIAK, Dan. The Economics of Data: Implications for the Data-Driven Economy. Chapter 2. *In*: "Data Governance in the Digital Age" Centre for International Governance Innovation, **SSRN**, 2018.

seus respectivos usos como novos fatores de sustentação do sistema capitalista[63], gerando, também, dependência operacional, econômica e regulatória pelo mercado.

Junto a isso, entende Oliveira[64] que exercícios de ponderação entre a *big data* e direitos e garantias fundamentais são essenciais, considerando a relevância protetiva de direitos fundamentais, isso somado ao fato de que a inovação tecnológica hoje é dependente de coleta e processamento de dados em estruturas de *big data.*

Por fim, no que diz respeito à dependência, tem-se a existência de instituições empresárias e a economia de forma propriamente dita. Nesse diapasão, Mariana Mazzucato[65] expressa de forma cirúrgica um fator quase que imperceptível no dia a dia, qual seja, a criação e extração de valores digitais como fator competitivo e, em certas vezes, até monopolista por parte das *big techs*. Similar ao que diz Oliveira[66], há um massivo uso de dados para fins econômicos, com isso, tais empresas de serviços digitais utilizam de suas inovações e "comercialização" de dados para gerar demandas ara outras instituições, assim como o possível controle sobre o mercado e a economia.

Para finalizar, tem-se os conceitos "fantasmas digitais" e "cansaço da informação", cunhado por Han[67]. O primeiro deles trata da "comunicação automática das coisas", não dependendo de ações e intervenções humanas, com capacidade de influenciar cenários econômicos, políticos e sociais, como, por exemplo, em casos de guerra.

O "cansaço da informação", como o próprio termo indica, ocorre diante da densidade de informações recebidas pelo ser humano, gerando uma espécie de "definhamento do pensamento", tornando a sociedade incapaz de "reduzir coisas ao essencial", principalmente no campo do pensamento analítico e reflexivo sobre as

---

[63] OLIVEIRA, Dânton Zanetti de. Big Data e Dualidade: Uma problematização entre Tecnologia e a Lei Geral de Proteção de Dados Pessoais Brasileira. *In*: FREITAS, Cinthia Obladen de Almendra; OLIVEIRA, Dânton Zanetti de (Org.). **Sociedade informacional e a Lei Geral de Proteção de Dados Pessoais**: diálogos contemporâneos entre direito e tecnologia. Rio de Janeiro: Lumen Juris, 2022a. p. 18-19.

[64] OLIVEIRA, Dânton Zanetti de. **Big Data e a Lei Geral de Proteção de Dados Pessoais**: Diálogos necessários em prol da livre iniciativa. Rio de Janeiro: Lumen Juris, 2022b. p. 167-168.

[65] MAZZUCATO, Mariana. **O valor de tudo**: Produção e Apropriação na economia global. Trad. Camilo Adorno e Odorico Leal. 1. ed. São Paulo: Portfólio-Penguin, 2020. p. 274-275.

[66] OLIVEIRA, *op. Cit 2022b.*

[67] HAN, *op. cit.*, p. 97-100.

coisas[68]. A partir das reflexões de Han, percebe-se a existência de diferentes camadas envolvendo a influência das TICs sobre a sociedade, somando-se em sinergia aos demais conceitos trazidos pelos demais autores citados na pesquisa. Portanto, em síntese, entende-se que a evolução e inovação tecnológica são fatores influenciadores da atividade humana em todas as camadas de sua vida, ensejando possíveis atuações “positivas ou extremamente negativas”[69].

Como dito alhures, as tecnologias fazem parte das rotinas dos empregadores e seus respectivos trabalhadores, desde o ambiente produtivo até a proteção da propriedade da empresa[70].

Considerando os níveis de dependência e necessidade expostos, vale considerar como relevantes quaisquer medidas que visam o tratamento preventivo de potenciais riscos atrelados aos recursos tecnológicos e seus respectivos usos. Com a dependência, impactos oriundos de crises envolvendo tecnologias colocam em xeque a integridade financeira, reputacional e operacional de uma entidade empresarial, ensejando indicativos de impacto à continuidade dos negócios empresariais e à sociedade na qual a empresa está inserida.

Para tanto, é necessário entender as tipologias de incidentes ou eventos de segurança da informação, assim como a modalidade de atuação para, no último tópico, demonstrar a relevância de se ter o fator da cibersegurança como novo ponto de atenção por administradores como requisito de atendimento do dever de diligência, considerando a nova realidade de uma sociedade informacional e tecnológica.

2.2 TIPOS DE INCIDENTES DE CIBERSEGURANÇA E MODUS OPERANDI CLÁSSICO DOS ATAQUES

Considerando a característica multidisciplinar desta pesquisa, coube apresentar definições basilares sobre incidentes de tecnologia, os quais trarão norte e possibilitarão a compreensão do leitor sobre as diversas camadas de reflexão, constatação e provocação presentes na problemática deste trabalho.

---

[68] HAN, *op. cit.*, p.105.
[69] EFING, *op. cit.*, p. 109.
[70] *Ibid.*, p. 117.

Adiante, compreende-se ciberespaço como o mecanismo não visível e materialmente intangível, responsável por interligar pessoas, empresas, entidades governamentais com agilidade e rapidez, independente da região, reduzindo distâncias físicas, por meio de conexões em rede[7172]. Esse recurso de conexão viabiliza interações sociais e comerciais diante de longas distâncias e em curtos períodos, interpretadas no tópico anterior como componentes de uma rede, em um paradigma *everyware*, modo que se tornou um dos principais meios de comunicação e realização de atividades empresariais entre instituições. Isso se fortalece pelo movimento econômico adotado no tratamento e utilização de dados, visto como um novo "insumo"[73], viabilizando a produção e o comércio. Também utilizado em larga escala para estimular a competitividade[74] entre organizações[75].

Como descrito no tópico anterior, o uso de recursos tecnológicos, sobretudo instrumentos de comunicação e leitura de dados, passaram a compor o eixo de inteligência estratégica das organizações. À medida que o uso do ciberespaço aumenta, cresce a necessidade de reconhecer o surgimento de novas fontes de risco, possivelmente oriundas de uma má utilização do recurso, obsolescência da tecnologia, implementação inadequada ou incorreta, ou, ainda, sendo este o foco da abordagem, por ataques realizados por grupos especializados na modalidade, classificados como cibercriminosos[76].

Tais intercorrências sobre recursos de tecnologia e segurança da informação são percebidos no meio técnico como incidentes de tecnologia e segurança da informação[77], ocasionados por falhas de implantação, condições físicas de

---

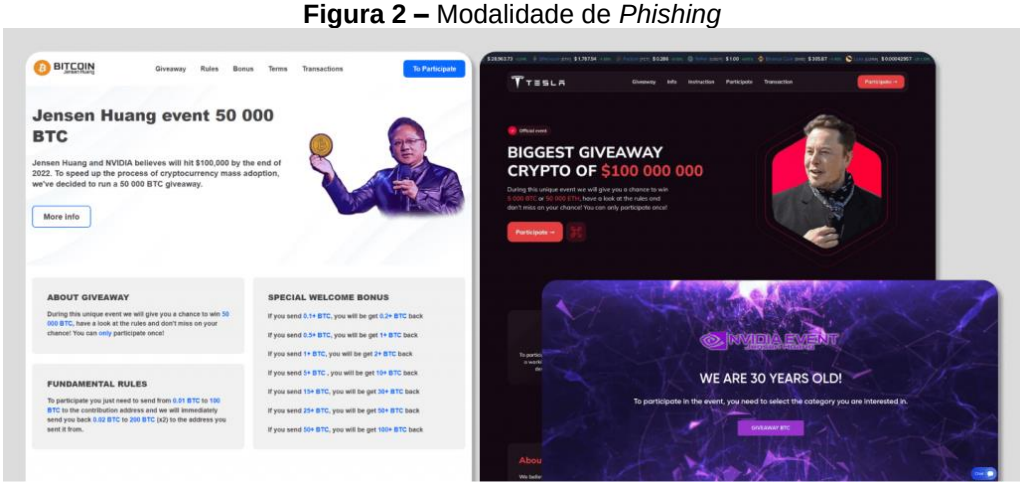
[71] SILVA, Michel Bernardo Fernandes. **Cibersegurança**: uma visão panorâmica sobre a segurança da informação na internet. 1. ed. São Paulo: Freitas Bastos, 2023. p. 17.
[72] Ciberespaço pode ser definido como o ambiente onde as comunicações são realizadas por meio de redes de computadores. *Cf. Ibid.*, p. 20.
[73] CIURIAK, *op. cit.*
[74] SCHWEITZER, Heike; WELKER, Robert. Competition policy for the digital era. **The Antitrust Chronicle**, v. 3. 2019, p. 16-24.
[75] Sobre a definição de data driven economy, *Cf.* CIURIAK, *op. cit.*
[76] O cibercrime é compreendido como o delito praticado no meio cibernético, ou seja, que adota práticas ilícitas por meio do uso de um computador na rede de tecnologia de informações e comunicações (TICs), "fenómeno da criminalidade informática estão, sem dúvida, condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime". *Cf.* SIMAS, Diana Viveiros de. **O cibercrime**. 2014. Dissertação (Mestrado em Ciências Jurídico Forenses) – Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.
[77] Entende-se por incidente de tecnologia a ocorrência de interrupção não planejada de um serviço de T.I., na redução da qualidade do serviço ou a falha em determinado componente. Durante o tratamento, há o gerenciamento do incidente e o gerenciamento de problemas. O primeiro refere-se

hardwares, bem como por invasões realizadas por agentes especializados em quebras e invasões a sistemas, comumente reunidos em organizações cibercriminosas[78].

A partir de tais concepções, relevantes para o entendimento do objeto da pesquisa, é imperioso abordar as tipologias de incidentes, aqui enfocadas em ataques de terceiros, em especial, praticados pela modalidade de *ransomware.*

A primeira categoria refere-se aos ataques de *phishing*[79], considerados como uma das técnicas mais utilizadas em fraudes no ano de 2022[80]. O *phishing*[81] pode ser traduzido como “pescaria”, consiste numa metodologia na qual a vítima é atraída por um conteúdo atrativo, geralmente com promessas de ganhos e aparentemente legítimo, cujo clique leva para um *site* falso ou que realiza execução automática de arquivos de furto de dados ou acesso não autorizado a informações e aplicações privilegiadas, como contas nas redes sociais ou aplicativos bancários.

Figura 2 – Modalidade de *Phishing*



Fonte: Kapersky, 2023.

---

ao restauro da operação, garantindo melhor disponibilidade dos serviços. Já o gerenciamento de problemas objetiva identificar e remover erros, buscando a causa raiz, almejando a estabilidade e a segurança dos serviços. *Cf.* COBIT, Aligning. **4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit**. IT Governance Institute, 2008; CESTARI FILHO, Felício. **ITIL v3 Fundamentos**. Rio de Janeiro: RNP/ESR, 2011.

[78] “O carácter transfronteiriço destas infracções entra em conflito com a territorialidade das autoridades nacionais competentes para a aplicação da lei. As legislações nacionais estão confinadas a um território delimitado, pelo que se torna cada vez mais importante que exista legislação internacional.”. *Cf.* SIMAS, *op. cit.*

[79] PINHEIRO, Patricia Peck. LOTUFO, Larissa. Proteção de Dados Pessoais. *In*: PINHEIRO, Patricia Peck. **Segurança Digital** – Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2020. p. 15.

[80] Em relatório emitido pela Kapersky, o Brasil, em 2022, foi o 8º país com mais usuários vítimas de ataques por *phishings*. *Cf.* DEDENOK, Roman; KOVTUN, Andrey; KULIKOVA, Tatiana; SHIMKO, Irina; SVISTUNOVA, Olga. Spam e Phishing Report. Kapersky. **Securelist**, 16 fev. 2023.

[81] PINHEIRO, *op. cit.*, p. 15.

O *modus operandi* clássico dessa modalidade de invasão consiste no envio de *e-mails* ou mensagens de SMS mascaradas e de aparência idônea. Sendo uma técnica de engenharia social, induz a vítima a acessá-lo por meio de um aspecto visual atrativo ou que causa espanto, como a promessa de ganhos fáceis ou, ainda, supostas notificações de autoridades governamentais e bancárias sobre boletos, dívidas e aparentes não-conformidades[82].

Há também a modalidade de ataque por meio de *malware*[83], referindo-se um *software* malicioso, comumente conhecido como vírus ou até mesmo *ransomware*, cujo objetivo é infectar sistemas de computadores, dispositivos móveis e redes TI[84] e OT[85]. O objetivo desse modo de ataque, assim como sua modalidade comum e crescente de atuação consiste no acesso não autorizado a informações internas, dados pessoais e consequente bloqueio ou "furto" de dados com a finalidade de extorsão, com a posterior solicitação de pagamentos de resgate em criptomoedas.

Durante os ataques, é possível que os invasores realizem ações[86] de: a. gravação de dados e espelhamento de informações exibidas em telas; b. modificação de dados, sobretudo relacionados a envio de dados para pagamentos; c. invasão de sistemas de captação de áudio e vídeos, para extorsão de possíveis vítimas com intimidade e privacidade expostos; d. destruição de dados; e. captura do modo de tráfego de dados em redes; f. acesso a credenciais, de modo amplo; g. realização de fraudes por intermédio de sistemas representantes de empresas; h. paralisação de operações e sistemas significativos para o bom andamento da empresa, objetivando resgates em criptomoedas; i. furto de criptomoedas; j. ações de guerra cibernética em resposta a ataques 'físicos"; k. utilização de máquinas e sistemas para disseminação do *ransomware*/*malware*.

Para a contenção dessa modalidade de ataque, há uma série de medidas de proteção que envolvem desde o processo de aculturamento sobre pessoas que

---

[82] KIM, David. SOLOMON, Michael. **Fundamentos de Segurança de Sistemas de Informação**. 1. ed. Editora: LTC, 2014.
[83] PINHEIRO, *op. cit.*, p. 17.
[84] Sistemas de tecnologia da informação. *Cf.* FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. **Implantando a governança de TI**. 2. ed. Porto Alegre: Brasport, 2008.
[85] Sistemas de tecnologia operacional. *Cf.* STALLINGS, William. **Criptografia e Segurança de Redes**: Princípios e Práticas. 6. ed. São Paulo: Editora Pearson, 2014. p. 6-19; 389-395.
[86] GRIMES, Roger A. **Manual de proteção contra ransomware**: como criar um plano de segurança cibernética. São Paulo: Grupo A, 2022.

utilizam equipamentos informáticos e tecnológicos, em sentido amplo, até a adoção de técnicas de proteção de redes, como metodologias de criptografia de ponta a ponta[87], que percorrem toda a estrutura da rede e a blinda de espaços de acesso.

Sobre o *ransomware*[88], foco desta pesquisa, trata-se de categoria correspondente ao uso de códigos maliciosos para invadir e posteriormente exigir o pagamento de resgates, para que haja a liberação dos dados e informações do atacado[89]. Destaca-se que o *ransomware* não pode ser entendido pela prática de usufruir dos dados, mas como o bloqueio ao acesso, especialmente com o intuito de gerar impactos negativos e urgentes pela dependência desses dados e sistemas envolvidos[90]. Inclusive, práticas iniciais apenas bloqueavam a tela dos usuários, fazendo-os crer que haviam cometido alguma falha culposa, assim devendo repará-lo mediante pagamento[91].

Em um cenário mais avançado e recente, há a utilização de algoritmos de criptografia para realizar o bloqueio dos dados e solicitar o resgate, bastando, para tanto, que o usuário apenas acesse esse algoritmo malicioso como, por exemplo, *e-mails* com arquivos contaminados.

---

[87] BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip; SHORT, Donald. **Cybersecurity Essentials**. 1st ed. Wiley: Sybex. 2018.

[88] GRIMES, *op. cit.*

[89] KIM; SOLOMON, *op. cit.*, p. 30-35.

[90] RICHARDSON, Ronny; NORTH, Max. **Ransomware**: Evolution, Mitigation and Prevention. International Management Review, 2017. p. 2.

[91] A doutrina americana entende que o primeiro ataque de sequestro ocorreu em 1989, mas reconhecem que somente a partir de 2006 os ataques passaram a tomar maior proporção de sequestro de sistemas ao invés de informações. Neste ponto, Richardson e North (2017) destacam um breve histórico, que colaciono para curiosidade: “1989. The first ransomware virus, called the AIDS Trojan (and also known as the PC Cyborg), was created by Joseph L. Popp. Popp was a Harvard-trained evolutionary biologist. It was distributed by floppy disk at the World Health Organization’s International Aids conference. It used simple symmetric cryptography to encrypt file names and tools were soon available to decrypt them (Sjouwerman, 2015b). 2005. The first modern ransomware was Trojan.Gpcoder, also known as GP Code and GPCoder. It was released in May 2005 and initially used a custom symmetric encryption technique that was weak and easily overcome. Its authors continued to improve the malware (Savage, Coogan, & Lau, 2015). Trojan.Gpcoder was spread via a spam email attachment claiming to be a job application (Sjouwerman, 2015b). The bulk of the early ransomware was developed in Russia by Russian organized criminals. It was mostly aimed at Russian victims and those in neighboring countries, like Belarus, Ukraine, and Kazakhstan (Cawley, 2016). 2006. In early 2006, ransomware was starting to gain traction, and more attackers started to try their hand. Trojan.Cryzip appeared in March 2006. It copied data files to password-protected archive files and deleted the originals. The code for the malware included the password, so recovering it was straightforward. Trojan.Archiveus also came on the scene in 2006. It operated much like Trojan.Cryzip, except instead of asking for a ransom, it required victims to buy medication from specific online pharmacies and submit the order ID to get the password (Savage, Coogan, & Lau, 2015)”. *Cf. Ibid.*, p. 2.

Há dois modelos de ataque *ransomware*, o primeiro deles consiste no bloqueio da tela dos usuários, ataque esse denominado como "*lockscreen*"[92], impedindo o acesso ao equipamento. O outro modelo, como mencionado anteriormente, utiliza a criptografia para a realização dos ataques, criptografando os dados e informações dos equipamentos informáticos, modalidade nomeada como "*cryptolocker*"[93].

Em níveis de recuperação, a primeira modalidade possui menor índice de perda de informação, por consequência, o gerenciamento da crise é mais simples. Isso porque não há a criptografia dos dados, basta a limpeza do disco rígido da máquina para retirar o componente malicioso. Para os cibercriminosos, essa prática utiliza fatores de engenharia social como parte principal para a obtenção de vantagem, persuadindo e utilizando técnicas para comover o usuário e induzi-lo a pagar resgate.

Já a modalidade com criptografia domina todo o ambiente, impedindo o acesso a arquivos, sistemas e até comandos de maquinários. Utiliza da modalidade através de alterações na estrutura de documentos e arquivos, demandando da utilização de uma chave[94], a qual se mantém em posse dos invasores para realizar o desbloqueio. Há a opção de restauração dos arquivos e sistemas aos seus estados originários, situação de rara escolha, dada a quantidade de dados tratados em rotinas empresariais e, em alguns casos, necessidade de integridade dos dados e seus históricos para operações e atendimento de requisitos legais.

Sobre as formas de propagação, são utilizados *e-mails* com informações falsas, geralmente atrativas aos olhos do usuário que, em um momento de emoção, acessa ao arquivo, de modo que o ataque facilmente contamina toda a rede a qual está interligado.

---

[92] É uma modalidade de ataque que bloqueia a tela inicial e demais acessos. *Cf.* NATIONAL CYBER SECURITY CENTRE (NCSC), **Mitigating malware and ransomware attacks**, 13 feb. 2020.

[93] A modalidade *cryptolocker* realiza a criptografia de todos os sistemas, impedindo acesso aos usuários. *Cf. Ibid.*

[94] Algumas importantes terminologias sobre criptografia: "O termo 'criptografia' provém das palavras gregas kryptos (oculto, secreto) e graphos (escrever). Assim, a criptografia foi criada para codificar informações, de forma que somente as pessoas autorizadas pudessem ter acesso ao seu conteúdo. Conceitualmente, a criptografia faz parte de um escopo mais amplo de conhecimento. Criptografia: técnicas para codificar/decodificar informações, ocultando seu conteúdo de pessoas não autorizadas; Criptanálise: conjunto de técnicas usadas para "quebrar" uma criptografia, expondo a informação ocultada por ela; Criptologia: área geral, englobando criptografia e criptanálise. Criptossistema: conjunto de algoritmos/mecanismos para realizar um tipo específico de criptografia". *Cf.* MAZIERO, Carlos. **Sistemas Operacionais**: Conceitos e Mecanismos. Curitiba: Editora UFPR, 2019. p. 349-350. Ainda neste tema, recomenda-se a leitura de *Cf.* STALLINGS, *op. cit*.

A título de exemplo, utilizam órgãos governamentais, bancos ou temas que simulam exposição da intimidade do usuário. A partir do momento que o usuário clica no arquivo indicado no *e-mail*, inicia-se o *download* do arquivo malicioso, que bloqueia os acessos a dados, arquivos e sistemas.

Há também a modalidade de *download* de arquivo de *software* pirata, na qual o usuário realiza *download* de *software* falso em uma rede *peer-to-peer* (P2P)[95], através da oferta de *software* gratuito, site falso (muito similar ao real) ou metodologias de quebra de licenças. Nesse caso, geralmente o sistema solicita a desativação de proteção antivírus para habilitar o *download* do software, é através dessa prática que se contamina toda a rede envolvida, ocorrendo bloqueio de sistemas e dados de todo o grupo.

Vale a pensar citar que havia um modelo de *ransomware* denominado *WannaCryptor*[96], que explorava vulnerabilidades do protocolo SMB, utilizado em arquivos compartilhados, que executava o código malicioso remotamente, realizando cópias em todas as máquinas que estivessem com o mesmo fator de vulnerabilidade em uma mesma rede.

Ao todo, ao sofrer um ataque *ransomware*, há impactos negativos diante da perda de dados operacionais e pessoais, os quais – no campo dos dados pessoais – deverão ser indenizados e, nesse sentido, há perda financeira por parte da instituição empresarial.

Casos em que há recursos de propriedade intelectual, como marcas, patentes, fórmulas ou demais pesquisas e composições objeto da atuação laboral, há riscos de impacto parcial ao negócio, considerando a dificuldade de recomposição. Se a entidade empresarial depende somente de servidores em nuvem para todas as rotinas operacionais, há o risco de interrupção dos negócios por impacto operacional. Nesse sentido, é necessário um plano de continuidade e de recuperação de crises, possibilitando o exercício *offline* de algumas atividades.

---

[95] É um modelo de arquitetura de rede, em que cada ponto funciona como cliente ou servidores, permitindo compartilhamento de informações entre todas as pontas da rede. *Cf.* SCHOLLMEIER, Rüdiger. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architetures and Applications. Conference. **IEEE Internet Computing**, 2022.

[96] Essa é uma modalidade de ataque que explora vulnerabilidades de servidores *Windows*, comprometendo sua estrutura. Para mais informações sobre a modalidade de ataque *Cf.* NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATIONS CENTR. **What tis wannacry/Wannacryptor?**.

Tem-se também o risco reputacional e de imagem quando há exposição e mau tratamento do caso. Isso porque, com o bloqueio de sistemas, é possível que ocorra um impacto na produção, comercialização ou prestação de serviços, o que demanda tratamento assertivo junto aos clientes e demais interessados nas rotinas, como fornecedores sobre o pagamento de valores devidos no tempo hábil.

A depender do ramo da empresa, o impacto de sofrer um ataque *ransomware* pode trazer a perda da confiança por parte dos clientes, abrindo margem para cancelamento de pedidos ou contas, por exemplo.

Por fim, a companhia vítima do ataque e seus responsáveis, como administradores, podem ser responsabilizados em razão das ações tomadas (ou não tomadas) para evitar o vazamento e exposição de dados pessoais dos públicos envolvidos na empresa, como clientes, colaboradores e sócios de fornecedores e parceiros. Tema que será debatido no próximo item desta pesquisa.

Ao todo, entendendo o *modus operandi* dos cibercriminosos e de atuação do ransomware, é possível estabelecer medidas preventivas e de gerenciamento de crises[97] no ambiente empresarial.

Uma das primeiras vias de mitigação de riscos de *ransomware* consiste no treinamento[98] de colaboradores e terceiros que possuam acesso aos sistemas, objetivando demonstrar os meios empregados para praticar o cibercrime, evitando ou reduzindo a probabilidade de acesso indevido (por desconhecimento) a arquivos maliciosos.

Ocorre também o uso de *softwares* de segurança[99], como de bloqueio de arquivos maliciosos, bloqueio ao acesso a sistemas ou *sites* falsos ou de detecção precoce de movimentações atípicas nos sistemas. Para que haja uma rápida reabilitação dos dados e sistemas é importante a presença de processos[100] e sistemas para a realização de *backups* contínuos[101] de toda base relevante às

---

[97] Recomenda-se o aprofundamento através da letura da seguinte obra *Cf.* REZENDE, Denis Acides. **Planejamento de sistemas de informação e informática**. 3 ed. São Paulo: Atlas, 2008. Capítulo 2.
[98] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISSO/IEC 27002**: Tecnologia da Informação, técnicas de segurança e código de prática para controles de segurança da informação. Rio de janeiro, 2013.
[99] **ABNT NBR – ISO/IEC 27002**, *Ibid.*; ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27005**: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio e janeiro, 2011.
[100] LAURINDO, Fernando José Barbin. **Gestão da tecnologia da informação**. São Paulo: Atlas, 2008.
[101] **ABNT NBR – ISO/IEC 27002**, *op. cit.*; **ABNT NBR – ISO/IEC 27005**, *op. cit*.

operações e sistemas, evitando sua paralisação ou perda/roubo de dados, sobretudo os pessoais.

Em ambientes empresariais e industriais[102], existem técnicas de proteção das redes interligadas, como exemplo, monitoramentos que bloqueiam ou desvinculam um equipamento interligado a partir do momento que identificam que ele foi danificado ou invadido. Por outro lado, o pagamento do resgate não é recomendável, isso em razão do risco de os cibercriminosos não cumprirem com a promessa e, ainda, ser uma empresa financiadora desta categoria criminosa, podendo ensejar no aumento de ataques ou aprimoramento do *modus operandi*.

Seguindo essa percepção, o Grupo de Ação Financeira Internacional GAFI[103] recentemente publicou um estudo sobre como o financiamento aos ataques por *ransomware* também podem financiar o terrorismo, a proliferação de armas de destruição em massa, principalmente incentivando práticas de lavagem de capitais[104].

Partindo dessa publicação do GAFI, percebe-se que não são raros os encontros entre os cibercriminosos com demais grupos de atuação em crimes. É possível exprimir que os ataques podem, inclusive, surgir através da atuação de grupos terroristas que, através dos resgates, financiam ataques ou a aquisição de armas de destruição em massa.

Seguindo essa tendência, não é forçoso frisar a reprovabilidade do pagamento do resgate e a possível tendência à responsabilização pelo financiamento do terrorismo ou facilitação à lavagem de dinheiro por meio do pagamento de resgates.

As situações elencadas aqui apontam que diversos pontos estão interligados, decorrentes da dependência tecnológica. Não é fato, mas realidade: a sociedade depende de tecnologia para existir e os indivíduos para serem reconhecidos como um ser no meio social por meio dela. Essa característica, inclusive, corrobora para o surgimento de novas práticas, as quais se utilizam de técnicas simples de ataque, ou

---

[102] MACHADO, Felipe Nery Rodrigues. **Segurança da Informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

[103] GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL. **Countering ransomware financing**. GAFI Report. 14 mar. 2023.

[104] Lavagem de capitais, de acordo com a Lei de Lavagem de Dinheiro, consiste no processo de "Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal". *Cf.* BRASIL. **Lei 9.613, de 3 de março de 1988. Lei de Lavagem de Dinheiro, 1998**.

cada vez mais sofisticadas, como crimes utilizando mecanismos de inteligência artificial ou em ambiente metaverso.

Um exemplo disso pode ser visualizado na prática por uso do *software jackware*, uma versão mais sofisticada do *ransomware,* cujo objetivo consiste em meramente controlar um dispositivo do qual o usuário é dependente e solicitar resgate para liberá-lo, trabalhando o aspecto emocional do usuário, portanto.

No geral, medidas de segurança da informação[105], ou, especificamente, *cibersecurity*[106], constituem-se como um fator essencial para a prevenção, manutenção e perenidade das organizações, evidenciando, para tanto, um novo ponto relevante de atenção contínua dos administradores de uma sociedade, motivado pela quantidade de consequências inerentes à ocorrência de um ataque de *ransomware* mal gerenciado.

Para além dos impactos na seara operacional, financeira, de imagem e reputação, como destacado supra, há a possível responsabilização por falhas ao tratamento e proteção de dados pessoais. No Brasil, o cenário da proteção de dados pessoais tomou grande força legislativa quando da publicação da Emenda Constitucional 115, de 10 de fevereiro de 2022[107], que incluiu a proteção de dados pessoais no rol de direitos e garantias fundamentais, fator que evidencia a presença e significância do tema, tornando essencial para toda organização, e, em decorrência, a tomada de decisões e ações compatíveis com a atividade empresarial desenvolvida.

A mencionada emenda fixou a competência privativa da União para legislar sobre o tema de proteção e tratamento de dados pessoais. Reflete-se, que, diante disso, a ausência de mecanismos de proteção e de tratamento legal aos dados pessoais passa, portanto, a ser reprovável também pelo viés constitucional.

2.3 DIMENSÃO NORMATIVA DAS MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS E CIBERSEGURANÇA NO CONTEXTO DAS EMPRESAS

Um dos principais insumos da sociedade tecnológica consiste no tratamento

---

[105] SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Ed. Campus, 2003.
[106] STAMP, Mark. **Information Security**: Principles and Practice. Indianapolis, USA: Wiley Publishing, 2008.
[107] BRASIL. **Emenda Constitucional Nº 115, de 10 de fevereiro de 2022**.

de dados pessoais, almejando oferecer produtos ou serviços direcionados aos nichos pretendidos. Parte dos frutos de dados obtidos são oriundos de redes sociais, tais como *Facebook*, *TikTok*, *Instagram*, dentre outras plataformas comumente usadas. Isso porque os usuários acessam conteúdos de suas preferências, fornecendo seus dados e assinalando tendências de preferência para continuar acessando tais veículos.

Como muito bem explanado por Oliveira[108] “somando-se a isso, tem-se a existência de termos de uso da plataforma, os quais, contratualmente falando, indicam a legitimação do tratamento de dados pessoais por estas”, há medidas contratuais geralmente utilizadas diante dos usuários de redes sociais. No entanto, por ser um eixo que cresceu de forma desenfreada e com valor econômico agregado, há discussões sobre a existência de supressão de direitos dos usuários, considerando casos recentes em que se tomou o abuso sobre a utilização de dados pessoais, mesmo que houvesse o fornecimento e ciência sobre os termos de uso da plataforma[109].

Um desses casos remete à decisão proferida pela *European Data Protection Board* (EDPB) perante à Meta Inc[110], que considerou ilegal o tratamento de dados pessoais em atividades de publicidade comportamental. Aqui, o órgão entendeu que a utilização de termos e condições de uso da plataforma de forma genérica não constituiu base legal adequada, sendo devido, portanto, a coleta de consentimento expresso e inequívoco.

Através do relatório da decisão do EDPB, desde maio de 2018 a Meta incorreu práticas envolvendo o tratamento irregular[111] de dados pessoais, colocando como marco temporal o período de recebimento das primeiras reclamações e denúncias. Com a violação dos deveres legais estabelecidos no RGPD, o EDPB fixou multas contra a Meta em um valor pouco superior a €390 (trezentos e noventa) milhões de euros.

---

[108] OLIVEIRA, 2022, *op. cit.* p. 134. 2022b.

[109] Para aprofundamento ao tema, sugere-se a seguinte leitura *Cf.* OLIVEIRA, Ana Paula; ZANETTI DE OLIVEIRA, Dânton Hilário; LIMA, Flávio Santos; SAMPAIO, Themis Ortega. A Lei Geral de Proteção de Dados Brasileira na Prática Empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, v. 4, n. 1, 2019.

[110] EUROPEAN DATA PROTECTION BOARD. **DPC Inquiry Reference**: IN-18-5-6.

[111] Cabe mencionar que no direito brasileiro o vocábulo “tratamento irregular” remete a toda e qualquer operação envolvendo dados pessoais que não observa a legislação vigente e aplicável à empresa investigada, especialmente o disposto na Lei Geral de Proteção de Dados Pessoais, nos moldes do art. 44, da Lei Geral de Proteção de Dados.

Partindo do *case* brevemente apresentado no cenário internacional, cita-se a existência de um dos principais diretivos a respeito da temática, qual seja, a *General Data Protection Regulation*[112]. Normativo europeu, publicado em 2016 e implantado em 2018, que regula[113] o tratamento de dados pessoais e proíbe, extensivamente, ações lesivas à privacidade e proteção de dados de pessoas por ações abusivas a entidades, sejam públicas ou privadas.

No contexto das discussões envolvendo proteção de dados no Brasil, houve a publicação do Marco Civil da Internet em 2014[114], responsável por versar sobre questões concernentes ao uso da *internet* no país, considerado como um momento de importância ao desenvolvimento tecnológico no país, mas também da compreensão do referido tema.

É importante destacar a existência de princípios de proteção de dados já no dispositivo do marco civil da *internet*, os quais se encontram alocados em seus artigos 3º e 10º[115]. No entanto, foi entre 2010 e 2018 que o tema da proteção de dados pessoais foi discutido de forma específica no país, culminando na aprovação de uma normativa específica em 2018, sendo vigente em 2020.

A estrutura aprovada da LGPD[116] classifica princípios basilares, categorias de dados pessoais, as bases legais de tratamento e consequentes sanções aplicáveis por sua violação.

Como se vê através do caso inicialmente apresentado, das normativas europeias às brasileiras, junto com outras relacionadas à proteção de dados pessoais, como a *California Consumer Practices Act* (CCPA), empresas e entidades públicas tornaram-se obrigadas a estar em conformidade sobre o tratamento de dados pessoais. Assim sendo, os ajustes sobrevieram de processos internos das organizações, os quais trazem possíveis riscos de exposição de dados e ao tratamento irregular de dados.

Giovani Saavedra e Gabriel Borges[117] assinalam que, com os princípios protetivos no mundo *online*, haverá o impedimento sobre a criação de um poder

---

[112] EUROPEAN DATA PROTECTION BOARD, *op. cit.*
[113] O inteiro teor do RGPD encontra-se disponível no link: https://bit.ly/48sCeDG. Acesso em: 30 abr. 2023.
[114] BRASIL. **Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet, 2014**.
[115] BRASIL, *Ibid.*
[116] BRASIL. **Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, 2018**.
[117] SAAVEDRA, Giovanni Augusto; BORGES, Gabriel Oliveira de Aguiar. CONSTITUCIONALISMO DIGITAL BRASILEIRO. **Revista da AJURIS**, v. 49, n. 152, 2022. p. 174-175.

central que possa trazer riscos à autonomia dos usuários no momento da escolha sobre o que acessar ou, em cenários mais severos, na ameaça à oferta de produtos, aplicativos ou serviços em "paridade de condições"[118]. No mesmo artigo, os autores concluem pela vivência de um momento de constitucionalismo digital, considerando, por exemplo, os debates acerca das normas sobre o tema, como foi o caso do Marco Civil da Internet, que contou inclusive com ampla participação popular na discussão[119].

Para tanto, cotejando o contido na LGPD[120], há aplicabilidade em toda e qualquer operação de tratamento de dados em território nacional, cuja atividade tenha por objetivo a oferta e fornecimento de bens ou serviços, também casos em que haja a coleta dos dados pessoais em território nacional[121].

Em reflexo às movimentações após publicação da LGPD e evidenciando o cenário no Brasil, em julho de 2023 a Autoridade Nacional de Proteção de Dados (ANPD) aplicou a primeira sanção por descumprimento à norma. Naquele momento, a primeira sanção foi resultado de um processo administrativo instaurado em 2021, que verificou uma denúncia de oferta de listagem de contatos de aplicativos de mensagens de pessoas eleitoras residentes em Ubatuba (SP) durante as eleições de 2020.

A autoridade reconheceu a empresa divulgadora das listagens como controladora de dados pessoais, como a entidade que estava obtendo vantagem econômica sobre os dados tratados[122]. Assim, tratando dados pessoais de forma irregular. As irregularidades identificadas nesse caso foram geradas pelo não fornecimento de documentos, ausência de transparência e demais informações que comprovassem a regularidade ao tratamento, não respeitando o artigo 7º da LGPD que dispõe sobre bases legais de tratamento de dados[123].

---

[118] Aqui os autores realizam cotejo à obra de Guilherme Magalhães Martins, que aborda a neutralidade e proteção dos consumidores ante a restrições ao uso de internet fixa. *Cf.* MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed. São Paulo: Atlas. 2016.
[119] SAAVEDRA, *op. cit.*, p. 174-175.
[120] BRASIL. **Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, 2018**.
[121] BRASIL. *Ibid.*
[122] PRIMEIRA SANÇÃO por descumprimento da LGPD é publicada pela ANPD. **Trench Rossi Watanabe**, 14 jul. 2023.
[123] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - Mediante o fornecimento de consentimento pelo titular;
II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;

Quanto às sanções aplicadas, a ANPD aplicou uma advertência e duas multas simples, no valor total de R$14.400, considerando a entidade empresarial como de micro porte e o limite de dois por cento do faturamento da empresa na dosimetria[124].

Considerando a densidade e relevância empregada ao tema, em fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115/2022[125], que acrescentou a proteção de dados pessoais no rol de direitos e garantias fundamentais dos cidadãos. O mesmo texto legal acrescentou competência privativa da união para legislar sobre ações preventivas, protetivas e de tratamento de dados pessoais, dada a relevância do tema.

Nas palavras de Waldemar Gonçalves, tal medida corrobora para que "seja dada maior segurança jurídica ao país na aplicação da Lei Geral do Proteção de Dados Pessoais, atraindo ainda mais investimentos internacionais para o Brasil"[126].

Diante do cenário abordado, há necessários investimentos em pessoal e capital para que as companhias, sobretudo as de atuação digital, estejam adequadas para continuar operando e mantendo uma reputação positiva junto aos titulares de dados pessoais por ela tratados, seja através de controle ou operação.

Como bem explanado por Patrícia Peck Pinheiro e Larissa Lotufo, restou

---

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente". *Cf.* BRASIL. BRASIL. **Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, 2018**.

[124] PRIMEIRA SANÇÃO por descumprimento da LGPD é publicada pela ANPD. **Trench Rossi Watanabe**, *op. cit*.

[125] "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". *Cf.* BRASIL. **Emenda Constitucional Nº 115, de 10 de fevereiro de 2022**.

[126] PROTEÇÃO DE Dados Pessoais agora é um direito fundamental. **Ministério da Justiça e Segurança Pública**, 14 fev. 2022.

evidente que “os setores – públicos e privados – têm assinalado dificuldades em ficar em conformidade com as regras de proteção de dados impostas por seus países”[127]. Assinalam, para além, uma questão importante para as empresas com atuação multinacional, a necessidade de *compliance* em mais de uma legislação[128], como é o caso de empresas com atuação no Brasil e em países europeus que, de forma conjunta, precisam realizar adequações tanto sobre a LGPD quanto à GDPR. Com esse propósito, as autoras teceram breves direções de boas práticas sobre proteção da privacidade e dados pessoais.

Aqui, portanto, cabe destacar que não é de difícil busca por parte dos administradores de sociedades anônimas e suas respectivas equipes, considerando que o tema está aquecido no mercado desde a publicação da GDPR, com profissionais em recorrente especialização e identificação de melhores práticas desde então. Reconhece-se a viabilidade de tomadas de decisões adequadas sobre ações de cibersegurança, de forma específica, considerando as normas existentes, de proteção à privacidade e dados pessoais.

Como os temas estão intrinsecamente relacionados, a primeira diretiva consiste na adoção de política de segurança da informação. As autoras reforçam a relevância de medidas sólidas na criação e manutenção da política, de modo que haja real e efetiva adoção de ações de segurança da informação[129].

Nesse item, reforçam ainda a necessária adoção de um sistema de gestão de segurança da informação, ações capazes de dar corpo à temática a níveis gerenciais de uma organização, especialmente às maiores corporações. Ainda, assim como apresentado no capítulo posterior, colocam como justificativa a alta incidência e a categorização como risco a nível temerário pelas empresas, em pesquisa realizada pela *Allianz Risk Barometer,* por elas replicado[130].

As autoras destacam a definição de atores responsáveis pela proteção de dados da organização, com claras distinções e nomeações sobre as figuras do controlador, operador e encarregado de dados pessoais, agentes de definição obrigatória pelas organizações. O destaque da orientação subsome-se pelas alçadas de reporte desses agentes, que serão “centrais no desenvolvimento de toda e

---

[127] PINHEIRO; LOTUFO, *op. cit.*, p. 31.
[128] *Ibid.*
[129] *Ibid.*, p. 33.
[130] *Ibid.*, p. 33-34.

qualquer atividade que envolva o tratamento de dados pessoais”[131].

Mesmo com a divisão de papéis e responsabilidades em atividades próprias, em casos de incidente envolvendo dados pessoais em tratamento, haverá responsabilidade solidária entre os entes envolvidos, ponto que reforça a imperiosa adoção de postura transparente e de alinhamento adequado entre os atores[132].

Posteriormente, sugere-se a adoção de fatores de anonimização de dados ou pseudoanonimização dos dados pessoais nas hipóteses em que seja possível[133]. A justificativa insere-se na desconsideração da LGPD sobre dados que passam por processos de anonimização. Segundo essa orientação, empresas que atuam com informações obtidas por meio de dados podem ter como premissa na política de segurança da informação, por exemplo, a priorização quanto ao uso de dados anonimizados ou na criação de procedimentos de anonimização[134]. Aqui, vale destacar, que ocorrendo evento por ataque *ransomware*, serão reduzidos os riscos de vazamento de dados pessoais.

Por fim, são esses os pontos obrigatórios pela LGPD, o enfoque à figura do DPO, análise aprofundada sobre transferência internacional de dados pessoais e a emissão do relatório de impacto de proteção de dados como boa prática[135]. O RIPD consiste em um documento com descrição sobre os procedimentos existentes pela organização para mitigação e redução de riscos à privacidade e dados pessoais. Quanto à forma, como as autoras mencionam, não existe modelo específico que deva ser seguido, desde que haja: a. a identificação dos agentes; b. necessidade de elaboração do reporte; c. descrição sobre as medidas de tratamento; d. identificação de partes interessadas consultadas; e. necessidades e proporcionalidades de medidas; f. identificação e avaliação de riscos e suas respectivas ações de tratamento e, por fim; g. aprovação do relatório[136].

---

[131] *Ibid.*, p. 34.
[132] *Ibid.*, p. 34.
[133] *Ibid.*, p. 35.
[134] Sobre uma leitura aprofundada sobre esse tema, recomenda-se *Cf.* BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *In*: DONEDA, Danilo; MENDES, Laura; CUEVA, Ricardo (Org.). **Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020. p. 38-39.
[135] PINHEIRO; LOTUFO, *op. cit.*, 36-37.
[136] Exigências do Governo Brasileiro sobre informações basilares ao relatório de Impacto à Proteção de Dados Pessoais. Como forma de apoio às entidades privadas, a Secretaria do Governo Digital preparou uma oficina dirigida para orientar sobre o modo de confecção do referido relatório. *Cf.* BRASIL. **Oficina Dirigida – Relatório de Impacto à Proteção de Dados Pessoais. Dezembro de 2020**.

Ainda, recomenda-se a criação de um comitê de proteção de dados pessoais, com o objetivo de acompanhar o andamento das medidas de adequação e avaliar conjuntamente demandas que possam surgir a partir do tratamento de dados pessoais.

Relacionando as ideias do tópico, observa-se o fácil encontro de informações sobre proteção de dados pessoais, assim como a importância e peso legal de tais medidas. Para tanto, já há a presença de fator de necessária diligência por parte dos administradores das sociedades anônimas, sobretudo em seu dever de se informar e fiscalizar.

Encerra-se com a exemplificação do RIPD, cuja orientação do Governo Federal consiste na obtenção de aprovação sobre o relatório, que deve definir o grau de risco sobre incidentes com dados pessoais e a indicação de medidas adotadas pela companhia para tratar o risco apresentado.

Nesse diapasão, mesmo que haja diretivo legal específico sobre dados pessoais, as demais ações de cibersegurança se correlacionam, haja vista que dados pessoais pertencem à mesma cadeia de sistemas da informação e comunicação em uma companhia, possuindo o mesmo peso e mesma medida de proteção quando nos referimos à segurança da informação de modo macro. Eis aqui uma das primeiras evidências sobre o encaixe da cibersegurança como novo ponto de atenção e de necessária conduta para satisfação e compreensão quanto ao cumprimento do dever de diligência do administrador. O que será reforçado com a apresentação de casos envolvendo companhias abertas, ataques por *ransomware* e impactos negativos sofridos.

3 CENÁRIOS ENVOLVENDO ATAQUES POR RANSOMWARE: ALERTAS PARA ADOÇÃO DE MEDIDAS PELOS ADMINISTRADORES

Para aterrissar no contexto da dependência tecnológica e visualizar os incidentes de segurança da informação destacados como novos fatores de risco no capítulo anterior, cabe demonstrar eventos em que houve real prejuízo a entidades empresariais de capital aberto.

Vê-se que os riscos de cibersegurança estão presentes na rotina de todas as pessoas que utilizam dispositivos celulares ou computadores, sejam crianças ou adultos. Nesse sentido, a partir do momento em que se está no ambiente de *internet*, o usuário é automaticamente exposto aos riscos de ataques. Basta o acesso a uma caixa de *e-mails* e à caixa de lixo eletrônico, com envios maliciosos *de e-mails* com intimações judiciais falsas, *e-mails* sobre boletos de pagamento fraudulentos, dentre outras práticas em correios eletrônicos.

Destaca-se também a existência de *links* com a promessa de ganhos fáceis, jogos atrativos aos olhos de crianças ou, ainda, mensagens de *spam* durante a transmissão de conteúdos, como vídeos. Com efeito, introduz-se o tema com algumas breves constatações oriundas de pesquisas sobre ataques virtuais e o nível de exposição, objetivando destacar a relevância da abordagem e fator significativo. Isso para defender a existência de um novo fator de atenção e de dever de diligência por parte de administradores de sociedades empresárias, em razão da existência de públicos relacionados à atividade, investidores, consumidores, empregados, fornecedores e até mesmo agentes não definidos, a depender da extensão dos danos por um evento de ciberataque.

Outrora, a pesquisa delimitou-se ao cenário das sociedades anônimas de capital aberto, dada a negociação pública de valores mobiliários, como ações, debêntures, partes beneficiárias, os quais são lançados para negociação em bolsas de valores. Nesse sentido, qualquer incidente de crise abre margem para a desestabilização do mercado, sobretudo o de valores mobiliários, para além dos demais possíveis danos a investidores, consumidores, trabalhadores e outros[137].

Somando ao recorte desta pesquisa, as sociedades anônimas de capital

[137] SILVA, Américo Luís Martins da. **Sociedades Empresariais**. Volume 2. São Paulo: Editora Forense, 2007. p. 97-99.

aberto estão sujeitas aos regramentos da Comissão de Valores Mobiliários, como na realização de comunicações de temas relevantes ao mercado, por exemplo[138].

Para tanto, estima-se que o tempo médio de inatividade de uma empresa após a ocorrência de um incidente de cibersegurança é de 22 dias[139]. Em simples constatação, empresas que passam por eventos de cibersegurança possuem suas operações interrompidas num período de quase um mês, acarretando possíveis prejuízos financeiros, reputacionais, de proteção de dados e de saúde emocional por quem faz parte da instituição empresarial, dadas as incertezas sobre a severidade dos impactos oriundos do evento.

Como anteriormente mencionado, *e-mails* com conteúdos maliciosos sofreram um aumento de 600% após o período da pandemia da Covid-19[140]. Junto a isso, 37% das entidades entrevistadas pela pesquisa da *Sophos* foram afetadas por alguma modalidade de ciberataque no ano de 2020. Ademais, a referida pesquisa também destacou a baixa maturidade em segurança da informação pelas entidades, o que foi evidenciado com o isolamento social gerado pela pandemia.

No cenário brasileiro, em pesquisa realizada pela *SonicWall*[141], estima-se que o Brasil sofreu mais de 33 milhões de tentativas de ataque *ransomware* em 2021, evidenciando o aumento em tempo de distanciamento social e aumento de atividades *online* nas searas de trabalho, ensino e relações sociais. Em 2021, identificou-se que 55% das empresas brasileiras sofreram ataques de *ransomware*[142], as quais tiveram consequências negativas com perdas financeiras, operacionais e reputacionais, principalmente.

Conforme mencionado durante a exposição técnica sobre o *modus operandi* dos ataques de *ransomware* no capítulo anterior, o envio de *e-mails* maliciosos para contaminar os sistemas e redes é um método comum de disseminação do *malware*. E, diante desse ponto, em estudo publicado pela *Cybersecurity & Infrastructure Security Agency,* DE 2021[143], o método mais comum de disseminação é realmente o

---

[138] *Ibid.*, p. 102-105.
[139] STATISTA. **Distribution of information security incidents in 2020**.
[140] MUNCASTER, Phil. Cyber-Attacks up 37% over past months as #COVID19 bites. **Infosecurity Magazine**, 1 jun. 2020.
[141] SONICWALL. **Relatório de ameaças cibernéticas 2021**, 2022.
[142] SOPHOS. **The state of ransomware**, 2022.
[143] As táticas mais comuns que os *hackers* usam para realizar ataques de *ransomware* são campanhas de *Phishing* por e-mail, vulnerabilidades RDP e vulnerabilidades de *Softwares*. *Cf.*

envio de campanhas de *phishings* por *e-mails*, junto com vulnerabilidades em RDP e de segurança dos *softwares*.

Sobre a realização de pagamento de resgates, em pesquisa feita pela *Cyberreason*, avaliou que, de 1.263 empresas participantes, cerca de 80% delas realizaram o pagamento de resgate e sofreram outro tipo de ataque pouco tempo após o primeiro evento; dentre elas, 46% tiveram seus dados acessados. No entanto, alegaram que grande quantidade das informações foram corrompidas durante o ataque[144]; ainda, a pesquisa apontou que 69% das empresas entrevistadas sofreram perdas de receita; 53 afirmaram prejuízos à marca e reputação[145].

Por fim, diante dos dados destacados, em avaliação da consultoria *Gartner*[146], 60% das empresas, em conjunto com seus *stakeholders*, utilizarão ações de segurança cibernética como fatores condicionantes para a realização de investimentos ou identificação de novas oportunidades de negócio até o ano de 2025. *Gartner* conclui que ciberataques são uma nova categoria de risco empresarial, com impactos negativos multiníveis.

Em relatório emitido pelo Fórum Econômico Mundial de 2024, os ciberataques foram classificados como o 5º maior risco global conforme a percepção dos públicos participantes da pesquisa[147]. Uma informação relevante para esta pesquisa consiste no fato de que os ataques não são realizados sempre com o fito de obter vantagem financeira através dos pagamentos de resgate de sistemas – por intermédio do fornecimento de chaves de criptografia. O caso da guerra entre Ucrânia e Rússia é um dos exemplos.

Para o conflito iniciado em fevereiro de 2022, os ataques territoriais não foram os únicos meios utilizados pela Rússia em confronto com a Ucrânia. Desde o início da guerra houve alegado aumento massivo de ataques cibercriminosos, como a

---

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **2021 Top Malware Strains**, 25 ago. 2022.

144 BISSON, David. FBI Pegs 2020 Cybercrime Costs at $4 Billion – Actual Losses Likely Higher. **Cybereason**, 2021.

145 *Ibid*.

146 PANETTA, Kasey. As oito principais previsões de segurança cibernética para 2021-2022. **Gartner**, 20 out. 2021.

147 WORLD ECONOMIC FORUM. **The global risks report 2024**. 19th edition. January, 2024. p. 7.

transformação do *malware wiper*[148] para interromper operações de sistemas de proteção e contra-ataques significativos da Ucrânia[149].

A fim de elucidar o fato acima mencionado, em fevereiro de 2022 houve a implantação de três *wipers*, denominados de *hermeticwiper, hermeticwizard* e *hermeticransom*. Junto a eles houve um ataque direcionado à rede elétrica em abril de 2022, através da utilização do malware *Industroyer*, que paralisou parte significativa do sistema de energia da Ucrânia. Assim sendo, percebe-se a dimensão da utilização dos ciberataques, os quais objetivam obtenção de ganhos, mas também a obtenção de vantagens em ambientes de conflito, motivados por questões geopolíticas.

O mesmo ocorre no conflito entre Israel e Hamas, cujo grupo de *hackers* conhecido por *Charming Kitten*, declaradamente ligado ao *Islamic Revolutionary Guard Corps* (IRGC), realizou ataques aos setores logísticos de suprimentos e insumos básicos, transportes e demais tecnologias essenciais. Em função da possibilidade de uso de ciberataques contra “inimigos”, abre-se a possibilidade de utilização dos recursos ilícitos obtidos pelos ataques para consequente financiamento de ações e grupos terroristas.

Por essa razão, o GAFI[150] publicou um relatório sobre indicadores de risco na identificação de atividades suspeitas associadas ao *ransomware*. No mesmo relatório, a entidade apontou o necessário reconhecimento do *ransomware* como delito antecedente à lavagem de dinheiro, em que seus recursos obtidos são facilmente lavados no sistema financeiro.

A justificativa desse apontamento consiste na utilização de criptomoedas como a moeda solicitada para o resgate dos sistemas invadidos e criptografados, posteriormente utilizados para proveito dos criminosos e possivelmente para o financiamento de guerras, conflitos, ações terroristas e demais situações de

---

[148] ”Wiper worms, however, consist of a destructive payload and a propagation mechanism, which allows the wiper to spread across machines and networks. NotPetya and Olympic Destroyer are examples of wiper worms, meaning they were able to self-propagate – to remotely copy and execute the wiper – and perform lateral movement. While conventional understanding of wipers assumes their singular purpose is destruction or disruption [3], the following case studies show that functionality is different from intent and purpose. The function of all wipers is destruction, but the intent behind their destructive capability varies and seems to be evolving”. *Cf.* NAUMANN, Saher. Now You See It, Now You Don’t: Wipers in the Wild. **Virus Bulletin Conference**, Montreal, 2018.

[149] MACHADO, Léia. Um ano de guerra: Conflito envolve o ciberespaço como frente de batalha. **Security Report**, 24 fev. 2023.

[150] GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL. **Countering ransomware financing**. *op. cit.*

interesse da organização infratora.

Seguindo essa mesma linha de raciocínio, cabe dizer, inclusive, que há uma tendência ao reconhecimento dos pagamentos de resgate como incentivo ou facilitação à lavagem de dinheiro, bem como ao financiamento do terrorismo e proliferação de armas de destruição em massa[151].

Considerando, portanto, a sobrevinda da hipótese de utilização para financiamento do terrorismo, as ações de pagamento de resgate serão ainda mais reprováveis quando divulgadas em mídia. Com isso, as vítimas de ataques sofrerão possíveis consequências financeiras, operacionais e de imagem pelo ataque *per si*, agravando ainda mais o cenário se identificado e divulgado o pagamento de resgate com o fito de recuperar as operações da entidade empresarial.

Enfim, fechando com breves demonstrações sobre a gravidade, relevância e comparência do tema em diversos plexos da sociedade, incumbe apresentar recente movimentação da *Security Exchange Commission* (SEC), autoridade federal norte-americana independente de regulamentação e controle de mercados financeiros (traduzida ao português como Comissão de Valores Mobiliários dos Estados Unidos), que publicou novas regras sobre segurança cibernética aplicáveis às companhias[152].

O objetivo do novo regramento consiste na indução das entidades empresariais à realização do devido e adequado gerenciamento de riscos cibernéticos; adoção de melhores estratégias, governança do tema e consequente divulgação de incidentes de cibersegurança.

Almeja-se a prestação de divulgações padronizadas sobre o enfrentamento de ciberataques, objetivando maior transparência e agilidade na comunicação, favorecendo a rápida contenção de riscos sobre ações em bolsa da empresa vítima do ataque. Ou seja, há relevante interesse econômico em conter ou reduzir crises

---

[151] GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL. **Countering ransomware financing**. GAFI Report, *op. cit.*

[152] "According to Audit Analytics data, in 2021, it took on average of 42 days for companies to discover breaches, and then it took an average of 80 days and a median of 56 days for companies to disclose a breach after its discovery.412 These data do not tell us when disclosure occurs relative to companies' materiality determinations.

[...]

Additionally, evidence suggests registrants may be underreporting cybersecurity incidents.415 More timely, informative, and standardized disclosure of material cybersecurity incidents may help investors to assess an incident's impact better". *Cf.* SECURITIES AND EXCHANGE COMMISSION. **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 2022**. p. 108-111.

geradas por incertezas ou desconfianças dos investidores sobre empresas americanas, sobretudo em tempos de economia digital ou da “monetização dos dados”.

Passadas as evidências brevemente expostas, é inegável, portanto, concluir que ataques de *ransomware* são fatores geradores de crises em empresas e, por isso, há riscos sobre a perenidade da própria organização sujeita ao ciberataque, assim como há exposição da sociedade aos impactos e da própria economia de um país, gerando movimentações no sentido de proteger ou reduzir danos aos diversos personagens da sociedade.

Ainda, visando apresentar a realidade sobre ataques de *ransomware* e consequente exposição dos cenários de crise em empresas, apresenta-se estudos de casos que geraram impactos negativos a sociedades anônimas de capital aberto, demonstrando também como as regras da SEC foram frutos de uma realidade existente nas organizações e na economia de ações em bolsas de valores em nível mundial. Em conjuntura semelhante, há tendência de seguimento das mesmas propostas no Brasil, através da Comissão de Valores Mobiliários (CVM), regulamentadora das atividades de sociedades anônimas de capital aberto no país.

Para tanto, serão destacados os ataques vivenciados no Brasil pelas Lojas Americanas (Grupo B2W), Lojas Renner e JBS, as quais sofreram ataques em contextos diferentes, mas, da mesma forma, na modalidade de *ransomware*. Tais casos analisados sofreram consequências diferentes, mas com os mesmos tipos de impacto negativo, especialmente impactos financeiros.

Um ponto convergente entre as instituições empresariais e os ataques de *ransomware* consiste na forma qual as respectivas crises foram gerenciadas, o que determinou o agravamento ou atenuação das consequências negativas geradas.

Considerando a incidência de ciberataques e a dimensão de seus impactos, encerra-se o capítulo com estândares já existentes sobre a temática geral, de modo a evidenciar a presença de orientações e diretivos capazes de trazer informação e aconselhamento sobre melhores métodos aos administradores de sociedades, sobretudo anônimas e de capital aberto, dada a regulação e extensão de impactos oriundos por situações de crise.

3.1 CASO LOJAS AMERICANAS, SUBMARINO E SHOPTIME

A Lojas Americanas é controladora da varejista B2W, resultado da fusão entre o *e-commerce* Americanas.com e Submarino. Também é responsável pela marca *Shoptime*, cujo segmento é predominantemente de varejo e comércio eletrônico[153].

Em 19 de fevereiro de 2022 suas plataformas de vendas eletrônicas tiveram suas operações paralisadas em razão de suspeita de invasão aos servidores da companhia pela modalidade de ataque *ransomware*[154]. Em alegações realizadas em veículos de mídia, a empresa sinalizou ter realizado a suspensão de forma preventiva, objetivando reduzir possíveis impactos e ou evitar a exposição de dados pessoais e demais informações relevantes para a empresa[155].

Em um comunicado emitido pela consultoria Economática, que realizou a avaliação da empresa controladora das Lojas Americanas e demais *sites* do grupo, foram estimadas perdas na monta de R$3,488 (três bilhões e quatrocentos e oitenta e oito milhões de reais) em valor de mercado, sendo avaliada ao final do pregão do dia 22 de fevereiro de 2022 por R$26,4 (vinte e seis bilhões e quatro milhões de reais). Para além do mais, essa perda em *valuation*, houve perdas por efeitos reputacionais negativos em um mercado de comércio eletrônico altamente competitivo. Tais montas não foram divulgadas e analisadas sobre esse fato.

Conforme exposto pelo gerente de relacionamento da consultoria economática Einar Rivero[156], a perda de valor de mercado focou no problema operacional enfrentado pelas lojas americanas, somando-se às incertezas relacionadas ao fato, como possíveis responsabilizações que o mercado possa imputar à empresa.

Um fator considerado agravante ao ataque *ransomware* e a consequente crise gerada consistiu na ausência de comunicação clara e transparente aos clientes e investidores, promovendo situação de incerteza e desconfiança sobre os administradores da empresa e seus respectivos papéis[157].

---

153 Informações sobre a composição do grupo disponíveis em *Cf.* https://ri.americanas.io/a-companhia/nossas-marcas/. Acesso em: 18 set. 2023.
154 SANTINO, Renato. Americanas, Submarino e Shoptime saem do ar nesta segunda (21) após ataque. **Canaltech**, 21 fev. 2022.
155 MACHADO, Léia. Alerta: ciberataque aos canais eletrônicos da Americanas e Submarino indicam sinais de aliciamento. **Security Leaders**, 21 fev. 2022.
156 NALIN, Carolina; ALCÂNTARA, Camila. Americanas: Com suspensão das vendas on-line, empresa já perdeu quase R$ 3,5 bi em valor de mercado. **Jornal o Globo**, 23 fev. 2022.
157 *Ibid.*

Houve também uma severa queda das ações da empresa na B3 (Bolsa de São Paulo) na segunda-feira após o incidente, mesmo com orientações e sugestões de compra de ações da Americanas (AMER3) por especialistas em investimentos[158].

Posteriormente, ocorreu a publicação do balanço financeiro, referente ao terceiro trimestre de 2022 da *holding* mencionada. O balanço apresentou o atingimento de 77% do valor bruto de mercadoria (GMV) no período, 17% superior ao valor anterior à fusão entre Americanas.com, Sou Barato, Submarino, *Shoptime* e as lojas Americanas em operação de loja[159]. Para além, apontou o atingimento de R$9,9 bilhões em volume bruto sobre mercadorias vendidas pelo *e-commerce*, das quais R$5,4 (cinco bilhões) vindos de produtos dos *sellers* no *marketplace* e R$4,5 bilhões por produtos próprios[160]. Nesse sentido, utilizando como base o balanço reportado, Carlos Daltozo, da Eleven Financial[161], estimou R$50 milhões de perda por dia, período em que os *sites* estavam indisponíveis para vendas.

Pela análise realizada, considerou-se tão somente as vendas de produtos próprios, considerando, assim, perdas por vendas realizadas pelos *sellers*, a perda diária estimada sobe para R$100 milhões.

Seguindo a mesma linha, a XP investimentos divulgou um relatório a fim de alertar sobre a importância do monitoramento do tempo necessário para a normalização das operações. Considerou-se o tempo como fator agravante para os resultados da companhia[162].

Tal incidente de tecnologia também gerou especulações pelos bancos, instituições que realizam aportes de crédito ao Grupo Americanas. Um deles, o Banco Citi, sinalizou publicamente a percepção sobre o aumento de ataques cibernéticos, citando, para além desse, os casos da Natura, das Lojas Renner e da CVC.

De forma específica, sobre o caso Americanas, sinalizaram a percepção sobre o impacto sofrido ser de monta considerável, assim como, por decorrência, a diminuição de vendas no canal. Outrora, sinalizaram publicamente que as

---

158 *Ibid.*
159 MADUREIRA, Daniele. Americanas apresenta balanço de 2022 nesta segunda. **Folha de São Paulo**, 12 nov. 2023.
160 MADUREIRA, *Ibid.*
161 AMERICANAS FORA do ar: prejuízo pode chegar a R$ 100 milhões por dia. **AGÊNCIA O GLOBO, Revista Exame**, 22 fev. 2022.
162 *Ibid.*

expectativas foram de retomada rápida das operações[163].

Por fim, em relação ao contexto envolvendo o *case* apresentado, houve a divulgação de informação ao mercado sobre a suspensão das operações e servidores do *e-commerce*, sinalizando o início de protocolo de identificação da modalidade de ataque. Como anteriormente mencionado, a referida comunicação fora percebida como de baixa transparência[164].

Partindo para uma análise específica ao caso, em cotejo à análise realizada por Martha Carbonelli, verifica-se um tendente aumento dos ciberataques, sobretudo a empresas do *e-commerce* brasileiro. Ainda nesse sentido, destacou que os ataques possuem como intenção prejudicar a credibilidade das organizações ao expor vulnerabilidades da empresa, como ocorreu no caso Americanas[165].

Diante de tais considerações, são necessárias medidas de cibersegurança, mas, como ponto de especial importância, a realização massiva de treinamentos a todos os colaboradores e terceiros relacionados[166]. Isso porque, em sua grande maioria, os ataques surgem por acessos indevidos ou induções a erros por parte dos públicos mencionados, o que demanda conhecimentos específicos sobre segurança da informação e proteção de dados pessoais.

Por outro lado, Fabio Assolini[167], da Kapersky, sinaliza que os ciberataques no Brasil atingem majoritariamente o financeiro das Americanas, mas também afetam os usuários finais. Pontua que os ataques de *ransomware*, como o utilizado para esse caso, são cada vez mais comuns. Ao final, explana que os ataques possuem caráter racional e direcional para com as empresas e órgãos vítimas, isso considerando a pressão existente na contenção a ataques e possível realização do pagamento de resgate como forma de evitar o vazamento de dados pessoais e sofrer consequentes responsabilizações e danos reputacionais.

Diante do contexto do ataque e a situação de crise, percebe-se que, logo

---

163 *Ibid.*
164 COMUNICADOS AO MERCADO. Disponíveis em: https://api.mziq.com/mzfilemanager/v2/d/347dba24-05d2-479e-a775-2ea8677c50f2/dc001752-9438-197c-1352-7ee725df4110?origin=1; https://api.mziq.com/mzfilemanager/v2/d/347dba24-05d2-479e-a775-2ea8677c50f2/74befd9f-dfb2-42de-0f94-1f665b3441af?origin=1; https://api.mziq.com/mzfilemanager/v2/d/347dba24-05d2-479e-a775-2ea8677c50f2/68104b1e-9787-6630-a3f5-81dd5bf81e3e?origin=1. Acesso em: 23 ago. 2023.
165 AMERICANAS FORA do ar: prejuízo pode chegar a R$100 milhões por dia. **AGÊNCIA O GLOBO, Revista Exame**, *op. cit.*
166 *Ibid.*
167 *Ibid.*

após a ciência da situação, as Americanas realizaram medidas para interromper a invasão e possível vazamento de dados pessoais, suspendendo as operações dos canais de *e-commerce*. Logo após, iniciaram os protocolos de identificação do ataque e dos impactos incorridos nos sistemas internos. Como forma de levar a conhecimento de mercado, realizaram um comunicado, mas sem, contudo, dar maiores detalhes. Fator que ensejou certo receio aos investidores e mercado, dadas as incertezas trazidas pela generalidade do comunicado.

Em conclusão, sofreram perdas estimadas em milhões, resultado dos impactos negativos do ataque de *ransomware* sofrido. Portanto, o agravante consistiu na generalidade da comunicação e a situação atenuante foi a interrupção imediata dos sites e redes.

3.2 CASO LOJAS RENNER

Outro caso similar ocorreu com as Lojas Renner, também nas operações no *e-commerce*. Contextualizando o fato, as Lojas Renner (LREN3) foi alvo de um ataque cibernético no dia 19 de agosto de 2021, resultando na indisponibilidade de seu *site* e aplicativo após o incidente[168].

A empresa, na sequência do ataque, emitiu um comunicado ao mercado, afirmando ter acionado seus protocolos de controle e segurança para bloquear a invasão, com o objetivo de assegurar a preservação dos principais bancos de dados[169]. No mesmo comunicado, sinalizaram deter política e padrões rígidos de segurança e que continuariam aprimorando a infraestrutura para ter sempre como boa prática a adoção de novos protocolos de proteção de dados e sistemas internos.

Houve especulação do mercado sobre o ataque sofrido ter sido na modalidade de *ransomware*, dado ao tempo despendido até a recuperação dos bancos de dados e sistemas[170]. No entanto, a empresa não confirmou a informação.

Como impacto, os papéis da Renner na bolsa (LREN3) apresentaram queda de 1,5%, passando a ser negociados a R$38,87[171]. Seguindo mesma perspectiva

---

[168] MACHADO, Léia. CISOs se manifestam diante de ciberataque à Renner. **Security Leaders**, 23 ago. 2021.
[169] BRAUN, Daniela. Lojas Renner aguarda análise de peritos para identificar origem de ciberataque. **Valor Investe**, 1 set. 2021.
[170] MACHADO, *op. cit.*
[171] BRAUN, *op. cit.*

analítica, em avaliação da XP Investimentos[172], a ocorrência foi negativa, considerando o tempo e custo para potencial resgate dos sistemas. Deduziu-se um impacto negativo nas operações digitais da companhia, sendo efeito atenuante o fato de a maior receita ser originária das operações de loja, as quais não foram afetadas. Como resultado da avaliação, a XP não adotou recomendações ou contraindicações, apenas sinalizou uma rápida retomada e crescimento do valor da quota, para uma média estimada de R$50.

Uma avaliação também foi realizada por profissionais do Itaú BBA, que trouxe o seguinte posicionamento:

> Essa, infelizmente, não é a primeira vez que uma empresa sob nossa cobertura é alvo de um ataque cibernético. Dito isso, todas as companhias que foram vítimas desses ataques conseguiram normalizar suas operações, sem grandes danos operacionais. Por isso, esperamos que a Renner consiga normalizar totalmente suas operações em breve[173].

Neste aspecto, realizaram recomendação de investimento *outperform*, considerado, na seara de investimentos, como uma recomendação acima do mercado sobre os papéis da Renner, tendo em conta preço pouco superior a R$50 para o ano de 2022.

As consultorias *Levante* e *Guide Investimentos*[174] avaliaram o ciberataque como negativo ao mercado, devido a dimensão que geralmente os ataques possuem, muito embora, à época, ainda não fossem conhecidos os danos causados pelo incidente.

Em contrassenso com as avaliações supracitadas, a consultoria *Infinity Asset*[175] considerou que o ataque acarretaria baixo impacto para a empresa vitimada. Para tanto, utilizaram como parte atenuante o fato de a Renner ter conseguido manter as operações de loja normais, sem riscos nos sistemas aos envolvidos.

É imperioso destacar que, na mesma colocação do consultor da empresa mencionada, o incidente envolvendo a JBS – próximo caso a ser analisado – foi

---

[172] LOJAS RENNER: os possíveis impactos do ataque hacker nas operações e nas ações da companhia. **Infomoney**, 22 ago. 2021.
[173] *Ibid.*
[174] *Ibid.*
[175] *Ibid.*

relembrado, com uma conclusão sobre o aumento da suscetibilidade das empresas em sofrer ciberataques.

Seguindo o mesmo raciocínio que o evento da JBS, o consultor deduziu que o pagamento de eventual resgate não acarretaria impacto negativo severo, considerando que a Renner valia R$35 bilhões de reais na bolsa em 2021. Concluindo as avaliações dos especialistas em investimentos, Victor Hugo Gonçalves[176], considerou grave a situação, considerando a alta quantidade de servidores internos atacados, estimados em 2,6 mil.

Asseverou que a Lei Geral de Proteção de Dados não se trata somente de fazer documentos com respaldo jurídico, mas de uma mudança de mentalidade corporativa, cujas empresas devem trabalhar com segurança da informação, processos internos e treinamentos aos seus colaboradores. Nesse sentido, entende que houve a falta dessas categorias de investimento por parte das Lojas Renner.

Por fim, teceu uma crítica sobre a varejista, ao fato de ter atuado sobre o ciberataque somente para encerrar a situação de crise, sendo uma forma simplória de convencer o mercado e seus respectivos investidores de que é uma empresa segura sob o viés de proteção do ambiente cibernético.

Sobre o posicionamento supra, destaca-se que os consultores de investimento e demais profissionais atuantes no mercado realizam comparações sobre segurança da informação, ciberataques e eventuais riscos de exposição de dados pessoais, lançando à mídia a importância da adoção de medidas preventivas eficazes para além das documentalmente por lei exigidas.

Encerrando o contexto sobre o ciberataque, houve especulação do mercado sobre as Lojas Renner terem realizado o pagamento de resgate na monta de US$20 milhões de dólares aos cibercriminosos. Sinalizaram, para além, que o sequestro por *ransomware* inicialmente objetivada a obtenção de R$1 bilhão em criptomoedas para liberar a chave criptográfica e viabilizar o reestabelecimento dos sistemas atacados[177]. No entanto, em comunicado, a companhia negou ter realizado o pagamento de resgate. Como posição padrão da empresa, disseram que

> [...] a companhia atua de forma diligente e com foco para mitigar os efeitos causados, com a maior parte das operações já restabelecidas

[176] *Ibid.*
[177] RENNER DIZ não ter pago resgate após ataque hacker. **O Globo**, 24 ago. 2021.

> e tendo sido verificado que os principais bancos de dados permanecem preservados[178].

Asseveraram naquele momento que a adoção de política de restabelecimento dos sistemas através de *backups*, metodologia capaz de acessar informações armazenadas a título de histórico, mas os sistemas se mantiveram fora do ar por ao menos 48h. Ao final, as lojas Renner comunicaram ao mercado a volta dos sistemas, mas sem abordar sobre a eventual exposição de dados pessoais dos clientes do *e-commerce*. Por essa razão, o Programa de Proteção e Defesa do Consumidor (Procon)[179], notificou a empresa para que fornecessem esclarecimentos sobre eventuais riscos envolvendo dados pessoais, bem como se houve incidente envolvendo dados pessoais.

Em comparação ao caso anteriormente analisado, verifica-se que o diferencial entre os casos está na comunicação rápida sobre a ocorrência do ciberataque, o que corroborou para avaliações positivas ou neutras de consultores de investimento. A ação que possivelmente segurou eventuais quedas bruscas nos valores dos papéis da Renner.

Em similaridade, viu-se que as Lojas Renner não trouxeram clareza às informações, como, por exemplo, sobre a exposição de dados pessoais relacionados ou o tipo de ciberataque enfrentado, mantendo-se em situação de comunicação genérica. Isso acarreta especulações do mercado e, possivelmente, incertezas ou inseguranças sobre o investimento, gerando posições dúbias e contraditórias.

3.3 CASO JBS

O último caso abordado envolve a JBS S.A, considerada uma das maiores empresas frigoríficas do mundo. Em maio de 2021, sofreram um ataque *ransomware* que paralisou as operações nos Estados Unidos da América e Austrália[180].

Em entrevista emitida para o *The Wall Street Journal*, o então presidente das subsidiárias localizadas na região Norte Americana, André Nogueira, declarou que a companhia teve ciência do ciberataque na manhã do dia 30 de maio, em um

---

178 *Ibid.*
179 PROCON. **Notificação do Procon-SP sobre ataque cibernético, 1 out. 2021**.
180 JBS USA CEO Andre Nogueira and Feeding America on soof supply chain. **WALL STREET JOURNAL**, 16 maio 2020.

domingo, quando colaboradores da área de tecnologia notaram anormalidades nos sistemas, localizando mensagem com exigência de pagamento de resgate na sequência[181].

Uma das primeiras atitudes tomadas pelos administradores da JBS após o conhecimento do ciberataque foi a comunicação ao Governo dos Estados Unidos da América, denunciando a possível origem de uma organização situada na Rússia.

Em comunicação, a equipe de tecnologia da informação da empresa realizou o desligamento do sistema responsável por fornecer informações sobre o setor de carne, com o fito de retardar o avanço do *ransomware*[182]. Em mesmo período, ocorreram as primeiras tratativas de comunicação do incidente ao governo norte-americano e autoridades policiais.

Como medida adicional, a organização também contratou empresas externas para a realização de análises forenses sobre os sistemas de tecnologia internas, objetivando identificar os pontos de vulnerabilidade, meio de acesso empregado, e se houve possível acesso indevido aos dados da empresa, sobretudo aos dados pessoais[183].

Com o intento em atenuar ameaças mais graves pelo grupo *hacker* ou até mesmo exposição de informações da empresa e dados pessoais, a JBS também acionou os demais fornecedores de tecnologia e especialistas em segurança digital para início das negociações com o grupo *REvil*[184].

A avaliação da Federal Bureau of Investigation (FBI), departamento de investigações federal dos Estados Unidos da América, identificaram que o ataque foi perpetrado pelo grupo da *REvil*, também identificado por *Sodinokibi*, organização criminosa originária da Rússia.

Segundo a análise realizada pelo governo norte-americano, o ataque sofrido pela JBS foi considerado o terceiro maior ataque eletrônico ligado a cibercriminosos russos[185]. Sua gravidade, junto de outros incidentes anteriores vislumbrados nos EUA, foi uma questão levantada pelo Presidente norte-americano, Joe Biden, em

---

[181] *Ibid.*
[182] *Ibid.*
[183] *Ibid.*
[184] CRESWELL, Julie; PERLROTH, Niole; SCHEIBER, Noam. Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business. **The New York Times**, 1 jun. 2021.
[185] SHALAL, Andrea. Após ataque hacker contra JBS, EUA devem mostrar postura mais agressiva diante da Rússia. **Terra**, 2 jun. 2021.

encontro com o Presidente russo, Vladimir Putin, realizado em junho de 2021[186].

Sobre o ciberataque, a imprensa da JBS comunicou que o crime ocorreu por *ransomware*, com consequente cobrança de resgate para liberação dos sistemas[187].

Quanto ao fator operacional, todas as atividades na Austrália foram afetadas conjuntamente, com 25 filiais industriais da JBS na América do Norte, ensejando cancelamento de turnos e interrupção de operações anexas (como logística).

As operações do setor de aves foram restabelecidas em menor tempo (dois dias) e as de carne bovina se mantiveram fechadas por maior período.

As atividades foram retomadas no início de junho – na quinta-feira após o ciberataque, identificado no domingo[188] – e não foram localizados pontos de ataque nas demais filiais, situadas em outros países da América Latina, como a matriz, no Brasil[189]. Explorando a breve narração dos fatos acima, dá-se a entender que a empresa adotou meios similares aos casos anteriores, quais sejam: comunicações, contratação de suporte em tecnologia e segurança da informação para restabelecimento das informações e demonstração pública de receio sobre eventual exposição de informações internas e dados pessoais.

Após as investigações preliminares – até então não conclusas –, afirmaram que os servidores de *backup* não foram comprometidos, considerando que essa foi a metodologia empregada para restauração dos sistemas e informações da organização, bem como não houve indício de comprometimento de dados da empresa, clientes e funcionários[190].

Em discrepância aos casos envolvendo as Lojas Americanas e Lojas Renner, a JBS comunicou as autoridades e ao mercado sobre a realização de pagamento de resgate aos cibercriminosos. Esse fato veio a público posteriormente, quando da comunicação sobre o pagamento da monta estimada em US$11 milhões de dólares em bitcoins[191].

O CEO da JBS USA, André Nogueira, declarou a decisão foi originada após consulta a especialistas em segurança digital, com o intento de reduzir riscos e

---

[186] *Ibid.*
[187] JBS PARALISA 25 unidades nos EUA e Canadá após ataque hacker. **CNN BRASIL**, 1 jun. 2021.
[188] ARBULO, Rafael. Ataque à JBS foi executado pelo grupo hacker REvil. **Olhar digital**, 4 jun. 2021.
[189] O QUE se sabe sobre ataque cibernético a JBS investigado pelo FBI. **BBC News Brasil**, 2 jun. 2021.
[190] JBS DIZ que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. **G1 Globo**, 9 jun. 2021.
[191] O QUE se sabe sobre ataque cibernético a JBS investigado pelo FBI. **BBC News Brasil**, *op. cit.*

problemas associados à invasão, além de buscar evitar o vazamento de dados[192]. Asseverou, ainda, que a decisão foi de difícil tomada, mas sentiram que a decisão "deveria ser tomada para evitar qualquer risco potencial para nossos clientes'[193].

Segundo levantamento realizado pela empresa de *software* de segurança *Immunefi*, esse foi o segundo maior pagamento de resgate em bitcoins[194], considerando o primeiro realizado pela *CNA Financial*, na monta de US$40 milhões de dólares[195].

A mesma organização considerou que a escolha por transações envolvendo criptomoedas originou-se pelo crescimento de criptomoedas e consequente confiança dos cibercriminosos sobre a anonimização e não rastreabilidade dessas transações, o que pode facilitar operações maiores do que as por intermédio de sistemas financeiros tradicionais[196].

Em vias de conclusão ao tópico, meses após o ciberataque, executivos da JBS prestaram depoimento e esclarecimentos perante audiência especial realizada no Congresso Norte-americano, a respeito do incidente de ciberataque perpetrado pelo grupo *REvil*.

Durante a sessão, em avaliação feita pela Presidenta do Comitê de Supervisão e Reforma do Governo dos Estados Unidos, Carolyn Maloney, a pressão ao caso foi agravada por garantias dos cibercriminosos sobre o pagamento de resgate para resolver situação de publicidade negativa para a empresa. Mencionou, ainda, mensagem emitida pelos criminosos que, em tradução literal, foi: "Podemos desbloquear seus dados e manter tudo em segredo. Tudo o que precisamos é de um resgate"[197].

Ainda na sessão, os executivos da JBS confirmaram ter sofrido danos relacionados a custos para restauração de sistemas, custos sobre obrigações com clientes, de reparação de processamento de produtos nas instalações, além do pagamento do resgate[198].

---

[192] JBS DIZ que pagou US$11 milhões em resgate a ataque hacker em operações nos EUA. **G1 Globo**, *op. cit.*
[193] *Ibid.*
[194] CRESWELL; PERLROTH, *op. cit.*
[195] IMMUNEFI. **Top Crypto Ransomware Payments Report**, 2022.
[196] *Ibid.*
[197] EXECUTIVOS DA JBS contam como foi o ciberataque. **CISO Advisor**, 29 nov. 2021.
[198] CONGRESS OF THE UNITED STATES. **Supplemental Memo on Committee's Investigation into Ransomware**. Memorandum.

Sobre as negociações realizadas com os criminosos, os executivos comentaram sobre promessas de entrega da chave criptográfica e evidências de não comprometimento dos dados sequestrados, mas que, ao final das negociações, os *hackers* não forneceram evidências sobre destruição das cópias de dados realizadas[199].

No relatório da sessão, o FBI identificou que o grupo *REvil* obteve acesso aos sistemas através do acesso a uma antiga conta de administrador de rede não desativada e protegida apenas por uma senha de fraca segurança[200].

Em novembro de 2021, as autoridades norte-americanas identificaram e indiciaram envolvido nos ataques[201]. Eles anunciaram que seria um *hacker* ucraniano, chamado Yaroslav Vasinskyi, imputando sua participação em diversos ciberataques, dentre eles, o da JBS[202]. Em conjunto, anunciaram a apreensão do montante de US$6,1 milhões ligados a um outro membro pertencente à organização, chamado Yevgeniy Polyanin[203], indiciado pelas mesmas infrações, mas solto até aquele momento[204].

Logo após a discussão sobre o ciberataque e o encontro realizado entre EUA e Rússia, especialistas em cibersegurança identificaram que *sites* ligados ao grupo *REvil* desapareceram repentinamente da *internet*.

As teorias sobre o desaparecimento levantadas indagaram sobre: a. operações especiais norte-americanas para derrubar os referidos canais; b. ordens russas sobre a retirada dos *sites* do ar; c. retirada voluntária pelo grupo, considerando exposição em mídia e investigações em andamento por dois países com alta inteligência tecnológica e investigativa[205].

Após o processo de apuração sobre o ocorrido, a empresa de segurança

---

[199] *Ibid.*
[200] CONGRESS OF THE UNITED STATES. **Supplemental Memo on Committee's Investigation into Ransomware**. Memorandum.
[201] *Ibid.*
[202] OFFICE PUBLICA AFFAIRS – U.S. DEPARTMENT OF JUSTICE. **Ukrainian Arrested and Charged with Ransomware Attack on Kaseya**, 8 nov. 2021.
[203] Destaca-se a correlação entre investigações envolvendo *ransomware* e ações de compliance, em específico, sobre processos de *due diligence*, considerando aqui, por exemplo, que um dos membros da organização teve seu nome indicado na lista restritiva *Office os Foreign Assets Control (*OFAC). *Cf.* https://sanctionssearch.ofac.treas.gov/Details.aspx?id=33858. Acesso em: 25 ago. 2023.
[204] JOBIM, Caio. Europol e FBI prendem hackers ligados aos ataques ransomware contra JBS e Kayzea. **Cointelegraph**, 10 nov. 2021.
[205] SANGER, David. Russia's most aggressive ransomware group disappeared. It's unclear who made that happen. **The New York Times**, 13 jul. 2021.

Securityscorecard[206] publicou relatório que indicou vazamento de dados da matriz da JBS no Brasil, demonstrando ausência de conhecimento total e confiável pela JBS sobre o evento sofrido.

Segundo o relatório, os criminosos iniciaram a etapa de reconhecimento de cenários em fevereiro de 2021, com retiradas furtivas de dados iniciadas em março de 2021 a maio de 2021, até o período da criptografia dos sistemas e dados[207]. Ressaltaram que, durante a etapa de exfiltração de dados, ocorreram retiradas de dados do Brasil para o mesmo serviço de transferências utilizado, os quais foram ofertados para *download* no *site* de compartilhamento "*mega*"[208].

Traz-se outras consequências acessórias oriundas do ataque. Houve efeito dominó no setor de carnes, acarretando aumento no preço do produto nos Estados Unidos da América, gerando prejuízos a comerciantes, restaurantes e, em geral, a pequenas cidades[209]. As fábricas tiveram que operar com horas extras de trabalho, para restabelecer produção e fornecimento, considerando a posse de fatia de 23% do processamento de gado dos Estados Unidos em 2021[210].

No entanto, a JBS não forneceu informações apuradas sobre a totalidade de danos e eventuais impactos negativos adicionais ao negócio em ação voluntária. Não houve qualquer responsabilização interna evidenciada e publicada em mídia.

Outrora, ainda em junho de 2021, a Comissão de Valores Mobiliários emitiu uma solicitação de esclarecimentos sobre os motivadores pelos quais a JBS não comunicou os eventos ocorridos no cenário internacional como fato relevante ao mercado[211]. O desdobramento da notificação foi protegido por confidencialidade.

Como fato destoante em comparação aos demais casos, a JBS obteve recorde de lucro líquido no ano de 2021, mesmo ano em que sofreu o ataque nas operações norte-americanas[212].

---

[206] SHERSTOBITOFF, Ryan. JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified. **Security Scorecard**, 8 jun. 2021.
[207] SHERSTOBITOFF, *Ibid.*
[208] *Ibid.*
[209] PREJUÍZO DO ataque hacker contra JBS se estendeu à indústria de alimentos dos EUA. **Infomoney**, 11 jun. 2021.
[210] *Ibid.*
[211] COMISSÃO DE VALORES MOBILIÁRIOS. **Solicitação de esclarecimentos, de 10 de junho de 2021**.
[212] BEVILACQUE, Rafael. Lucro da JBS em 2021 foi o maior da história da empresa; como ficam ações? **UOL**, 23 mar. 2022.

3.4 IMPORTÂNCIA DE AÇÕES DE PREVENÇÃO E GESTÃO DE CRISES EM CIBERSEGURANÇA

Uma nova realidade de riscos oriunda da sociedade em rede, explanada por Castells, torna o dever de diligência de administradores um desafio constante, considerando o fator de dependência, desenvolvimento contínuo e volátil de novas tecnologias, assim como da inteligência aplicada nos ciberataques. Esses riscos, como se vê, possuem o condão de gerar danos operacionais, contratuais, financeiros de imagem, e, em evolução, o regulatório/legal.

Em específico, tem-se os compromissos de dimensão internacional sobre proteção de dados, conforme mencionado no capítulo anterior, discussões as quais tiveram como resultado a estruturação de normas, como a Lei Geral de Proteção de Dados Brasileira, a *General Data Protection Regulation*, aplicável na Europa, a *California Consumer Privacy Act*, Norte-americana, assim como demais publicadas com o mesmo objetivo. Para além dessas, há as normas em discussão, como a *IA Act* – em discussão europeia para a regulamentação do uso e criação de mecanismos de inteligência artificial.

Aqui, cabe destacar que não se objetiva esgotar o tema, mas se aproveita para mencionar que o precursor para as discussões relacionadas à inteligência artificial consistira nos possíveis riscos que essas tecnologias poderiam causar à sociedade. Os vértices principais fundaram-se nos riscos à privacidade e dados pessoais, também na impossibilidade de contenção de determinadas inteligências, como as utilizadas em veículos autônomos e indústrias.

Assim como observado nos tópicos anteriores, há a presença de situações de risco sobre tecnologia. Acentua-se as ocorrências de ataque por *ransomware* em diversos nichos de atuação empresarial, independentemente de sua estrutura, quantidade de colaboradores, faturamento e região de atuação. É preciso considerar, além disso, possível aumento de ciberataques, gerando fator de maior suscetibilidade por parte de empresas.

Sem embargo, à medida que novos crimes virtuais surgem, novas ações de prevenção e combate também são constituídas, em especial, buscando proteger dados pessoais. Ou ao menos deveriam ser constituídas, como forma de garantir a perenidade da organização e saúde operacional, financeira e reputacional ao

mercado. Nesse sentido, o objetivo do presente tópico consiste na demonstração de guias e normas para boas práticas em segurança da informação e proteção de dados disponíveis.

Em conjunto, propõe-se a adoção de programas de *compliance*, cujas ações de prevenção, detecção e resposta a riscos – se bem implementadas – possuem o potencial de trazer segurança à continuidade dos negócios empresariais, assim como cultura resiliente de proteção de dados pessoais, segurança da informação e comunicação ágil de eventos de crise, possibilitando rápida tomada de decisões e ações.

A demonstração de alternativas e boas práticas já consolidadas em mercado advém pela inegabilidade quanto ao impacto negativo à própria empresa ao ser vitimada por um ataque. As consequências tendem a ser econômicas, de imagem, operacionais e legais, caso haja incidente envolvendo dados pessoais.

Nessa oportunidade, considerando as características norteadoras do dever de diligência do administrador de uma sociedade anônima, há fortes indicativos de que cibersegurança ou ciberataques *per si* não são questões de difícil acesso à informação, bem como os impactos de seus riscos e medidas de mitigação ou prevenção de incidentes de segurança da informação e proteção de dados em um modo amplo.

Para tanto, almeja-se demonstrar o acesso às informações sobre segurança da informação pela indicação de referencial doutrinário, mas, além desse, em referências por meio de normas da Associação Brasileira de Normas Técnicas (ABNT); por recomendações emitidas pela própria CVM, que, muito embora possam não ser diretamente aplicáveis ao ramo empresarial ou estrutura, podem ser utilizadas a título de boa prática em cibersegurança.

Não aparenta ser de difícil obtenção de conhecimento necessário e de grau ótimo para a tomada de decisões no ambiente empresarial.

Noutra face, não se nega a possível sobrevinda de vieses comportamentais ou heurísticas existentes por um ou mais administradores da sociedade, se considerado, por exemplo, questões sobre gastos em contraste com lucros auferidos

e a existência do viés de ancoragem[213] atrelado, mas esse não é um ponto a ser discutido neste trabalho[214].

Posto isso, existem medidas de prevenção e redução de riscos sobre ataques de *ransomware*.

A CVM, através do então presidente João Pedro Nascimento, em evento de divulgação de pesquisa setorial em cibersegurança, reconheceu abertamente a urgência de medidas de segurança da informação, orientando consequente dever de consciência sobre a importância do tema. Aduziu, ainda, que a CVM deseja que as companhias identifiquem a segurança da informação como fator de risco para o negócio. É uma questão de *awareness*[215].

Destacou que a preocupação com cibersegurança deve ocorrer à medida do nível de risco que a empresa está inserida e exposta, exemplificando o caso de instituições que se apoiam em aplicativos, as quais se sujeitam a riscos maiores[216].

Na ocasião, houve a recomendação de comunicação à CVM sobre comunicação a clientes e mercado sobre a ocorrência de ciberataques em período de até 30 dias após o incidente, sinalizando inspiração à determinação da *Security Exchanges Commission* (SEC), que obriga as companhias norte-americanas a comunicar em até cinco dias[217]. Assim sendo, um dos primeiros pontos de acesso à informação por administradores consiste na Resolução nº 135, da própria CVM[218], que dispõe sobre o funcionamento dos mercados por esta regulamentados.

Na mencionada resolução há a definição de orientações de segurança da informação aplicáveis a entidades administradoras de mercado organizado, considerando o poder de desequilíbrio das negociações por eventuais falhas nas operações destas. No entanto, não cabendo aqui estressar os riscos próprios, é interessante analisar as orientações trazidas pela norma a título de boa prática para

---

[213] Consiste na tomada de rumos com bases e situações previamente estabelecidas, de modo a tornar difícil a mudança de decisão e postura. *Cf.* MOCHON, D., & FREDERICK, S. Anchoring in sequential judgments. **Organizational behavioral and human decision processes**, v. 122, n. 1, 2013.

[214] Recomenda-se, ainda, as seguintes leituras *Cf.* GONÇALVES, Oksandro. MIRÓ, Gustavo. CORNASSINO, Maria. LUCIANO, Danna. **IV Livro de resultados de pesquisa do GRAED PUCPR**. Londrina: Thoth Editora, 2023; KAHNEMAN, Daniel. **Rápido e devagar**: duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

[215] GARÇON, Juliana. CVM diz que não deve baixar novas regras de segurança; entenda. **Estadão Investidor**, 13 set. 2023.

[216] *Ibid.*

[217] *Ibid.*

[218] COMISSÃO DE VALORES MOBILIÁRIOS. **Resolução CVM Nº 135, de 10 de junho de 2022**.

toda e qualquer outra organização empresarial, como as próprias companhias abertas reguladas pela CVM.

Um dos primeiros pontos consiste na orientação do dever de desenvolver e implementar regras, procedimentos e controles internos adequados para a garantir a confidencialidade, integridade e disponibilidade de dados e informações sensíveis[219]. Demandou-se a estruturação de diretrizes de identificação e classificação de dados, de avaliação de relevância dos incidentes de segurança da informação, da proteção de dados e suas consequentes exposições, e, por fim, os procedimentos adotados para registro da ocorrência de incidentes relevantes, suas causas e impactos negativos[220].

Há apontamentos específicos sobre a necessidade de procedimentos adequados para o gerenciamento de riscos e controles internos, de modo a mensurar, monitorar, controlar, mitigar e reportar riscos inerentes aos mercados pelas empresas acima mencionadas administrados. Resta claro o objetivo de prevenir eventual situação de crise e desequilíbrio de determinado mercado ou fatia de empresas com ações na bolsa[221].

Em seção própria, aborda-se a demanda pela existência de planos de continuidade de negócios, almejando a perenidade da organização administradora de mercado organizado[222].

Um fato importante sob o viés de gestão de riscos de tecnologia, presente na mencionada resolução, consiste no foco sobre sistemas críticos que, em outra leitura, pode indicar a existência de dependência a certos recursos de tecnologia e na resolução em comento; há seção própria sobre o desenvolvimento de políticas e procedimentos sobre capacidade, integridade, resiliência e disponibilidade para manutenção plena das operações e consequente funcionamento regular dos mercados organizados administrados.

A resolução determina a presença mínima de planejamento sobre a capacidade, com realização de testes de estresse da tecnologia empregada na rotina operacional; na realização de testes de periodicidade mínima anual; testes prévios quando da implantação ou alteração envolvendo os sistemas críticos, planos

---

[219] *Ibid.*
[220] Artigos 108 e 109, *Cf.* COMISSÃO DE VALORES MOBILIÁRIOS. **Resolução CVM Nº 135, de 10 de junho de 2022**. p. 54. .
[221] Artigos 101 a 103. *Cf. Ibid.*, p. 48 a 50.
[222] Artigos 104 a 106. *Cf. Ibid.*, p. 50 a 52.

de monitoramento, diretrizes para avaliação da relevância dos incidentes, requisitos mínimos de qualificação e experiência dos funcionários relevantes para a operação, e, ainda, implementação de indicadores de níveis de tolerância que permitam avaliação do desempenho[223].

Por fim, a norma da CVM, em avaliação, considerada como um manual com pontos de boas práticas por organizações interessadas, consiste na estruturação de programa próprio de segurança cibernética.

A norma estipula que as empresas por ela reguladas devem, minimamente, atender critérios de identificação e avaliação de riscos cibernéticos internos e externos, os quais a administradora de mercado organizado esteja exposta. Junto a essa, determina sobre a identificação de funções e informações críticas ao negócio e na instrumentalização de critérios de proteção[224].

Seguindo o mesmo fluxo, define sobre a adoção de medidas de redução de vulnerabilidades, como: a. prevenção, limitação e combate de possíveis impactos oriundos de algum incidente cibernético; b. detecção da ocorrência de anomalias indicativas de potencial incidente; c. contenção, retomada e recuperabilidade de dados e sistemas; d. definição de ações de comunicação interna e externa[225].

Cabe registrar que a norma traz uma definição expressa sobre a periodicidade de revisão, treinamento dos públicos envolvidos, incluindo administradores (aqui em modo amplo) e formas de compartilhamento de informações sobre ameaças e vulnerabilidades consideradas relevantes[226].

Ao todo, observa-se que, para entidades administradoras de mercados organizados, já existem medidas destinadas à adoção de metodologias de segurança da informação, em específico, de cibersegurança. Isso considerando riscos de desestabilização do mercado e de negociações em bolsa.

Vale considerar a existência de informações disponíveis a todo plexo de atividades empresariais. O que se diferencia aqui consiste na obrigatoriedade ou adoção das ações a título de boas práticas, considerando os riscos a que a empresa esteja sujeita. Sobre boas práticas em segurança da informação para ambientes cooperativos, trazem o contexto de um ambiente com importância e dependência

---

[223] Artigo 107. *Cf. Ibid.*, p. 52 a 54.
[224] Artigo 110. *Cf. Ibid.*, p. 54 e 55.
[225] Artigo 110. *Cf. Ibid.*
[226] Artigo 110. *Cf. Ibid.*

cada vez maior da tecnologia, que acarreta busca de altos níveis de competitividade entre as organizações, com grandes disputas sobre novos mercados[227].

Assim, com a utilização de recursos tecnológicos não há de se olvidar sobre a presença de concorrentes em todos os lugares possíveis do globo e que para poder competir é necessário deter os mesmos conhecimentos e instrumentos de TICs[228].

Para os autores, um ambiente cooperativo consiste na

> [...] integração dos mais diversos sistemas de diferentes organizações, nos quais partes envolvidas cooperam entre si, na busca de um objetivo em comum: velocidade e eficiência nos processos e nas realizações de negócios[229].

Contudo, evidenciam a ocorrência de problemas nos ambientes cooperativos, em que existem partes como filiais, parceiros de negócio, clientes, mecanismos de acesso remoto e usuários móveis. Um dos problemas destacados na obra refletiu, à época, a exposição de informações confidenciais entre uma das organizações parte da rede ou a exposição de dados sensíveis sobre a relação entre as entidades pertencentes à rede cooperada[230].

Em cotejo a esse cenário, abordam boas práticas em segurança da informação, iniciando pela política de segurança, que ganha destaque por ser base para as demais questões de segurança.

Sobre a política de segurança, frisam que "[...] trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando também em consideração os processos e os negócios, além da legislação local"[231]. Encerram com o entendimento de que ela faz a vez de desenho de cultura na empresa, atuando na função de facilitadora e simplificadora do gerenciamento dos recursos tecnológicos.

Para os autores, há um ponto relevante para a pesquisa, qual seja, a necessidade de apoio dos executivos das empresas para que a política de segurança aconteça e seja eficiente ao que se objetiva. O motivador remete à necessidade de investimentos e direcionamento de recursos por parte dos executivos, assim carecendo do comprometimento deles.

---

[227] BARRETO, *op. cit.*, p. 13-15.
[228] NAKAMURA, *op. cit*., p. 22.
[229] *Ibid.*
[230] MACHADO, *op. cit.*, 2014, p. 29-32.
[231] MACHADO, *Ibid.*, p. 162.

Logo na sequência, tratam da relevância de se ter uma política para gestão de senhas na organização. A razão dessa orientação se subsome ao uso de senhas como fator de autenticação e acesso a sistemas, sendo assim, o "[...] elo mais fraco da corrente de segurança". Em mesmo teor, avaliam que senhas fracas consistem no maior e principal fator de vulnerabilidade sobre riscos de acesso não autorizado[232].

Há também a recomendação de adoção de política para *firewall*, mecanismo de filtragem de fornecimento de informações aos usuários, realizado através da classificação dos servidores e o que pode ou não ser acessado pelos usuários[233].

Sobre as políticas a serem adotadas, há a política para acesso remoto, considerando aqui ambientes que demandam e tenham interesse em utilizar acesso remoto.

Em 2003, por exemplo, a realização do trabalho remoto não era prática comum ao mercado. Em contraponto, no período após a pandemia da Covid-19 (2019), houve um aumento notório de atividades laborais em casa. Razão pela qual se utilizou a obra destacada como referencial, dada a visibilidade de aplicação das medidas pelo período de 20 anos.

Direcionando a análise de boas práticas em segurança da informação para um aspecto mais técnico e prático, tem-se a efetiva utilização de *firewalls*, de sistema de detecção de intrusão, criptografia e PKI, redes privadas virtuais (VPN), gestão e controle de tráfego e autenticações de sistemas e usuários.

A obra referenciada destaca as principais recomendações e componentes necessários para a adoção das medidas de proteção. A título de exemplo, o uso do *firewall* com o recurso de *proxy* para a simples liberação ou bloqueio de usuários da corporação, considerada como um recurso simples, mas que já seria eficaz para a organização com baixos riscos à época[234].

Sobre o sistema de detecção de intrusão, recomendam o *network-bases intrusion detection system* para casos em que há interesse em monitorar o tráfego de toda rede e conhecer os usuários e demais movimentações[235].

---

[232] NAKAMURA; GEUS, *op. cit.*, p. 189.
[233] STALLINGS, *op. cit.*, p. 6-19; 389-395.
[234] NAKAMURA; GEUS, *op. cit.*, p. 228.
[235] SÊMOLA, *op. cit.*, p. 123-124; 158.

De forma geral, os autores destacam que as medidas de segurança devem ser aderentes à realidade da empresa. Com efeito, não há demanda pela adoção de todos os procedimentos de segurança existentes, desde que a empresa observe seus riscos e consequentes vulnerabilidades[236].

É interessante mencionar a existência de outras classificações identificadas à época da mencionada obra, como *script kiddies*[237], *ciberpunks*[238], *insiders*[239], coders[240], *White hat*[241], *black hat*[242], *gray hat*[243] e *ciberterroristas*[244], algumas posteriormente parcialmente suprimidas pelo entendimento como parte da prática de *ransomware.*

Noutro vértice, decorridas as análises por meio de doutrina a respeito do tema, cabe mencionar as normas ISO sobre segurança da informação e de gestão da privacidade, as quais possuem poder como norma técnica referência sobre determinados temas, como os mencionados supra.

As normas ISO são originárias da Organização Internacional de Normalização, que tem como objetivo a criação de regramentos que facilitem o comércio e promovam boas práticas de gestão, disseminando segurança ao mercado sobre organizações empresárias que sejam certificadas ISO aos temas de interesse[245]. Em um aspecto macro, estão disponíveis para acesso as normas da classe 27000, sendo a 27001 a que define requisitos mínimos para um sistema de gestão de segurança da informação, como políticas e monitoramentos adequados e necessários.

---

[236] NAKAMURA; GEUS, *op. cit.*, p. 229.
[237] São pessoas com baixo conhecimento tecnológico, que se aproveitam de conteúdos livres na *internet* para buscar proveito em brechas de sistemas de empresas. *Cf. Ibid.*, p. 52.
[238] São considerados “aqueles que se dedicam às invasões de sistemas por puro divertimento e desafio”. Considera-se aqui a posse de alto conhecimento e utilização de criptografia nos ataques para evitar exposições de suas pessoas. *Cf. Ibid.*, p. 52.
[239] Considerada como a modalidade de ataque mais utilizada no ano de 2001. A metodologia empregada poderia consistir na espionagem de sistemas, ou, ainda, no bloqueio dos acessos e na negação de serviços. *Cf. Ibid.*, p. 55 e 56.
[240] Tidos como “*hackers* que resolveram compartilhar seus conhecimentos escrevendo livros ou proferindo palestras e seminários sobre suas proezas”. *Cf. Ibid.*, p. 58.
[241] Conhecidos “hackers do bem”, empregando conhecimentos detidos para a descoberta de vulnerabilidades e aplicação de correções. *Cf. Ibid.*, p. 59.
[242] Grupo que acessa sistemas para roubar informações secretas. *Cf. Ibid.*, p. 60.
[243] São grupos com notório conhecimento sobre as atividades de *hacking. Cf. Ibid.*, p. 61.
[244] Por fim, são grupos que realizam a invasão de sistemas para emissão de mensagens de cunho político ou religioso ou, ainda, buscando derrubar infraestruturas de comunicação ou obter informações sobre segurança de alguma nação ou organização. *Cf. Ibid.*, p. 61.
[245] É a organização responsável pela padronização e normalização de práticas em 162 países. Mais informações disponíveis em: http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp. Acesso em: 2 abr. 2024.

Há também a ISO 27002, responsável pela certificação em cibersegurança, com a disponibilização de código de práticas e controles adequados ao ciberespaço. Inclui-se também uma diretriz própria para a realização de auditoria sobre sistemas, inserido na ISO 27008.

Especificamente quanto à proteção da privacidade e dados pessoais, tem-se a ISO 27701 de 2019[246], que corrobora para a adequação das entidades empresariais à Lei Geral de Proteção de Dados Brasileira (LGPD). As diretrizes da ISO 27701 trazem requisitos legais, como a avaliação de riscos a exposição de dados pessoais, a realização de controle de acessos a dados pessoais, a nomeação de pessoa encarregada pelas operações, dentre outros[247].

Ao todo, sobre as normas ISO, cabe destacar o acesso disponibilizado em *sites* e/ou através de consultores em segurança da informação, os quais utilizam as recomendações por padrão durante a atuação consultiva e de identificação de cenários para adequação ou melhoria.

Há também as recomendações e *framework* do *National Institute of Standards and Technology* (NIST), agência governamental norte-americana responsável por estruturar padronizações para a promoção da concorrência nas empresas. Cumpre destacar que o objetivo consiste na apresentação de estândares praticáveis em âmbito nacional e internacional, os quais podem nortear o conhecimento sobre o tema e a tomada de decisões a respeito, não sendo foco o aprofundamento de cada indicação.

O NIST possui *frameworks* próprios, cuja estrutura básica consiste em um núcleo, níveis de implementação e perfis[248]. Nessas estruturas, há a categorização sobre formas de tratamento de cibersegurança, classificadas por: a. identificação de cenários, dados e riscos; b. proteção dos sistemas, dados e informações; c. detecção de situações de risco e tentativas de ataque; d. resposta aos incidentes, ataques e situações de crise; e. recuperação[249].

---

[246] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27001**: Sistema e Gestão em Segurança da Informação. Rio de Janeiro, 2019.
[247] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27001**, *op. cit.*, p. 48-55.
[248] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity, 12 feb. 2014**.
[249] *Ibid.*

Vale mencionar a possibilidade de utilização de programas de *compliance*[250] como metodologia de reforço e adoção de medidas de prevenção a incidentes de tecnologia ou no processo de identificação de um ciberataque.

Nessa linha, considerando a importância de um tratamento adequado aos desafios para garantir a preservação da estrutura empresária, junto a um novo panorama normativo de normas de proteção de dados pessoais e demais iniciativas preventivas, tem-se como alternativa a implantação de programas de *compliance*, os quais apoiarão na etapa da identificação de riscos internos e externos que as organizações estão sujeitas, bem como medidas de prevenção. Ressalta-se desde já que o *compliance* somente será bem aplicado se houver o comprometimento de todas as pessoas envolvidas para ter eficiência e investimento nas ações de conformidade.

Seguindo a análise para a apresentação dos pilares e metodologias de *compliance*, incumbe destacar que atualmente o mercado reconhece a existência de atividades basilares[251], resumidos em: 1. apoio da alta administração; 2. análise de riscos; 3. código de conduta e demais políticas; 4. controles internos; 5. comunicação e treinamento; 6. canal de denúncia; 7. investigações internas; 8. *due diligence*; 9. auditoria e monitoramento; 10. diversidade e inclusão.

Dentre todas as ações existentes em um programa básico de *compliance*, tem-se a percepção de que as ações de análise de riscos, normas e políticas internas, monitoramentos e treinamentos são medidas recomendáveis e de fácil implantação pelo viés de tecnologia. Quanto a esse aspecto, brevemente mencionado no trabalho, considera-se o uso de metodologias de identificação de riscos para o mapeamento de riscos de tecnologia e segurança da informação[252].

Há também o apoio da equipe de *compliance* na definição, estruturação e atualização de normas; na definição de monitoramentos[253] que apresentam indícios

---

[250] *Compliance*, em uma tradução literal, compreende estar em conformidade. Assim sendo, amplia-se o seu uso para a conformidade legal, operacional e de boas práticas em ética e integridade aos negócios.
[251] NEVES, Edmo Colnaghi. Compliance empresarial: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan Editora, 2018.
[252] ANTONIK, Luis Roberto. Compliance, ética, responsabilidade social e empresarial: uma visão prática. Rio de Janeiro: Alta Books, 2016.
[253] ANTONIK, Luis Roberto. Compliance, ética, responsabilidade social e empresarial: uma visão prática. Rio de Janeiro: Alta Books, 2016.

de ataque ou demais riscos de tecnologia que comprometam a continuidade dos negócios.

Por fim, tem-se os treinamentos[254], capazes de ensinar e reforçar orientações sobre pontos de atenção, condutas proibidas, comunicação de incidentes e demais ações de prevenção, como, por exemplo, não acesso a *links* estranhos ou realização de *download* de arquivos suspeitos. Dessa forma, vislumbra-se a importância da adoção de medidas de cibersegurança e resta evidenciada a presença do tema, assim como o longo arcabouço orientativo e direcionador sobre boas práticas de segurança da informação ou, de forma mais específica, de segurança no ciberespaço e proteção de dados pessoais.

Aqui se considera, portanto, práticas já consolidadas no mercado, o dever de conhecer e se informar sobre, por parte não somente dos técnicos e especialistas em segurança e tecnologia da informação, mas também dos dirigentes e administradores das organizações. Destaca-se, no entanto, a diferença entre os níveis de instrução necessários, mas não excluindo o conhecimento mínimo a respeito[255].

Faz-se necessário o entendimento, diante do que já foi exposto, sobre padrões de conduta esperados dos administradores de sociedades anônimas, objetivando evidenciar o conhecimento sobre incidentes de tecnologia, ataques por *ransomware* e consequente adoção de ações de cibersegurança como fatores indissociáveis ao reconhecimento do atendimento do dever de diligência no contexto da sociedade tecnológica.

---

[254] NEVES, Edmo Colnaghi. Compliance empresarial: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan Editora, 2018.
[255] LUPION, Ricardo; HACKMANN, Evaldo Osorio. Cibersegurança e dever de diligência do administrador. **Revista jurídica Luso-brasileira**, ano 9, n. 2, 2023. p. 1445-1473.

4 PADRÕES DE CONDUTA ESPERADOS E RESPONSABILIDADES CIVIS DOS ADMINISTRADORES DAS SOCIEDADES DE CAPITAL ABERTO AOS TEMAS ASSOCIADOS A INCIDENTES CIBERNÉTICOS

A atividade empresária possui caráter profissional, razão que impõe alguns conhecimentos e informações necessários[256], como deveres no exercício.

Considera-se que sociedades anônimas de capital aberto em situação de crise possuem capacidade de impacto negativo não somente para com seus clientes, fornecedores e ramo de atuação, mas também à classe de investidores que possuem títulos negociados na empresa, capazes de gerar condições de crise econômica de natureza grave, desestabilizando a economia de uma região, desencadeando outros focos de crises e prejuízos em diversos eixos na cadeia social.

Deve-se entender o funcionamento e objetivo de seus produtos e serviços, seu modo de utilização, riscos, defeitos, público-alvo, sendo parte indissociável de seu dever conhecer e informar-se sobre[257]. Para além do dever, é preciso constituir uma atividade organizada e estruturada.

Percebe-se, portanto, que os deveres primordiais dos empresários objetivam a garantia do bom andamento da atividade empresarial, com foco é direcionado à manutenção da atividade empresarial, não do empresário[258].

No que diz respeito a esse aspecto, a teoria geral do direito empresarial traz definições próprias para cada modelo de empresa, de modo a designar deveres, responsabilidades e características próprias para cada negócio planejado por seus constituidores.

Pensando sobre as estruturas empresárias existentes no Brasil, esta pesquisa pondera sobre estruturas e características próprias das sociedades anônimas de capital aberto, não aprofundando o estudo da origem e evolução histórica de tais configurações.

---

[256] SACRAMONE, *op. cit.*, p. 27.
[257] COELHO, Fábio Ulhoa. **Manual de direito comercial**. 28. ed. São Paulo: Revista dos Tribunais, 2016. p. 34-35.
[258] Visão trazida por Calixto Salomão Filho, após análise dos interesses sociais dentro do direito societário durante a etapa de recuperação de empresa. *Cf.* SALOMÃO FILHO, Calixto. Recuperação de empresas e interesse social. *In*: SOUZA JUNIOR, Francisco Satiro de; PITOMBO, Antonio Sergio A. de Moraes (Coord.). **Comentários à lei de recuperação de empresas e falências**. 2. ed. São Paulo: Revista dos Tribunais, 2007. p. 43-54.

A justificativa para tanto se subsome ao fato de que as sociedades de capital aberto são moldadas mediante norma própria: a Lei das Sociedades Anônimas (Lei No 6.404, De 15 de Dezembro de 1976). O funcionamento dessa categoria empresarial é disciplinado pela Comissão de Valores Mobiliários (CVM), autarquia federal constituída com a finalidade de regular, desenvolver e fiscalizar o funcionamento de tais estruturas empresárias.

Os motivadores para a existência da CVM[259] e seus normativos são alinhados conforme fatores de desenvolvimento econômico por meio da livre iniciativa (liberdade para exercer atividade empresarial), e na defesa dos interesses da figura dos investidores e o mercado de valores mobiliários.

Modesto Carvalhosa, ao avaliar os interesses tutelados pela lei das Sociedades Anônimas, verifica a existência de 5 principais proteções: a. proteção com viés contratual ao corpo de acionistas; b. proteção a credores e acionistas de caráter estatal; c. proteção aos investidores em sentido amplo, pelo viés do interesse público e sob responsabilidade estatal; d. a autotutela reguladora do interesse público; e. a respectiva proteção jurisdicional[260]. Nota-se que as proteções destacadas por Carvalhosa muito se relacionam aos princípios de cibersegurança.

Diante disso, a adoção de medidas de cibersegurança corrobora para a tutela dos investidores, dada a relação de confiança e segurança estabelecida entre eles e a empresa. Assim, não haverá possíveis riscos de, por exemplo, desestabilização do mercado ou desencadeamento de efeito manada sobre a venda de ações após a incidência de um ciberataque. Isso porque o núcleo de investidores confiará nas medidas de contingência adotadas e na transparência sobre as informações. Em mesma rota, a proteção em sentido amplo, considerando a existência e adoção de processos e controles internos capazes de reduzir riscos de exposição de dados pessoais, por exemplo, junto das demais proteções mencionadas pelo autor.

Resta presente característica dada por Carvalhosa sobre o contrato, refletido através do estatuto social na sociedade anônima e sua força invocatória sobre acordos realizados e deveres destacados. Na estrutura das sociedades anônimas há as características da divisão por ações e a responsabilidade limitada dos

---

[259] BRASIL. **O que é a CVM?**

[260] CARVALHOSA, Modesto. **Comentários à lei das sociedades anônimas**. 3. ed. São Paulo: Saraiva, 2003. p. 8-12.

acionistas[261].

Para a constituição de uma sociedade por capitais abertos, a lei das sociedades anônimas, em seus artigos 82 a 87, define os respectivos requisitos, que partem do registro da emissão na CVM, abarcando necessariamente o estudo de viabilidade econômica, o projeto sobre o estatuto social e o prospecto assinado pelos fundadores e instituição financeira intermediária. Para além dessa demanda, há o dever de convocação de assembleia-geral, para realização de avaliação dos bens – nos casos em que seja necessário, bem como deliberar sobre a constituição da sociedade anônima.

Na estrutura da companhia aberta, há o tratamento pelo viés da teoria organicista[262], em que há o entendimento pelo pertencimento da administração como um dos órgãos integrantes da sociedade.

No ambiente dos órgãos das sociedades anônimas, tem-se: a. assembleia-geral; b. conselho de administração; c. conselho fiscal; d. corpo diretivo – diretoria. Nesse regimento, entende-se como parte da administração de uma sociedade anônima o conselho de administração e a diretoria.

Por intermédio da teoria da representação orgânica, reconhece-se a existência de estrutura de gestão, considerando que sua movimentação somente se dá por meio de processos decisórios de pessoas[263], compreensão similar ao perfil e

---

[261] CAMPINHO, Sérgio. **Curso de direito comercial**: sociedade anônima. São Paulo: Editora Saraiva, 2023. p. 137-140.

[262] Segundo Paulo Fernando Campos Salles de Toledo: "A Lei das Sociedades Anônimas é muito clara a respeito da adoção da teoria organicista. Lê-se, em seu art. 139, que 'as atribuições e poderes conferidos por lei aos órgãos de administração não podem ser outorgados a outro órgão, criado por lei ou por estatuto'. Além de explicitamente empregar a expressão 'órgão de administração', acentua uma das principais características do organicismo: a indelegabilidade das funções legalmente atribuídas a um órgão societário. Já o Código Civil, ao tratar das sociedades, não é tão ostensivo. Ainda assim, não deixa dúvidas quanto à também ter adotado a teoria organicista, seguindo, neste passo, a tradição do direito brasileiro. O maior exemplo da opção assumida encontra-se no art. 1.070, o qual, em termos muito próximos do art. 139 da Lei das S.A., dispõe que 'as atribuições e poderes conferidos pela lei ao conselho fiscal não podem ser outorgados a outro órgão da sociedade'. É certo que o dispositivo se refere exclusivamente ao conselho fiscal, mas obviamente deve ser estendido a outros órgãos societários. Não faria sentido, com efeito, que uma atribuição própria da assembleia de sócios, prevista por norma legal específica, fosse, por cláusula contratual, outorgada a outro órgão da sociedade limitada. Por outro lado, a regra do art. 1.070 é reforçada pelo disposto no art. 1.018, ao prescrever que 'ao administrador é vedado fazer-se substituir no exercício de suas funções'. Em outros termos, ele não pode delegá-las, e isto, como facilmente se depreende, por ser órgão da sociedade" *Cf.* CASTRO, Rodrigo R. Monteiro de; AZEVEDO, Luís André N. de Moura (Coord.). **Poder de controle e outros temas de direito societário e mercado de capitais**. São Paulo: Quartier Latin, 2010. p. 364-365.

[263] SACRAMONE, Marcelo Barbosa. **Ato de preenchimento de órgão de administração**. Tese (Doutorado em Direito Comercial) – Universidade de São Paulo, São Paulo, 2012. p. 11.

figura do empresário. Nessa toga, a constituição como órgão origina-se pela demanda de centralização de responsabilidades e "poderes funcionais"[264] para que haja movimentação da sociedade.

Para tanto, considerando o poder e dever de tomar decisões para mover uma estrutura empresária por capital aberto, é preciso compreender as responsabilidades e deveres de seu pertencimento na sociedade, sobretudo em cotejo aos riscos atrelados à atividade empresária desenvolvida e os demais riscos emergentes, como os relacionados à tecnologia e vivência no ciberespaço.

Nessa conjunção, serão avaliados os requisitos e pontos cruciais à configuração do dever de diligência ao administrador da sociedade anônima e as respectivas responsabilidades anexas e eventuais ações de responsabilização face a eventuais danos causados pela ausência de conduta diligente no exercício da administração.

4.1 PADRÕES DE CONDUTA ESPERADOS NO DEVER DE DILIGÊNCIA

Como abordado nos capítulos e tópicos anteriores, a sociedade atual é moldada pela dependência de recursos tecnológicos, especialmente tecnologias de informação e comunicação.

Diante da dependência, tem-se o aproveitamento indevido da situação, evidenciado pelas modalidades de ciberataque, como o *ransomware*, capaz de interromper as atividades de grandes empresas e indústrias e ensejar incidentes envolvendo dados pessoais relacionados à atividade da empresa vitimada, como vazamento de dados pessoais.

Nesse diapasão, a presença real de ciberataques que culminaram prejuízos a grandes empresas, constituídas formalmente por empresas de capital aberto, demonstram a latência do tema no cenário corporativo.

Com efeito, existem diretivos capazes de corroborar na mitigação ou redução de riscos emergentes, como os associados à contaminação da empresa por ataques de *ransomware*, fator independente de profunda identificação de estândares para a obtenção, inclusive, de certificações sobre segurança da informação. Entende-se que a posse de certificação em segurança da informação gera uma maior confiança

[264] *Ibid.*

ao mercado, por ver a adoção de uma postura diligente – tanto em relação a medidas operacionais de prevenção quanto diante de medidas de redução de impactos negativos e danos durante a situação de crise por conta de um ciberataque, desconsiderando aqui outras modalidades de incidentes de segurança da informação.

Destaca-se que na estrutura das sociedades anônimas há a posição dos administradores como parte necessária para a manutenção e perenidade da organização empresária. As obrigações e deveres são estabelecidos com o fito de manter o bom andamento da organização, como o dever de diligência, ponto focal desta pesquisa.

Cotejando brevemente o cenário internacional[265], relacionado a deveres de diligência e incidentes de cibersegurança, tem-se a avaliação do GAFI sobre o pagamento de resgates estar associado à facilitação de branqueamento de ativos, ou, ainda, na facilitação ao financiamento do terrorismo[266].

Outra movimentação interessante consiste no novo diretivo da Austrália sobre ações de comunicação das empresas sobre a ocorrência de ataques de *ransomware* e, ainda em discussão, sobre a legalidade quanto ao pagamento de resgates[267].

Durante as discussões sobre essa proposta, os legisladores entenderam informações sobre riscos de cibersegurança nas organizações que já são exigidos aos administradores como premissa básica ao cumprimento de seus deveres de diligência[268].

Analisando a norma australiana[269], percebe-se que, caso uma empresa que tenha violado as leis de sanções da Austrália, essa poderá contar com a defesa ao abrigo da seção 21(2E) da Carta das Nações Unidas. No entanto, somente se provar que tomou precauções razoáveis e exerceu a devida diligência para evitar a contravenção. O que pode ser difícil de comprovar, assim como nos possíveis riscos relacionados à publicidade negativa durante o processo de defesa.

---

[265] HANLEY, Rob. MACPHERSON; John. VIERTMANN, Maxine. Ransomware new legislation should criminalise making ransomware payments. **Ashust**, 26 nov. 2021.
[266] GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL. **Countering ransomware financing**. GAFI Report, *op. cit.*
[267] FEDERAL COURT OF AUSTRALIA. **Australian Securities and Investments Commission v RI Advice Group Pty Ltd Statement of Claim, 21 out. 2021**.
[268] PROOFPOINT. **2020 State of the Phish. 2020**.
[269] FEDERAL COURT OF AUSTRALIA. **Australian Securities and Investments Commission v RI Advice Group Pty Ltd Statement of Claim, 21 out. 2021**, *op. cit.*

No cenário internacional, tem-se as recomendações emitidas pela *Securities and Exchange Commission* (SEC), agência reguladora que controla o mercado de capitais nos Estados Unidos, que adotou novas regras exigindo que as empresas de capital aberto divulguem ataques cibernéticos dentro de quatro dias úteis após determinar que são incidentes materiais[270].

De acordo com a comissão de valores mobiliários, incidentes materiais são aqueles que os acionistas de uma empresa de capital aberto considerariam como importantes “na tomada de uma decisão de investimento”. A SEC também adotou novos regulamentos que obrigam os emissores privados estrangeiros a fornecer divulgações equivalentes após violações de segurança cibernética.

Resta evidente a necessária adoção do dever de diligência nesse caso, em função da tomada de conhecimento de incidentes, e comunicá-los ao mercado, como forma de agir em transparência para com seus investidores. Indispensável rememorar o caso das lojas Renner e caso envolvendo a JBS, cuja comunicação ao mercado constituiu fator relevante ao entendimento pela queda ou não das ações negociadas na bolsa.

Perante esses pontos, conforme a teoria geral do direito empresarial, cabe abordar mais a fundo sobre o dever de diligência dos administradores das sociedades anônimas. Para tanto, inicia-se pela constatação de que as sociedades anônimas se manifestam através das ações de seus órgãos administradores. E é pela definição trazida por Pontes de Miranda[271] que a compreensão do dever de diligência será moldado.

Aqui, cabe expressar que entre o administrador e a empresa não há uma relação contratual, mera prestação de serviço de administração ou simples poder de representatividade. A extensão da atividade de administração ultrapassa camadas simples de atividade, por isso a configuração como órgão social parte da companhia[272].

Há um caráter indelegável das funções exercidas pelos administradores, o qual se justifica pelo seu exercício como forma de manifestar interesses da

---

[270] *Ibid.*
[271] MIRANDA, Pontes. **Tratado de direito privado**. 3. ed. Rio de Janeiro: Borsoi, 1972. p. 384.
[272] LUCAS, Lais Machado. **Programas de integridade nas sociedades anônimas**: implementação como conteúdo do dever de diligência dos administradores. Porto Alegre: Livraria do Advogado, 2021. p. 132-134.

sociedade anônima[273].

Em mesma rota, Carvalhosa entende que o corpo diretivo acumula funções tanto de gestão quanto de representação da sociedade, a medida do exercício de seus cargos e eventuais divisões formalizadas em estatuto[274].

Aqui, portanto, reconhece-se a responsabilidade dos administradores como extracontratual, por não ser resultante de descumprimento contratual, mas de descumprimento de deveres legais a esses impostos.

Dentro dessa camada de deveres legais, tem-se o dever de diligência, objeto desta pesquisa, cujo objetivo inicial consiste na assunção do caráter de diligência que todo "homem ativo e probo" costumaria empregar durante o exercício de suas funções para exercício do interesse da empresa e ao bem público[275].

Em breve comparação a outros países, Paulo Roberto Tavares Paes traz a identificação do dever de diligência alemão como "a diligência de um gerente ordenado e consciencioso"[276], ou seja, há o afastamento da característica do homem ativo e probo, visualizado pelo autor como abstrato. Seguindo a mesma linha, trouxe o julgado sobre o caso francês *Glorieux*, que responsabilizou os dirigentes por não atenderem a função como um bom pai de família[277] e toda diligência de uma pessoa assalariada[278], visualização ponto de críticas entre parte dos doutrinadores, uma vez que a visão de bom pai de família como um ponto de comparação ao dever de diligência não é mais adequada.

A contrário senso do defendido por Antônio Menezes Cordeiro, mas seguindo o que foi suscitado por Paes, Fábio Ulhoa Coelho[279] entende que o termo não

---

[273] Marcelo Adamek ainda frisa que "sabe privativamente a eles a manifestação da vontade social a terceiros. *Cf.* ADAMEK, Marcelo Vieira Von. **Responsabilidade Civil dos Administradores de S/A e as ações correlatas**. São Paulo: Editora Saraiva, 2009. p. 23-25.

[274] CARVALHOSA, *op. cit.*, p. 62-63.

[275] Realizando um adendo histórico, o Código comercial de 1850 (Lei nº 556 de 25 de junho de 1850) já dispunha acerca do dever de diligência em seu artigo 142, com o seguinte texto: "Art. 142 - Aceito o mandato, o mandatário é obrigado a cumpri-lo segundo as ordens e instruções do comitente; empregando na sua execução a mesma diligência que qualquer comerciante ativo e probo costuma empregar na gerência dos seus próprios negócios". O presente código teve sua primeira parte revogada com o advento do Código Civil, em 2002.

[276] PAES, Paulo Roberto Tavares. **Responsabilidade dos administradores de sociedades**. São Paulo: Revista dos tribunais, 1997. p. 31.

[277] A alusão ao preceito do bom pai de família foi cunhada por Antônio Menezes Cordeiro. *Cf.* CORDEIRO, António Menezes. **Da boa fé no direito civil**. Coimbra: Almedina, 2015.

[278] "n'ont pas accompli leus mandat em bom pères de familles, et qu'ils n'y ont pas apporté toutes les diligences d'um mandataire salarié". *Cf.* PAES, *op. cit.*, p. 31.

[279] "A adoção do bom pai de família como paradigma não é mais operacional, hoje em dia. De um lado, por se tratar de padrão por demais impreciso e em total descompasso com a realidade, tendo

pertence à realidade, considerando as novas estruturas familiares, assim como a competência para o exercício da administração deve ser o substituto ao termo ‘bom pai de família’.

Pela visão do direito comercial português, em seu respectivo código sobre as sociedades comerciais, há o entendimento sobre a necessária observância aos deveres de cuidado, de modo a evidenciar a competência técnica e conhecimento sobre a atividade exercida pela empresa, o que faz empregar, portanto, decisões criteriosas e ordenadas[280].

Mariana Pinto[281], ao suscitar as múltiplas faces do dever de diligência, aborda a realidade italiana, que trata o dever de diligência como a diligência que é exigida pela própria função, assim como o dever de atender normas, como o próprio código civil italiano ou as regras determinadas pela sociedade empresária.

Sobre a realidade argentina, o dever de diligência também se relaciona com a figura do “bom homem de negócios[282]”; na realidade chilena, tratam o dever de diligência como parte modular dos deveres fiduciários dos administradores, considerando como integrantes de uma diretoria colegiada, com as respectivas responsabilidades de direção, gestão, administração e de representação à sociedade[283].

Por fim, em relação ao contexto mundial, no regramento empresarial norte-americano há a expressão *duty of care*[284], que, como trazido por Lais Machado

---

em vista as profundíssimas alterações na distribuição social de trabalho entre os sexos e as novas estruturas familiares”.

[280] O Código das Sociedades comerciais traz a seguinte exposição: “1 - Os gerentes ou administradores da sociedade devem observar: a) Deveres de cuidado, revelando a disponibilidade, a competência técnica e o conhecimento da atividade da sociedade adequados às suas funções e empregando nesse âmbito a diligência de um gestor criterioso e ordenado; e b) Deveres de lealdade, no interesse da sociedade, atendendo aos interesses de longo prazo dos sócios e ponderando os interesses dos outros sujeitos relevantes para a sustentabilidade da sociedade, tais como os seus trabalhadores, clientes e credores. 2 - Os titulares de órgãos sociais com funções de fiscalização devem observar deveres de cuidado, empregando para o efeito elevados padrões de diligência profissional e deveres de lealdade, no interesse da sociedade".

[281] PINTO, Mariana. As múltiplas faces do dever de diligência. **Análise editorial**, 9 dez. 2022.

[282] Como consta na Lei de sociedades comerciais: “Los administradores y los representantes de la sociedad deben obrar con lealtad y con la diligencia de un buen hombre de negocios.”. Sobre a realidade argentina, *Cf.* HALPERÍN, Isaac. **Sociedades Anónimas**. Buenos Aires: Editora De Palma, 1974.

[283] URQUIAGA, Francisco Pfeffer. Deber de lealtad de directores y gerentes de sociedades anónimas al interior de un grupo de sociedades, a propósito del denominado Caso Cascadas. **Revista ACTUALIDAD JURÍDICA**, n. 32, jul. 2015. p. 207-211.

[284] Em aprofundamento ao contexto norte-americano, *Cf.* HAMILTON, Robert. **The law corporations**. Saint Paul: West group, 2000. p. 445 *et seq.*

Lucas[285], é a fotografia de um “tensionamento” entre a discricionaridade durante a gestão e a responsabilidade sobre seus atos[286].

Em análise à lei das sociedades anônimas brasileiras houve ampliação dos deveres e condutas de adoção desejada aos administradores[287]. Os deveres foram elencados em seção específica, designando: dever de diligência[288]; exercício dos interesses da companhia e satisfação de exigências do bem público e da função social da empresa[289]; dever de lealdade[290]; dever de sigilo[291]; dever de não atuar em

---

[285] LUCAS, *op. cit.*, p. 132-134.

[286] Há aqui a presença do *business Judgment rule*, considerado como um padrão para a análise judicial, que estabelece a presunção de que os administradores atuaram de forma independente e com nível informacional adequado. *Cf.* COELHO, *op. cit.*, p. 274; COELHO, Fábio Ulhoa. A natureza subjetiva da responsabilidade civil dos administradores de companhia. **Revista de Direito de Empresa**, v. 1, n. 1, 1996, p. 247-248.

[287] Cabe destacar que, na exposição dos motivos da Lei das S/As, ressaltou-se o quanto a inspiração dos comportamentos esperados e as respectivas responsabilidades do Decreto-Lei 2.627, de 26 de setembro de 1940, norma que dispunha sobre as sociedades por ações. Especificadamente aqui, no artigo 116, parágrafo 7º. No entanto, a mencionada norma trazia ao escopo dos diretores das Companhias por ações.

[288] “Art. 153. O administrador da companhia deve empregar, no exercício de suas funções, o cuidado e diligência que todo homem ativo e probo costuma empregar na administração dos seus próprios negócios”. *Cf.* BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**.

[289] “Art. 154. O administrador deve exercer as atribuições que a lei e o estatuto lhe conferem para lograr os fins e no interesse da companhia, satisfeitas as exigências do bem público e da função social da empresa.

§ 1º O administrador eleito por grupo ou classe de acionistas tem, para com a companhia, os mesmos deveres que os demais, não podendo, ainda que para defesa do interesse dos que o elegeram, faltar a esses deveres.

§ 2° É vedado ao administrador:

a) praticar ato de liberalidade à custa da companhia;

b) sem prévia autorização da assembleia-geral ou do conselho de administração, tomar por empréstimo recursos ou bens da companhia, ou usar, em proveito próprio, de sociedade em que tenha interesse, ou de terceiros, os seus bens, serviços ou crédito;

c) receber de terceiros, sem autorização estatutária ou da assembleia-geral, qualquer modalidade de vantagem pessoal, direta ou indireta, em razão do exercício de seu cargo.

§ 3º As importâncias recebidas com infração ao disposto na alínea c do § 2º pertencerão à companhia.

§ 4º O conselho de administração ou a diretoria podem autorizar a prática de atos gratuitos razoáveis em benefício dos empregados ou da comunidade de que participe a empresa, tendo em vista suas responsabilidades sociais”. *Cf. Ibid.*

[290] “Art. 155. O administrador deve servir com lealdade à companhia e manter reserva sobre os seus negócios, sendo-lhe vedado:

I - Usar, em benefício próprio ou de outrem, com ou sem prejuízo para a companhia, as oportunidades comerciais de que tenha conhecimento em razão do exercício de seu cargo;

II - Omitir-se no exercício ou proteção de direitos da companhia ou, visando à obtenção de vantagens, para si ou para outrem, deixar de aproveitar oportunidades de negócio de interesse da companhia;

III - adquirir, para revender com lucro, bem ou direito que sabe necessário à companhia, ou que esta tencione adquirir”.

[291] “§ 1º Cumpre, ademais, ao administrador de companhia aberta, guardar sigilo sobre qualquer informação que ainda não tenha sido divulgada para conhecimento do mercado, obtida em razão do cargo e capaz de influir de modo ponderável na cotação de valores mobiliários, sendo-lhe vedado valer-se da informação para obter, para si ou para outrem, vantagem mediante compra ou venda de valores mobiliários.

conflito de interesses[292]; dever de informar[293].

Nesse quadro, Egberto Teixeira e José Guerreiro trouxeram a comento o dever de diligência como sendo um “dever fiduciário básico”[294] ao exercício da

---

§ 2º O administrador deve zelar para que a violação do disposto no § 1º não possa ocorrer através de subordinados ou terceiros de sua confiança.
§ 3º A pessoa prejudicada em compra e venda de valores mobiliários, contratada com infração do disposto nos §§ 1° e 2°, tem direito de haver do infrator indenização por perdas e danos, a menos que ao contratar já conhecesse a informação.
§ 4o É vedada a utilização de informação relevante ainda não divulgada, por qualquer pessoa que a ela tenha tido acesso, com a finalidade de auferir vantagem, para si ou para outrem, no mercado de valores mobiliários”. *Cf. Ibid.*

[292] “Art. 156. É vedado ao administrador intervir em qualquer operação social em que tiver interesse conflitante com o da companhia, bem como na deliberação que a respeito tomarem os demais administradores, cumprindo-lhe cientificá-los do seu impedimento e fazer consignar, em ata de reunião do conselho de administração ou da diretoria, a natureza e extensão do seu interesse.
§ 1º Ainda que observado o disposto neste artigo, o administrador somente pode contratar com a companhia em condições razoáveis ou equitativas, idênticas às que prevalecem no mercado ou em que a companhia contrataria com terceiros.
§ 2º O negócio contratado com infração do disposto no § 1º é anulável, e o administrador interessado será obrigado a transferir para a companhia as vantagens que dele tiver auferido”. *Cf. Ibid.*

[293] "Art. 157. O administrador de companhia aberta deve declarar, ao firmar o termo de posse, o número de ações, bônus de subscrição, opções de compra de ações e debêntures conversíveis em ações, de emissão da companhia e de sociedades controladas ou do mesmo grupo, de que seja titular. (Vide Lei nº 12.838, de 2013)
§ 1º O administrador de companhia aberta é obrigado a revelar à assembleia-geral ordinária, a pedido de acionistas que representem 5% (cinco por cento) ou mais do capital social:
a) o número dos valores mobiliários de emissão da companhia ou de sociedades controladas, ou do mesmo grupo, que tiver adquirido ou alienado, diretamente ou através de outras pessoas, no exercício anterior;
b) as opções de compra de ações que tiver contratado ou exercido no exercício anterior;
c) os benefícios ou vantagens, indiretas ou complementares, que tenha recebido ou esteja recebendo da companhia e de sociedades coligadas, controladas ou do mesmo grupo;
d) as condições dos contratos de trabalho que tenham sido firmados pela companhia com os diretores e empregados de alto nível;
e) quaisquer atos ou fatos relevantes nas atividades da companhia.
§ 2º Os esclarecimentos prestados pelo administrador poderão, a pedido de qualquer acionista, ser reduzidos a escrito, autenticados pela mesa da assembleia, e fornecidos por cópia aos solicitantes.
§ 3º A revelação dos atos ou fatos de que trata este artigo só poderá ser utilizada no legítimo interesse da companhia ou do acionista, respondendo os solicitantes pelos abusos que praticarem.
§ 4º Os administradores da companhia aberta são obrigados a comunicar imediatamente à bolsa de valores e a divulgar pela imprensa qualquer deliberação da assembleia-geral ou dos órgãos de administração da companhia, ou fato relevante ocorrido nos seus negócios, que possa influir, de modo ponderável, na decisão dos investidores do mercado de vender ou comprar valores mobiliários emitidos pela companhia.
§ 5º Os administradores poderão recusar-se a prestar a informação (§ 1º, alínea e), ou deixar de divulgá-la (§ 4º), se entenderem que sua revelação porá em risco interesse legítimo da companhia, cabendo à Comissão de Valores Mobiliários, a pedido dos administradores, de qualquer acionista, ou por iniciativa própria, decidir sobre a prestação de informação e responsabilizar os administradores, se for o caso.
§ 6º Os administradores da companhia aberta deverão informar imediatamente, nos termos e na forma determinados pela Comissão de Valores Mobiliários, a esta e às bolsas de valores ou entidades do mercado de balcão organizado nas quais os valores mobiliários de emissão da companhia estejam admitidos à negociação, as modificações em suas posições acionárias na companhia”. *Cf. Ibid.*

[294] TEIXEIRA, Egberto Lacerda; GUERREIRO, José Alexandre Tavares. **Das sociedades anônimas no direito brasileiro**. São Paulo: Editora José Bushatsky, 1979. p. 470-471.

administração de uma sociedade. Há também o reconhecimento da característica de ampla abrangência na atuação.

Ampliando as percepções acerca do dever de diligência, há o entendimento que esses não somente devem ser íntegros e honestos, mas também saber alocar riscos à medida de suas informações[295].

Dada a relevância quanto ao atendimento ao dever de diligência e considerando o Código Civil de 2002 como a norma que substituiu parcialmente o Código Comercial, há também disposição acerca do tema, alocado no artigo 1.011, que diz: “O administrador da sociedade deverá ter, no exercício de suas funções, o cuidado e a diligência que todo homem ativo e probo costuma empregar na administração de seus próprios negócios”[296].

Sobre a expressão “cuidado”, que não constava no Código Comercial de 1850 e no Decreto-lei 2627/1940, Carvalhosa advém de inspiração ao *stand of care* da doutrina norte-americana, ampliando para que haja cobertura de possíveis outras formas de inobservância às obrigações dos administradores, para além das elencadas na norma[297].

Ao todo sobre as definições em norma e, em análise à Lei das Sociedades Anônimas e Código Civil, não há um rol taxativo sobre quais sejam as atividades exercidas como necessárias para o atendimento ao dever de diligência.

Portanto, cabe aos intérpretes, durante as etapas de investigação ou defesa que recaiam sobre determinado administrador, comprovar ou não o atendimento ao dever de diligência. Aqui há um exercício hermenêutico[298].

Inclusive, reforça-se a necessidade de entendimento sobre cada cenário, dadas as diferentes estruturas de sociedades anônimas, ramo de atuação, quantidade de colaboradores, valores internos e de mercado, bem como objetivos corporativos. É quanto a esse aspecto que Ana Frazão muito bem elucida que é preciso considerar as diferentes posições dos administradores – conforme o contido no estatuto –, sendo esse um ponto relevante para a análise do atendimento ao

---

[295] CASTRO, Rodrigo Monteiro. Parametrização do dever de diligência. *In*: COELHO, Fábio Ulhoa (Coord.). **Lei das sociedades anônimas comentada**. Rio de Janeiro: Forense, 2021. p. 874.
[296] BRASIL. **Lei 10.406, de 10 de janeiro de 2002. Código Civil**.
[297] CARVALHOSA, *op. cit.*, p. 264-266.
[298] *Ibid.*, p. 267.

dever de diligência[299].

Na mesma esteira, Nelson Eizirik exemplifica o fato de que não se pode adotar as mesmas exigências aos diretores e conselheiros de administração, considerando as diferentes características e atribuições de cada função[300].

Assim sendo, o atendimento ao dever de diligência preconiza a reunião de elementos capazes de demonstrá-lo em cenários reais. Daí surgem outros deveres atrelados à cláusula geral[301].

O primeiro consiste no dever de informar-se, ponto necessário para a tomada de decisão zelosa, empenhada e cuidadosa, não somente tendo como base a questão da urgência, dos fatos e circunstâncias, mas também acrescidos de conhecimento prévio e em grau ótimo de racionalidade, assim como notório saber sobre a estrutura empresária, realidade da companhia, objetivos institucionais, mercado em que está inserido e nicho de atuação[302].

Sobre isso, Flávia Parente[303] acrescenta a relevância de se conhecer as políticas institucionais e, ainda, os riscos e dificuldades presentes na organização.

Aqui, em análise ao objeto da pesquisa, resta evidente que, caso a empresa seja altamente dependente de tecnologia, já tenha mensurado riscos de ciberataques, tenha conhecimento da realidade global sobre ataques por *ransomware* ou, sabendo que a empresa tem dificuldades relacionadas à tecnologia, é inegável o dever de se informar para alocar decisões efetivas, como forma de mitigar riscos e agir com diligência para manter a perenidade da organização.

Claro que, como mencionado por Lucas, citando Renato Ventura Ribeiro, compreende-se a necessidade de tempo para a aquisição de conhecimentos a respeito da organização empresária, considerando aqui o caráter por vezes intermitente da atuação no bojo administrativo de companhias abertas de ramos e

---

[299] FRAZÃO, Ana. **Função social da empresa**: Repercussões sobre a responsabilidade civil de controladores e administradores de S/As. Rio de Janeiro: Editora Renovar, 2011. p. 354-355.
[300] EIZIRIK, Nelson. **A lei das S/A comentada**. 2. ed. São Paulo: Editora Quartier Latin, 2015. p. 116.
[301] No trabalho sobre programa de integridade nas sociedades anônimas, Lais Machado Lucas aborda a característica de cláusula geral do dever de diligência, isso porque o dever é verificado em casos concretos. Ainda, complementa: “Acredita-se que a cláusula geral do dever de diligência se concretiza criando novos deveres jurídicos”, ou seja, novos deveres oriundos da própria generalidade da cláusula. *Cf.* LUCAS, *op. cit.*, p. 143.
[302] LUCAS, *Ibid.*, p. 143.
[303] PARENTE, Flavia. **O dever de diligência dos administradores das sociedades anônimas**. Rio de Janeiro. Editora Renovar, 2005. p. 113-114.

estruturas distintas[304].

Quanto ao nível informacional, tecendo breves comentários sobre análise econômica do direito[305], Oksandro Gonçalves define que “o processo de escolha é orientado pela quantidade de informações disponíveis”. Incorporando alguns dos conceitos de análise econômica do direito, o autor aborda a existência de duas categorias de obtenção de informação, ou seja, grau completo e grau ótimo de informação. A primeira delas está inserida na obtenção de todas as informações disponíveis sobre determinada questão. Já o grau ótimo consiste no alcance das informações necessárias para a tomada da decisão[306].

Nessa toada, claramente não se exige postura em busca de níveis completos de informação, mas sim na quantidade e qualidade necessária de informação para se bem fundamentar a decisão.

Luiz Antonio de Sampaio Campos[307] aduz a respeito do grau informacional, devendo ser equilibrada ao que se exigiria em outra situação similar e que pela falta de alguma informação não se indicie eventual negligência.

Junto ao dever de informar-se, há o dever de qualificar-se, muito embora a Lei das Sociedades Anônimas não tenha em seu bojo essa característica, dada a evolução social – destaca-se a sociedade tecnológica –, não é mais aceitável pelo mercado e pelos investidores o exercício da administração por pessoa sem o desenvolvimento de competências inerentes à administração de uma empresa.

Imperioso aqui reconhecer a necessidade de transparência do administrador ao assumir necessidade de auxílio específico e técnico sobre determinado tema ou avaliar suas competências pessoais e decidir por investir o cargo, assumindo eventuais responsabilizações por falta de diligência ou, ainda, denegar o posto[308].

Também resta presente os deveres fiscalizatórios, investigatórios e o dever de intervir quando comprometida a integridade da companhia anônima.

Acerca desses, o dever geral de vigilância[309], abarcando a fiscalização,

---

[304] *Cf.* LUCAS, *op. cit.*, p. 143; RIBEIRO, Renato Ventura. **Dever de diligência dos administradores de sociedades**. São Paulo: Editora Quartier Latin, 2006.
[305] Não objetivando o esgotamento do tema, indica-se a seguinte leitura *Cf.* GICO JR, *op. cit.*
[306] GONÇALVES, *op. cit.*, p. 12.
[307] CAMPOS, Luiz Antonio de Sampaio. Deveres e responsabilidades. *In*: LAMY FILHO, Alfredo; PEDREIRA, José Luiz Bulhoes. **Direito das Companhias**. Rio de Janeiro: Editora Forense, 2017. p. 805-807.
[308] *Ibid.*, p. 803-804.
[309] *Ibid.*, p. 806-807.

investigação e interferência, relaciona-se com a relevância sobre os administradores manterem um monitoramento contínuo sobre a empresa, frisando, por exemplo, o desempenho de áreas, rendimento de atividades, desenvolvimento de projetos, busca por resultados ou vigilância sobre o aspecto regulatório atinente à atividade desenvolvida pela empresa.

A título de exemplo, tem-se a companhia do ramo bancário, cuja atividade é diretamente regulada pelo Banco Central e Conselho Monetário Nacional. O descumprimento de determinados normativos do BACEN pode ensejar sancionamento que impeça o seguimento das atividades e a aplicação de altas multas, gerando impactos negativos na seara financeira.

Outrora, em entendimento doutrinário na linha de Ribeiro[310], o dever fiscalizatório não se deve portar tal qual um agente próprio para investigações, mas sim acompanhar todo um aspecto geral. Entende-se que somente casos de elevada desconfiança deverão seguir com análises mais aprofundadas, pois não gera o risco de desvio de função do administrador.

Anexo ao dever de fiscalização, há o dever de participação e assiduidade, deveres que são parte das rotinas do administrador que, para desenvolver os demais deveres e funções, possui como demanda a participação das atividades empresárias. Tem-se então a participação em reuniões, visitas, contato com colaboradores, análise de relatórios e apresentações, dentre outras atividades específicas ao ramo de atuação da sociedade anônima[311].

Por fim, concernente aos fatores que compõem o dever de diligência, há o dever de bem administrar, em decorrência, não cometer erros grosseiros. Acerca desses, as próprias terminações cunhadas refletem o objetivo, que é envidar os melhores esforços para exercer um bom papel de administração, além de tomar precaução para não cometer erros que possam facilmente expor a empresa a uma situação de crise.

Como vislumbrado por Lucas, o dever de bem administrar não depende do sucesso ou insucesso de uma decisão negocial[312], mas do caminho percorrido pelo administrador sobre determinada decisão, realizando a ligação pelos demais deveres, justamente pela rota informacional, fiscalizatória, ponto qualificatório

[310] RIBEIRO, *op. cit.*, p. 226.
[311] CAMPOS, *op. cit.*, p. 807-809.
[312] LUCAS, *op. cit.*, p. 150.

exigido e nível de presença nas rotinas da companhia[313].

Os pontos de responsabilização serão medidos no próximo tópico, no entanto, aqui o dever de não cometer erros graves já exprime ponto crucial ao atendimento ao dever de diligência. O subjetivismo da análise não abraça situações de omissão, ações dolosas, negligência, imprudência ou imperícia, as quais tendem a ensejar situações de crise à perenidade da organização.

Em comento aos deveres supracitados, cabe destacar o dever de ação em zelo, dedicação, cautela e atenção, além do princípio intrínseco e indissociável da boa-fé. Todavia, não se exclui o assentimento aos riscos atinentes à empresa, independente de seu grau. É inerente ao exercício da administração.

Para tanto, resta aqui uma obrigação de meio pelo administrador[314], dada a impossibilidade de determinar que as decisões dos administradores sempre resultarão impactos positivos, cujo fito consiste na maximização dos resultados[315]. Há uma frequente análise probabilística, com base em coeficientes empregados pelo nível de informação e capacitação desses.

Conclui-se previamente que o dever de diligência estará sempre atrelado ao contexto dos riscos e especificidades que a sociedade aberta esteja imbuída, cujas movimentações do mercado, economia e sociedade tornam a acomodação ou conformação inviável, dado o surgimento contínuo de externalidades negativas ou não. Não se exclui, também, a recorrente evolução social, principalmente quanto ao emprego de TICs.

É nesse sentido que Ricardo Lupion e Evaldo Osorio Hackmann[316], ao

---

[313] Seguindo a mesma linha, Ana de Oliveira entende “deste dever: (i) o dever de aquisição de competência técnica adequada às suas funções; (ii) o dever de obtenção do conhecimento sobre a atividade da sociedade (o que envolve a aquisição e análise crítica da mesma e a implementação de sistemas de gestão de riscos, sistemas de controlo interno e sistemas de auditoria interna [...]); (iii) o dever de disponibilidade (obrigação de orientação do tempo e energia do administrador à promoção do fim ou interesse da sociedade); a estes deveres acrescenta-se (iv) o dever de atuar segundo critérios de racionalidade empresarial (art. 72º/2)". *Cf.* OLIVEIRA, Ana Perestrelo de. **Manual de governo das sociedades**. Coimbra: Almedina, 2017. p. 233-234; ABREU, Jorge Manuel Coutinho de. Deveres de cuidado e de lealdade dos administradores e interesse social. *In*: Instituto de Direito das Empresas e do Trabalho (Org.) **Reformas do Código das Sociedades**. Coimbra: Almedina, 2007.

[314] Sobre a discussão acerca da obrigação dos administradores, *Cf.* SACRAMONE, Marcelo Barbosa. **Administradores de sociedades anônimas**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Comercial. Fábio Ulhoa Coelho, Marcus Elidius Michelli de Almeida (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

[315] COOTER, Robert; Ulen, Thomas. **Direito e Economia**. Trad. Luis Marcos Sander e Francisco Araújo da Costa. 5. ed. Porto Alegre: Bookman, 2010. p. 37.

[316] LUPION; HACKMANN, *op. cit.*, p. 1445-1473.

tratarem de forma específica da cibersegurança e o dever de diligência do administrador, suscitam boas práticas de governança corporativa como fatores chaves ao atendimento da responsabilidade corporativa, e, nessa perspectiva, “[a] responsabilidade corporativa (*corporate liability*) guarda relação com sustentabilidade do negócio, com a viabilidade econômica e financeira, numa palavra, com a continuidade da empresa”[317].

Em rota conclusiva, entenderam que há demanda sobre conhecimento em segurança da informação, devendo partir dos administradores decisões a respeito de ações mitigadoras, como políticas[318].

Por fim, encerraram na defesa da presença da cibersegurança como solução jurídica à governança corporativa, devendo, portanto, partir do cerne estratégico da organização, decisões cabíveis pelos administradores no exercício de suas funções, atendendo ao dever de diligência[319].

A completude da pesquisa até o tópico em comento extrai, em síntese, a correlação entre a sociedade em rede e as consequentes exposições no ciberespaço, desencadeando possíveis riscos de ataque por *ransomware* ou outras metodologias de ciberataque.

Como evidenciado nos casos do capítulo anterior, grandes companhias sofreram paralisações operacionais, danos de valorização e imagem, queda de ações na bolsa e perdas financeiras que, em destaque o caso da JBS, não houve identificação e publicação de todas as perdas resultantes do ataque.

Em confronto com as bases do dever de diligência, impera-se pela indissociabilidade entre a adoção de condutas voltadas à cibersegurança e a proteção de dados com o respectivo atendimento ao dever de diligência dos administradores de sociedades anônimas de capital aberto.

Resta evidente e necessária a composição desses pontos ao dever de diligência para a manutenção da condição perene da organização que, muito embora reconheça o caráter de obrigação de meio pelos administradores, conclui que a ausência ou maltrato a pontos de TICs deixam portas vulneráveis a impactos imprevisíveis à organização, mas que “invisíveis” tendem a gerar impactos negativos severos à organização.

---

[317] *Ibid.*, p. 1454.
[318] *Ibid.*, p. 1455.
[319] *Ibid.*, p. 1468.

Para tanto, em casos práticos – a medida do fato, estrutura corporativa e resultados negativos –, se constatada a ausência de conduta diligente e proba por parte dos administradores ou de um deles, seja por ausência de informação, presença ou erro grave, haverá análise das responsabilidades e consequente invocação dos instrumentos responsabilizadores existentes no direito brasileiro.

Como sequência, objetiva-se demonstrar a possibilidade preditora quanto à instauração de procedimentos face aos administradores, para consequente reparação de danos causados. Logo, o papel da CVM é fundamental para a invocação dos direitos dos acionistas, bem como a redução de efeitos negativos ao mercado e à economia.

4.2 RESPONSABILIDADE POR CULPA, DOLO, VIOLAÇÃO DE LEI OU ESTATUTO DOS ADMINISTRADORES

Não há um rol taxativo sobre situações ou fatores que desencadeiam o descumprimento ao dever de diligência, o ponto chave é a interpretação sobre o descumprimento de preceitos de atividade e probidade na administração dos negócios.

De forma mais específica, Coelho[320] assevera que

> [...] é aquele que emprega na condução dos negócios sociais as cautelas, métodos, recomendações, postulados e diretivas da "ciência" da administração de empresas. O dever de diligência, portanto, correspondente a obrigações de meio e não de resultado.

Portanto, os descumprimentos e eventuais responsabilizações surgem a partir de uma ação ou omissão desfavorável ou contrária ao dever de diligência, ensejando prejuízos a outrem, seja à organização empresária, acionistas ou sociedade em sentido amplo. Entende-se que os administradores são pessoas diretamente associadas à gestão da sociedade, objetivando o atingimento de metas e resultados, a medida das definições prévias e de acordo com sua produtividade e eficiência na tomada de decisões racionais.

No direito europeu e norte-americano, há o *business judgment rule*, cunhado

[320] COELHO, *op. cit.*, p. 253-254.

inicialmente nos Estados Unidos da América, ferramenta com descritivos basilares acerca dos princípios aplicáveis à tomada de decisões pelo órgão administrativo da sociedade anônima, com objetivo de respeitar a discricionaridade e liberdade decisória do administrador, desde que em boa-fé, devido a diligência e objetivando atendimento aos melhores interesses da organização[321].

Carvalhosa expressa que os administradores praticam atos de gestão e, dentro das decisões sobre as práticas, deve refletir sobre a não ultrapassagem de limites que seguramente não tomaria em sua rotina ou o descumprimento de atos legais ou contratuais – inclusive dispostos no estatuto – por mera liberalidade e argumento de sua gestão [322].

Entende-se a necessidade de responsabilização civil nos casos em que haverá a obrigação de reparar um dano, quando um ou mais administradores da sociedade violam norma ou acordos legais, como contratos[323].

Já é claro na esfera civil que se uma ação ou omissão causar danos a outrem, a causadora terá obrigação de repará-los[324]. Portanto, se durante o exercício de administração da sociedade o administrador não agir com diligência, transparência, lealdade e/ou descumprir com o estabelecido em lei ou estatuto, terá a responsabilidade e obrigação de reparar impactos negativos causados[325].

De acordo com o artigo 158 da Lei 6.404/1976, o administrador não é responsável pelas obrigações que contrair em nome da sociedade ou por meio de um ato regular de gestão[326].

Extrai-se do texto legal que o administrador será responsável civilmente pelos danos ou prejuízos causados, quando, ainda que dentro das suas atribuições, nos casos em que agir de forma culposa ou dolosa, violar lei ou estatuto social[327].

A responsabilidade do administrador é majoritariamente defendida pela

---

[321] "[...] o simples prejuízo não faz o administrador responsável; deve-se provar que o administrador praticou um ato inadmissível ao padrão do homem comum - que não o praticaria em semelhantes condições". *Cf.* SILVA, Alexandre Couto. **Responsabilidade dos Administradores de S.A.** – Business Judgment Rule. Rio de Janeiro: Elsevier, 2007. p. 141-142.
[322] CARVALHOSA, *op. cit.*, p. 138.
[323] DINIZ, Maria Helena. **Curso de direito civil brasileiro: direito de empresa**. São Paulo: Editora Saraiva, 2023. p. 63-64; 154-155.
[324] COELHO, *op. cit.*, p. 37-38.
[325] *Ibid.*, p. 37-38.
[326] BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**.
[327] *Ibid.*

doutrina, como subjetiva[328], devendo-se comprovar, além da ligação entre o evento danoso e a culpa, a culpa ou o dolo do administrador ou a violação de lei ou do estatuto social que possa ter ensejado dano. É necessária então a demonstração e constatação dos elementos de culpa ou dolo, bem como o nexo causal entre a ação ou a omissão e o dano sofrido[329].

Nos casos em que se analisa tão somente o nexo entre dano e conduta sem considerar eventual conduta dolosa, presumirá-se a culpa do administrador ofensor[330].

Não sendo objetivo do presente tópico esgotar as diversas classificações acerca da responsabilidade, destaca-se a existência da responsabilidade extracontratual e contratual. No campo extracontratual, extrai-se o contido no Art. 186 do Código Civil de 2002 sobre reparação civil[331].

Na mesma linha, a Lei das Sociedades Anônimas dispõe especificamente da responsabilização do administrador no Art. 158[332], imputando responsabilização civil quando houver ação ou omissão em culpa ou dolo e em violação à lei ou ao estatuto.

---

328 COELHO, *op. cit.*, p. 15-38.

329 *Ibid.*

330 CARVALHOSA, *op. cit.*, p. 311.

331 "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito". *Cf.* BRASIL. **Lei 10.406, de 10 de janeiro de 2002. Código Civil**.

332 "Art. 158. O administrador não é pessoalmente responsável pelas obrigações que contrair em nome da sociedade e em virtude de ato regular de gestão; responde, porém, civilmente, pelos prejuízos que causar, quando proceder:
I - Dentro de suas atribuições ou poderes, com culpa ou dolo;
II - Com violação da lei ou do estatuto.
§ 1º O administrador não é responsável por atos ilícitos de outros administradores, salvo se com eles for conivente, se negligenciar em descobri-los ou se, deles tendo conhecimento, deixar de agir para impedir a sua prática. Exime-se de responsabilidade o administrador dissidente que faça consignar sua divergência em ata de reunião do órgão de administração ou, não sendo possível, dela dê ciência imediata e por escrito ao órgão da administração, no conselho fiscal, se em funcionamento, ou à assembleia-geral.
§ 2º Os administradores são solidariamente responsáveis pelos prejuízos causados em virtude do não cumprimento dos deveres impostos por lei para assegurar o funcionamento normal da companhia, ainda que, pelo estatuto, tais deveres não caibam a todos eles.
§ 3º Nas companhias abertas, a responsabilidade de que trata o § 2º ficará restrita, ressalvado o disposto no § 4º, aos administradores que, por disposição do estatuto, tenham atribuição específica de dar cumprimento àqueles deveres.
§ 4º O administrador que, tendo conhecimento do não cumprimento desses deveres por seu predecessor, ou pelo administrador competente nos termos do § 3º, deixar de comunicar o fato a assembleia-geral, tornar-se-á por ele solidariamente responsável.
§ 5º Responderá solidariamente com o administrador quem, com o fim de obter vantagem para si ou para outrem, concorrer para a prática de ato com violação da lei ou do estatuto". *Cf.* BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**.

Amplia, ainda, nos casos de conveniência, conivência ou negligência ao descobrir condutas de outros administradores. Por fim, especialmente às sociedades abertas, haverá responsabilidade solidária quando os administradores tiverem atribuições específicas de cumprimento a determinados deveres, conforme definição em estatuto ou nos casos em que, havendo conhecimento sobre eventual descumprimento pelo predecessor ou o administrador competente, não comunicar à assembleia-geral.

Também nos artigos 245 e 246 reflete-se sobre as responsabilidades dos administradores e da sociedade controladora. Quando houver danos causados a outrem.

No campo da responsabilidade de natureza contratual, são invocados os acordos realizados entre as partes envolvidas na sociedade, incluindo acordos realizados em estatuto entre os administradores da companhia.

No campo da teoria subjetiva[333] da responsabilidade civil, suscita-se a máxima de que não se há responsabilidade sem a culpa – cunhada por Jean Domat, originando a frase "*pas de responsabilité sans faute"*.

Já aos olhares dos objetivistas, há funções de solidariedade e equidade que, portanto, não devem ensejar danos a outros e suas respectivas vertentes sociais, econômicas e culturais[334].

Incumbe destacar aqui a presença da imprudência, negligência e imperícia. Isso porque o administrador tem o dever de informar-se, qualificar-se, comunicar e vigiar. Intervir, ser assíduo, bem administrar e não cometer graves erros.

A inobservância de tais pontos, para Verçosa[335], gera a responsabilidade na esfera da negligência[336]. Importa declarar que, no mesmo texto mencionado, o autor reconhece a hipótese de gestão fraudulenta pela má intencionalidade do administrador, ultrapassando limites toleráveis de riscos. Vê-se, em suma, a presença de imprudência[337] ou imperícia[338] no mesmo cenário.

Por isso, a culpa *per si* é disposta em regra jurídica, seja normativa ou

---

[333] CAMPOS, 2017, *op. cit.*, p. 1219-1221.
[334] CARVALHOSA, 2003, *op. cit.*, p. 311-351.
[335] VERÇOSA, *op. cit.*, p. 454.
[336] Consiste na falta de atenção em determinada circunstância. *Cf.* VENOSA, Silvio de Salvo. **Direito Civil**. Responsabilidade Civil. 13. ed. São Paulo: Atlas, 2013. p. 554.
[337] Revela-se como a precipitação e falta de devido cuidado. *Cf. Ibid.*, p. 39; 342.
[338] Trata-se da falta de conhecimento adequado para bem tratar determinada situação. *Cf. Ibid.*, p. 553-554.

contratual, como anteriormente destacado do Código Civil e Lei das Sociedades Anônimas.

A seara da responsabilização não abrangerá as obrigações assumidas durante o exercício das funções de administração[339].

Analisando o campo de decisões sobre cibersegurança, entende-se haver dano quando, sabendo da ocorrência de ciberataque e riscos de exposição aos dados pessoais de clientes e colaboradores, o administrador nada delibera, deixando decisões de restauração e tratamento às expensas dos colaboradores de tecnologia da informação.

Em outro cenário, não haverá responsabilidade no caso em que, sabendo do ciberataque e riscos de exposição de dados pessoais, delibera sobre a contratação de recursos e consultoria para apoiar nas negociações de um ciberataque, mas que, mesmo com as negociações, comunicações ao mercado, ações de contenção de exposição de outros sistemas, retomada das operações, há a perda de históricos dos sistemas internos, com informações da companhia.

Como já foi demonstrado, a responsabilidade do administrador será subjetiva, ele não será responsável pelas obrigações que assumir em nome da sociedade no exercício de suas funções.

Em síntese, haverá responsabilidade dos administradores pelo desempenho de sua gestão, mas também no cumprimento das obrigações que a lei, o contrato social ou os estatutos impõem[340]. Salienta-se que a responsabilidade do administrador (aqui englobando conselho de administração e corpo diretivo) é questão de ordem pública, considerando o impacto de suas ações[341]. Portanto, não pode ser modificada por uma assembleia ou pelo estatuto, uma vez que o objetivo pessoal do administrador é prevenir atos ilícitos e reparar aos prejudicados os danos causados, mantendo as garantias que a lei e os estatutos sociais asseguram, atendendo aos deveres dispostos.

Noutra face, existem casos de isenção ou exclusão de responsabilidade do administrador, como nos casos de aprovação de contas apresentadas pelo administrador à assembleia. Se aprovadas as contas sem ressalvas, fica excluída a responsabilidade do administrador, excetuando-se, evidentemente, quando

[339] SACRAMONE, *op. cit.*, p. 119.
[340] COELHO, *op. cit.*, p. 127.
[341] SACRAMONE, *op. cit.*, p. 79.

constatar-se erro, dolo, fraude ou simulação ou for anulada a assembleia em que ocorreu a aprovação.

Na esfera judicial haverá decretação da exclusão da responsabilidade, via de regra, pelo juiz na ação de responsabilidade, quando ficar demonstrado que o administrador agiu de boa-fé e no melhor interesse da companhia, conforme descreve o art.159, §6º da Lei 6.4040 de 1976 (LSA)[342].

Como mencionado, se comprovada atitude dolosa ou culposa do administrador da sociedade anônima em qualquer caso, que resulte dano a outrem ou à própria sociedade, haverá o dever de repará-lo.

Vislumbra-se a aplicabilidade de responsabilização em contextos e cenários associados à cibersegurança ou, dito de outro modo, ciberataques. No entanto, restará necessário evidenciar a ausência de conduta por negligência, imprudência ou perícia, bem como por ação dolosa por má-fé, conflito de interesses, dentre outros.

Identifica-se, nos casos acima destacados, o possível descumprimento do atendimento ao dever de diligência, pela ausência somada dos elementos basilares ao dever de diligência, como se informar, comunicar, vigiar e não cometer erros graves.

Considerando o aumento de ciberataques, níveis aprimorados de pedido de resgate, casos de crises internas por ataques de *ransomware* evidenciados – assim como em estândares, diretrizes nacionais e internacionais, materiais disponíveis para conhecimento acerca de *ransomware* e boas práticas –, verifica-se que a ausência de decisões preventivas ou corretivas sobre o tema e a negligência quanto à busca de informação, vigilância e assiduidade são capazes de gerar responsabilizações aos administradores, conforme os danos causados por suas atitudes ou falta delas.

Para tanto, existem meios de invocação das responsabilidades ou ressarcimento de direitos, ponto de fechamento da pesquisa no próximo item.

4.3 NATUREZA DAS SANÇÕES E PROCEDIMENTOS PARA A RESPONSABILIZAÇÃO DO ADMINISTRADOR

[342] BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**.

Ao campo dos procedimentos e responsabilizações cabíveis, tem-se a modalidade pela esfera civil e pela esfera administrativa[343].

4.3.1 Natureza das sanções na esfera administrativa

Há possibilidade de instauração de processo administrativo sancionado pela CVM. Nesse caso, o objetivo é apurar, investigar e julgar ações que lesionam ou contrariam as normas do mercado imobiliário brasileiro[344].

Como anteriormente mencionado, a CVM é a entidade autárquica competente para dispor de regras disciplinares, exercer fiscalização e regulamentar o mercado de capitais no Brasil. Para isso, exerce o papel de polícia administrativa, visando atender seus deveres, supervisionando o mercado de valores mobiliários[345].

É parte indissociável da CVM a promoção de funcionamento eficiente e regular do mercado acionário, buscando assegurar o funcionamento eficiente e regular dos mercados, também protegendo os titulares de valores mobiliários e investidores do mercado.

A LSA[346] atribuiu à CVM[347] a competência para realizar apuração, julgamento e punição por irregularidades cometidas face ao mercado. Dada a fundada suspeita, há a possibilidade de abertura de inquérito administrativo, que busca informações e produz provas a fim de identificar eventuais práticas irregulares. Havendo indícios,

---

[343] Não se exclui outras possibilidades, como a via de responsabilização penal para casos de corrupção ativa, por exemplo, mas se destaca que esses demais casos não serão objeto da pesquisa. A título exemplificativo, o Ministério Público também pode requerer a responsabilização dos administradores em casos de operação fraudulenta, manipulação de preços ou criação de condições artificiais de procura, como a aquisição ou venda de valores mobiliários com base em informações privilegiadas. Além disso, como supramencionado o Ministério Público, seja estadual ou federal, pode-se promover uma Ação Civil Pública (com base na Lei 7.913/1989) perante o administrador, sem prejuízo à acumulação com ações anteriores, a fim de evitar ou reparar danos causados a investidores ou detentores de valores mobiliários.

[344] NORONHA, Ilene Patrícia. Os ritos procedimentais de competência da CVM. *In*: SIMÃO FILHO, Adalberto; LUCCA, Newton de (Coord.). **Direito Empresarial contemporâneo**. São Paulo: Juarez de Oliveira, 2004. p. 276; 278.

[345] *Ibid.*, p. 276; 278.

[346] BRASIL. **Lei 13.506, de 13 de novembro de 2017. Dispõe sobre o processo administrativo sancionador, 2017**.

[347] "Especialmente no que se refere ao processo administrativo sancionador (PAS), a Lei 6.385 estabelece em seu artigos 9º, incisos V e VI, que cabe à Autarquia apurar, mediante processo administrativo, atos ilegais e práticas não equitativas de administradores, membros do conselho fiscal e acionistas de companhias abertas, dos intermediários e dos demais participantes do mercado, assim como aplicar aos autores de tais infrações as penalidades previstas no artigos 11, sem prejuízo de eventual responsabilização civil ou penal". *Cf.* COMISSÃO DE VALORES MOBILIÁRIOS. **Relatório de atividade sancionadora – julho a setembro de 2023**.

oferece-se acusação, dispondo de direito de defesa. Em sequência ao processo, há a análise e julgamento em colegiado, com tramitação por meio de rito ordinário. Sobre os processos de rito sumário, é feita uma verificação direta pelos times técnicos da autarquia, com apreciação pelo colegiado[348].

Seguindo o rito para a aplicação de sanção e dosimetria da pena, são considerados o arrependimento eficaz e a confissão no cálculo da sanção a ser aplicada.

Por fim, ao processo administrativo sancionador, tem-se a possível aplicação de multa, não impossibilitando o ingresso a demais processos, como cíveis de reparação de danos ou criminais, a depender do ato praticado.

No cenário de incidência de ciberataques, se confirmada a adoção de postura dolosa ou culposa, que tenha posto em risco ou causado impactos negativos ao mercado, o administrador da sociedade empresária pode ser responsabilizado perante a CVM, tornando-se responsável ao pagamento de multa, além de demais possibilidades processuais em outras esferas, como o afastamento do cargo e reparação civil[349][350].

4.3.2 Procedimentos de responsabilidade em âmbito cível

O artigo 159 da Lei das Sociedades Anônimas (Lei 6.404/1976) é claro sobre

---

[348] COMISSÃO DE VALORES MOBILIÁRIOS. **Processos Sancionadores Julgados**.

[349] Como exemplo de processo administrativo sancionador, comenta-se sobre o caso envolvendo a Global Equity Administradora de Recursos S.A, condenada a pagar multa pecuniária na monta de quinhentos mil reais pela prática de operação fraudulenta.
EMENTA: Apuração de responsabilidades pela prática de operações fraudulentas no mercado de valores mobiliários (itens I e II, “c”, da Instrução CVM nº 8/1979); por descumprimento do dever de lealdade em gestão de fundo de investimento (art. 65- A, inciso I, da Instrução CVM n° 409/2004); e por descumprimento do dever de fiscalizar a prestação de serviços de terceiros contratados por fundo de investimento (art. 65, inciso XV, da Instrução CVM n° 409/2004). *Cf.* https://conteudo.cvm.gov.br/sancionadores/sancionador/2023/20230926_PAS_19957002026201930.html. Acesso em: 25 nov. 2023.

[350] “Apurar responsabilidade de ex-diretores financeiros da Companhia Paranaense de Energia S.A. – COPEL, por descumprimento dos artigos 153, 176 e 177 da Lei nº 6.404/76 pela não adoção de providências efetivas para reenquadrar os investimentos à política de investimentos da companhia e suas participações na elaboração ou aprovação das demonstrações financeiras anuais completas datas base 31.12.2014, 31.12.2015, 31.12.2016, 31.12.2017, em desacordo com as normas aplicáveis”. *Cf.* https://conteudo.cvm.gov.br/export/sites/cvm/sancionadores/sancionador/anexos/2023/SEI_19957009104_2019_27.pdf. Acesso em: 23 nov. 2023.

a ação de responsabilidade diante dos administradores da sociedade anônima[351].

O objetivo desse dispositivo legal insere-se na hipótese de recuperação de danos causados ao patrimônio da companhia, assim como também aos respectivos acionistas, sociedade e economia[352].

Uma ação pode ser proposta individualmente por um acionista ou terceiros prejudicados por atos do administrador da sociedade anônima de capital aberto (considerando o objeto da pesquisa).

A Lei das Sociedades Anônimas prevê duas modalidades, não excludentes, de ação de responsabilidade contra administradores, quais sejam, a ação social e a ação individual. A primeira pode ser movida pela própria sociedade empresária ou seus respectivos acionistas, devendo, no entanto, passar por assembleia geral prévia sobre o tema[353].

Nesses casos, existem as seguintes modalidades: a. deliberação em assembleia sobre a propositura da ação de responsabilidade – ação social *ut universi*[354]; b. deliberação em assembleia sobre a propositura da ação, havendo morosidade em prazo superior a três meses, possibilitando a realização por qualquer acionista da SA – ação social *ut singuli* derivada[355]; c. deliberação em assembleia no sentido de não propositura da ação, possibilitando ajuizamento por acionistas com ao menos 5% do capital – ação *ut singuli* originária[356].

---

[351] "Art. 159. Compete à companhia, mediante prévia deliberação da assembleia-geral, a ação de responsabilidade civil contra o administrador, pelos prejuízos causados ao seu patrimônio.
§ 1º A deliberação poderá ser tomada em assembleia-geral ordinária e, se prevista na ordem do dia, ou for consequência direta de assunto nela incluído, em assembleia-geral extraordinária.
§ 2º O administrador ou administradores contra os quais deva ser proposta ação ficarão impedidos e deverão ser substituídos na mesma assembleia.
§ 3º Qualquer acionista poderá promover a ação, se não for proposta no prazo de 3 (três) meses da deliberação da assembleia-geral.
§ 4º Se a assembleia deliberar não promover a ação, poderá ela ser proposta por acionistas que representem 5% (cinco por cento), pelo menos, do capital social.
§ 5° Os resultados da ação promovida por acionista deferem-se à companhia, mas esta deverá indenizá-lo, até o limite daqueles resultados, de todas as despesas em que tiver incorrido, inclusive correção monetária e juros dos dispêndios realizados.
§ 6° O juiz poderá reconhecer a exclusão da responsabilidade do administrador, se convencido de que este agiu de boa-fé e visando ao interesse da companhia.
§ 7º A ação prevista neste artigo não exclui a que couber ao acionista ou terceiro diretamente prejudicado por ato de administrador". *Cf.* BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**.

[352] CAMPINHO, *op. cit.*, p. 137-140.

[353] Ação social empresa ou acionistas

[354] PAES, *op. cit.*, p. 57-59.

[355] *Ibid.*

[356] CAMPINHO, *op. cit.*, p. 137-140.

Se houver intenção majoritária sobre o retardamento quanto à deliberação sobre o ingresso de ação de responsabilidade, cabe mencionar posição dominante da jurisprudência possibilitando ingresso direto pela ação *ut singuli* originária, caso destacado no item c[357].

Campinho[358] entende que a jurisprudência pátria de que há presunção de negação implícita, legitima os minoritários como capazes de propor a ação, em substituição aos demais casos e possíveis propositores.

Considera-se também caso de relativização do requisito da titularidade de pelo menos 5% do capital social para a propositura da ação no modo *ut singuli* originária[359].

Nos casos em que os controladores da sociedade anônima possuam mais de 95% do capital social da companhia, há a possibilidade de admissão de ingresso de ação sem carecer prévia deliberação em assembleia ou percentual mínimo acionário.

Tal entendimento objetiva possibilitar a propositura por grupos minoritários que sofreram danos à companhia, nos casos em que seja impossível exigir ou mensurar participação societária mínima, dados os riscos de desigualdade de tratamento, concessão ao direito de ingresso de ação ou, ainda, de pleitear reparação de danos[360].

Diferente à ação social, tem-se a ação individual, vista como meio no qual o acionista ou terceiros que sofreram danos por decisões proferidas pelos administradores poderão ajuizar para pleitear a respectiva reparação.

No caso em roga, prescinde-se de deliberação assemblear ou quórum acionário mínimo, isso porque os danos e reparações suscitadas são originados pelo próprio autor da ação que possa ter sofrido o dano. É individual e, portanto, não carece dos mesmos requisitos que o primeiro modo[361].

Em breve contextualização, eventuais decisões acerca de incidentes de cibersegurança ou das ações de segurança cibernética propriamente ditas, que acarretem danos, possuirão dois modos amplos de propositura de ação de reparação na esfera do direito e processo civil. Há possibilidade de ingresso através

---

357 *Ibid.*
358 PAES, *op. cit.*, p. 57-59.
359 *Ibid.*
360 CAMPINHO, *op. cit.*, p. 137-140
361 *Ibid.*

de requisitos prévios dentro da sociedade, assim como na modalidade individual aos afetados pela decisão em comento.

Quanto à responsabilidade, como mencionado, o artigo 158 da LSA trata sobre a responsabilidade do administrador em duas hipóteses, sendo a primeira delas consoante suas atribuições, mediante culpa ou dolo e, em segundo caso, pela violação de lei ou estatuto. Na esfera civil, haverá – se assim constatada – a obrigação de reparar os danos causados pelo ato ilícito perpetrado. Nesse caso, a responsabilidade civil é independente da invocação de outras esferas de responsabilização, como a criminal ou civil[362].

Em se tratando da responsabilidade a ser invocada ao administrador, tem-se a divergência de posições. Carvalhosa entende haver o caso de responsabilidade objetiva, em que há presunção de culpa[363]. Noutro lado, tem-se Coelho, que diz ser aplicável a responsabilidade subjetiva clássica[364]. Ainda, cabe mencionar posição doutrinária majoritária no sentido de reconhecimento de responsabilidade subjetiva com presunção de culpa[365].

Como anteriormente abordado, existem as modalidades de ingresso de ação na esfera civil, as quais demandarão análise judicial sobre os danos causados e a consequente extensão, assim determinando as medidas reparatórias adequadas ao caso[366].

---

[362] "[...] é a obrigação de reparar o dano resultante de um ato de que se é autor direto ou indireto". *Cf.* LOPES, Miguel Maria de Serpa. **Curso de Direito Civil**. Rio de Janeiro: Freitas Bastos, 1962. p. 187.

[363] CARVALHOSA, *op. cit.*, p. 368.

[364] COELHO, *op. cit.*, p. 260.

[365] Como abordado por Carvalhosa: "Com esse mesmo entendimento: Fábio Ulhoa Coelho, ob. cit., v. 2, p. 173; Tavares Borba, ob. cit., p. 434; Egberto Lacerda Teixeira e José Alexandre Tavares Guerreiro, ob. cit., v. 1, p. 164; Modesto Carvalhosa, Comentários à lei de sociedades anônimas, v. 3 (4ª ed. – 2009), p. 559-560. Em sentido contrário, ou seja, entendendo admissível o aumento do capital parcialmente subscrito: *Nelson* Eizirik. A lei das S/A comentada, v. II. São Paulo: Quartier Latin, 2011, p. 505; e Mauro Rodrigues Penteado. Aumentos de capital das sociedades anônimas, 2ª ed. São Paulo: Quartier Latin, 2012, p. 225".
A Comissão de Valores Mobiliários por bastante tempo esposou o entendimento de ser inadmissível a homologação de aumento de capital em bases diversas das originalmente estipuladas por ocasião de sua autorização (Parecer de Orientação CVM n. 8/1981). Ulteriormente, a posição foi reformulada para passar a admitir ser válido o aumento com insuficiência de subscrição, desde que prevista expressamente a possibilidade na deliberação do aumento e especificada a quantidade mínima de valores mobiliários ou o montante mínimo de recursos para os quais a oferta será mantida (arts. 30 e 31 da Instrução CVM n. 400/2003). Na decisão do Colegiado da Comissão de Valores Mobiliários, proferida no processo administrativo n. RJ2006/0214, relatado pelo Diretor Wladimir Castelo Branco Castro e julgado em 9-5-2006, entendeu-se que os mencionados arts. 30 e 31 também poderiam ser aplicados a aumentos de capital realizados mediante subscrição privada". *Cf.* CARVALHOSA, *op. cit.*, p. 203.

[366] Nesta linha, cita-se o seguinte julgado: AGRAVOS DE INSTRUMENTO. DECISÃO DE ARRESTO EM CONTA DE SÓCIO ADMINISTRADOR DE PESSOA JURÍDICA E DE AFASTAMENTO SUMÁRIO

Em resultado às demandas judiciais, pode-se ter a condenação ao pagamento de valores a título de reparação de danos, assim como em hipóteses de afastamento do administrador e a aplicação dos dispositivos da LSA sobre irregularidades envolvendo os órgãos da administração.

Ao todo, o que se compreende é na hipótese de ajuizamento de ação de reparação civil, reconhecendo-se a possibilidade de adoção de postura irregular, seja em dolo ou culpa, capaz de romper o *affectio societatis* entre os membros.

Em cotejo ao ambiente de cibercrimes, pode-se reconhecer a intenção em nada decidir sobre evento de ataque, bem como, se tendo fundada suspeita de algo, nada o faz, em razão de conflito de interesses com determinadas questões.

DELE DA ADMINISTRAÇÃO. QUEBRA DA AFFECTIO SOCIETATIS, DECORRENTE DA INJUSTIFICADA APROPRIAÇÃO DE ELEVADA QUANTIA QUE INTEGRAVA O CAPITAL DE GIRO DA SOCIEDADE. INEXISTÊNCIA DE PROVA DESCONSTITUTIVA DO DIREITO ALEGADO PELO AUTOR/AGRAVADO. DEVER DE DILIGÊNCIA NA CONDUÇÃO DOS NEGÓCIOS DA SOCIEDADE. VIOLAÇÃO DOS DEVERES IMPOSTOS AO ADMINISTRADOR. AUSÊNCIA DE JUSTIFICATIVA PLAUSÍVEL E EM RAZÃO DOS INTERESSES SOCIETÁRIOS PARA A REALIZAÇÃO DE SAQUE QUE IMPEDIRAM O ATENDIMENTO DAS OBRIGAÇÕES DA SOCIEDADE. INDÍCIOS DE ADMINISTRAÇÃO TEMERÁRIA. DECISÃO DE PRIMEIRO GRAU MANTIDA. RECURSO DESPROVIDO. O administrador da pessoa jurídica deve gerir a sociedade com o zelo e dever inerentes, com o bom senso do homem médio e a diligência que deferiria aos seus próprios negócios. A grave violação dos deveres societários, além disso, dá margem à quebra da affectio societatis, o que autoriza a tomada de medidas extremas, tal como o afastamento liminar do sócio da administração dos negócios, se necessário à manutenção da normalidade destes. (TJPR - 18ª Câmara Cível - 0009626-90.2021.8.16.0000 - Curitiba - Rel.: DESEMBARGADOR LUIZ HENRIQUE MIRANDA - J. 10.05.2021).

5 CONCLUSÃO

1. Percebe-se a sólida presença do paradigma *everyware* no contexto social, de modo que há a penetrabilidade da tecnologia nas diversas vertentes da sociedade, atravessando atividades básicas para subsistência, assim como o âmbito de ensino, trabalho e lazer;

2. Como reflexo de uma sociedade altamente voltada para a tecnologia, reconhece-se a incidência do cansaço digital, dado o cenário de volume e velocidade no curso das informações e conteúdo;

3. Nesse sentido, a sociedade faz uso de tecnologia em larga escala, ao ponto que um sujeito pode não se sentir pertencente à sociedade se não o fizer uso de recursos de tecnologia, sobretudo, redes sociais. Inclusive, as interações sociais hoje se baseiam na tecnologia;

4. Como resultado, tal qual muito bem abordado por Beck, há a presença da caracterização de uma sociedade de riscos que, paulatinamente, à medida de sua evolução e velocidade inovativa, enfrenta o surgimento de novos pontos de risco, e, ainda, consequências por vezes de probabilidade e impacto inestimáveis, como é o caso dos ciberataques;

5. Existindo a dependência tecnológica, impactos oriundos de crises envolvendo tecnologias colocam em xeque a integridade financeira, reputacional e operacional de uma entidade empresarial, ensejando indicativos de impacto à continuidade dos negócios empresariais e à sociedade na qual a empresa está inserida.

6. Diversas e nomináveis são as modalidades de ciberataque, como os ataques por *phishings, malwares* e o objeto da pesquisa, *ransomware.* Independente da modalidade, vê-se que o objetivo dos criminosos consiste na obtenção de vantagens indevidas por parte das vítimas, seja na utilização e comercialização de dados ou informações, na prática de atos de fraude por engenharia social ou, em um cenário mais elaborado, no pedido de pagamentos em criptomoedas, cuja rastreabilidade se torna difícil;

7. Na esteira dos estudos sobre conformidade e criminalidade, compreende-se que o fruto da prática de delitos no ciberespaço pode, inclusive, ser reconhecido como parte do fluxo de branqueamento de capitais, cotejando a

utilização dos recursos provenientes dos ataques ou em cenários de atenção global, na utilização para o financiamento e manutenção de organizações terroristas;

8. Junto a isso, há o fator econômico movido a dados. Nesse ponto, desde grandes corporações de tecnologia até pequenas empresas possuem no bojo de sua atuação o tratamento de dados pessoais;

9. Reconhece-se os diferentes motivadores sobre o tratamento de dados pessoais, os quais podem ser para fornecer produtos por meio de publicidade direcionada, para entendimento sobre perfis de consumo e simples operação de fornecimento de bens ou serviços;

10. Informações são utilizadas como composição da inteligência dos negócios, almejando entender o mercado atuante, a fim de empregar estratégias adequadas ao crescimento e perenidade de uma organização;

11. No Brasil, após a publicação e vigor da LGPD, o cenário de proteção de dados pessoais tomou relevante força, tornando essencial para toda organização a realização de adequações sobre seu tratamento, sobretudo aos sensíveis. Assim, impõe-se a adoção de metodologias de *privacy by design*;

12. A Ausência de mecanismos de proteção e de tratamento legal aos dados pessoais passa, portanto, a ser reprovável também pelo viés constitucional com a publicação da EC, que reconhece o tema como parte dos direitos e garantias fundamentais. A mesma emenda também atribuiu competência privativa da união para legislar sobre o tema;

13. Em análises aos casos apresentados no segundo capítulo, é possível destacar pontos de similaridade, como a modalidade de ataque e os pontos de fragilidade identificados e utilizados pelos cibercriminosos;

14. Outrora, cada companhia adotou medidas diferentes de gestão da crise, ações que tiveram o condão de corroborar ou agravar o cenário de crise. A título de exemplo, vê-se o cenário de transparência informacional da Renner em contraste com as incertezas sobre o ataque às Lojas Americanas;

15. Quanto ao caso da JBS, também restou evidente o esforço mundial e das entidades públicas, como o governo americano ao caso, sobre o combate aos cibercrimes e organizações criminosas;

16. Sobre as ações de contingenciamento do cenário de ataque, conclui-se que as principais medidas tomadas consistiram na interrupção dos demais sistemas,

almejando evitar que também fossem afetados pelo *ransomware*. Em seguida, adotaram procedimentos de recuperação de sistemas e informações por intermédio de *backups;*

17. Sobre o tópico acerca das boas práticas em segurança da informação, , cibersegurança, é notória a existência de práticas já consolidadas no mercado, resultando no dever de conhecer e se informar sobre tais problemas por parte não somente dos técnicos e especialistas em segurança e tecnologia da informação, mas também dos dirigentes e administradores das organizações. Não se olvidando, no entanto, na diferença entre pesos e medidas de conhecimento entre as mencionadas atribuições;

18. É imperioso o entendimento sobre padrões de conduta esperados dos administradores de sociedades anônimas, objetivando evidenciar o conhecimento sobre incidentes de tecnologia, ataques por *ransomware* e consequente adoção de ações de cibersegurança como fatores indissociáveis ao reconhecimento do atendimento do dever de diligência no contexto da sociedade tecnológica.

19. No que concerne aos padrões de conduta esperados, objeto do último capítulo, entende-se que medidas preventivas a ciberataques devem ser parte indissociável ao cumprimento do dever de diligência dos administradores de sociedades anônimas abertas, considerando indubitável a presença dessa categoria de risco no contexto social, ao fácil acesso à estândares de mercado aplicáveis;

20. Corroborando para uma adequada tomada de decisões, considera-se também a presença de tendências normativas relacionadas, como a Lei Geral de Proteção de Dados;

21. Por fim, considera-se que qualquer ausência ou razoabilidade de decisão oportuna e cabível demonstram falta para com os deveres de informar-se, qualificar-se, fiscalizar, intervir, participar, bem administrar e evitar erros grotescos, configurações básicas do dever de diligência, podendo agravar situações de crise por ataque *ransomware*, expondo a empresa, sociedade e o mercado à riscos;

22. Neste sentido, entende-se que cibersegurança na contemporaneidade é elemento de diligência dos administradores, as quais devem estar presentes dentro de suas obrigações, como a tomada de decisões razoáveis e cabíveis a cada momento (prevenção ou pós incidente);

23. Assim sendo, podem ser pleiteadas através da esfera civil, com o

ajuizamento de ação ou por meio de Processos Administrativos Sancionadores (PAS), pela CVM.

6 REFERÊNCIAS

ABREU, José Luis. Grandes patrocinadores. **Autosport**, 20 de março de 2024. Disponível em: https://www.autosport.pt/maismotores/grandes-patrocinadores-os-nomes-e-as-cores-da-nossa-memoria/. Acesso em: 9 abr. 2024.

ADAMEK, Marcelo Vieira Von. **Responsabilidade Civil dos Administradores de S/A e as ações correlatas**. São Paulo: Editora Saraiva, 2009.

AMERICANAS FORA do ar: prejuízo pode chegar a R$ 100 milhões por dia. **AGÊNCIA O GLOBO, Revista Exame**, 22 fev. 2022. Disponível em: https://exame.com/negocios/americanas-fora-do-ar-prejuizo-pode-chegar-a-r-100-milhoes-por-dia/. Acesso em: 9 abr. 2024.

ANTONIK, Luis Roberto. **Compliance, ética, responsabilidade social e empresarial: uma visão prática.** Rio de Janeiro: Alta Books, 2016.

ARBULO, Rafael. Ataque à JBS foi executado pelo grupo hacker REvil. **Olhar digital**, 4 jun. 2021. Disponível em: https://olhardigital.com.br/2021/06/04/seguranca/ataque-jbs-revil-ransomware/. Acesso em: 9 abr. 2024.

ASCARELLI, Tullio. Origem do Direito Comercial. Trad. Fabio Konder Comparato. *In*: **Revista de Direito Mercantil, Industrial, Econômico e Financeiro**. n. 114. São Paulo: Malheiros Editores, 1996.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27001**: Sistema e Gestão em Segurança da Informação. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27002**: Tecnologia da Informação, técnicas de segurança e código de prática para controles de segurança da informação. Rio de janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR – ISO/IEC 27005**: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio e janeiro, 2011.

BAUMAN, Zygmunt. **Vida para consumo**. Rio de Janeiro: Zahar, 2008.

BECK, Milton. **Emerging Jobs Report Brazil**. LinkedIn, 2020. 1 apresentação, 25 banners. Disponível em: https://bit.ly/3HsL4pq. Acesso em: 9 abr. 2024.

BECK, Ulrich. Sociedade de risco: Rumo a outra modernidade,2. ed. São Paulo: Editora 34, 2011.

BEVILACQUE, Rafael. Lucro da JBS em 2021 foi o maior da história da empresa; como ficam ações? **UOL**, 23 mar. 2022. Disponível em: https://shre.ink/8KcP. Acesso em: 9 abr. 2024.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. *In*: DONEDA, Danilo; MENDES, Laura; CUEVA, Ricardo (Org.). **Lei Geral de Proteção de Dados**. São Paulo: Thomson Reuters/Revista dos Tribunais, 2020.

BISSON, David. FBI Pegs 2020 Cybercrime Costs at $4 Billion – Actual Losses Likely Higher. **Cybereason**, 2021. Disponível em: https://bit.ly/42MmoSz. Acesso em: 31 ago. 2023.

BRASIL. **Emenda Constitucional Nº 115, de 10 de fevereiro de 2022**. Disponível em: https://bit.ly/3uthoFS. Acesso em: 16 mar. 2023.

BRASIL. **Lei 10.406, de 10 de janeiro de 2002. Código Civil.** Disponível em: https://bit.ly/3UNRNlK. Acesso em: 9 abr. 2024.

BRASIL. **Lei 12.965, de 23 de abril de 2014, Marco Civil da Internet, 2014**. Disponível em: https://bit.ly/49Gdwjz. Acesso em: 9 abr. 2024.

BRASIL. **Lei 13.506, de 13 de novembro de 2017. Dispõe sobre o processo administrativo sancionador, 2017**. Disponível em: https://bit.ly/3uDTqHQ. Acesso em: 9 abr. 2024.

BRASIL. **Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, 2018**. Disponível em: https://bit.ly/49kQa3i. Acesso em: 9 abr. 2024.

BRASIL. **Lei 6.404, de 15 de dezembro de 1976. Lei das Sociedades Anônimas**. Disponível em: https://bit.ly/3UPhCBJ. Acesso em: 9 abr. 2024.

BRASIL. **Lei 9.613, de 3 de março de 1988. Lei de Lavagem de Dinheiro, 1998**. Disponível em: https://bit.ly/49Hmg92. Acesso em: 9 abr. 2024.

BRASIL. **O que é a CVM?** Disponível em: https://bit.ly/3OO9MEx. Acesso em: 28 ago. 2023.

BRASIL. **Oficina Dirigida – Relatório de Impacto à Proteção de Dados Pessoais. Dezembro de 2020**. Disponível em: https://acesse.one/FaQiz. Acesso em: 9 abr. 2024.

BRAUN, Daniela. Lojas Renner aguarda análise de peritos para identificar origem de ciberataque. **Valor Investe**, 1 set. 2021. Disponível em: https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2021/09/01/lojas-renner-aguarda-analise-e-peritos-para-identificar-origem-de-ciberataque.ghtml. Acesso em: 9 abr. 2024.

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip; SHORT, Donald. **Cybersecurity Essentials**. 1st ed. Wiley: Sybex. 2018.

CAMPINHO, Sérgio. **Curso de direito comercial**: sociedade anônima. São Paulo: Editora Saraiva, 2023.

CAMPOS, Luiz Antonio de Sampaio. Deveres e responsabilidades. *In*: LAMY FILHO, Alfredo; PEDREIRA, José Luiz Bulhoes. **Direito das Companhias**. Rio de Janeiro: Editora Forense, 2017.

CARDOSO, Fernando Henrique. Prefácio. *In*: CASTELLS, Manuel. **A Sociedade em Rede**. Trad. Roneide Venancio Majer. 17. ed. São Paulo: Paz eTerra.

CARVALHOSA, Modesto. **Comentários à lei das sociedades anônimas**. 3. ed. São Paulo: Saraiva, 2003.

CASTELLS, Manuel. **A Sociedade em Rede**. Trad. Roneide Venancio Majer. 17. ed. São Paulo: Paz e Terra, 2016.

CASTRO, Rodrigo Monteiro. Parametrização do dever de diligência. *In*: COELHO, Fábio Ulhoa (Coord.). **Lei das sociedades anônimas comentada**. Rio de Janeiro: Forense, 2021.

CASTRO, Rodrigo R. Monteiro de; AZEVEDO, Luís André N. de Moura (Coord.). **Poder de controle e outros temas de direito societário e mercado de capitais**. São Paulo: Quartier Latin, 2010.

CESTARI FILHO, Felício. **ITIL v3 Fundamentos**. Rio de Janeiro: RNP/ESR, 2011.

CIURIAK, Dan. The Economics of Data: Implications for the Data-Driven Economy. Chapter 2. *In*: "Data Governance in the Digital Age" Centre for International Governance Innovation, **SSRN**, 2018. Disponível em: https://bit.ly/3OLtDEs. Acesso em: 9 abr. 2024.

COASE, Ronald. The Nature of the Firm. *In*: **The firm, the market and the law**. Chicago: The University of Chicago Press, 1990.

COBIT, Aligning. **4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit**. IT Governance Institute, 2008.

COELHO, Fábio Ulhoa. A natureza subjetiva da responsabilidade civil dos administradores de companhia. **Revista de Direito de Empresa**, v. 1, n. 1, 1996.

COELHO, Fábio Ulhoa. **Curso de Direito Comercial**. Volume 1: direito de empresa. 17. ed. São Paulo: Saraiva, 2013.

COELHO, Fábio Ulhoa. **Manual de direito comercial**. 28. ed. São Paulo: Revista dos Tribunais, 2016.

COMISSÃO DE VALORES MOBILIÁRIOS. **Processos Sancionadores Julgados**. Disponível em: https://bit.ly/3UJ1C4c. Acesso em: 9 abr. 2024.

COMISSÃO DE VALORES MOBILIÁRIOS. **Resolução CVM Nº 135, de 10 de junho de 2022**. Disponível em: <https://bit.ly/49Hs5mS. Acesso em: 9 abr. 2024.

COMISSÃO DE VALORES MOBILIÁRIOS. **Solicitação de esclarecimentos, de 10 de junho de 2021**. Disponível em: https://bit.ly/49Hsaaa. Acesso em: 9 abr. 2024.

CONGRESS OF THE UNITED STATES. **Supplemental Memo on Committee's Investigation into Ransomware**. Memorandum. Disponível em: https://bit.ly/3I61p3G. Acesso em: 9 abr. 2024.

COOTER, Robert; Ulen, Thomas. **Direito e Economia**. Trad. Luis Marcos Sander e Francisco Araújo da Costa. 5. ed. Porto Alegre: Bookman, 2010.

CORDEIRO, António Menezes. **Da boa fé no direito civil**. Coimbra: Almedina, 2015.

CRESWELL, Julie; PERLROTH, Niole; SCHEIBER, Noam. Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business. **The New York Times**, 1 jun. 2021.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **2021 Top Malware Strains**, 25 ago. 2022. Disponível em: https://bit.ly/42JauIW. Acesso em: 9 abr. 2024.

DEDENOK, Roman; KOVTUN, Andrey; KULIKOVA, Tatiana; SHIMKO, Irina; SVISTUNOVA, Olga. Spam e Phishing Report. Kapersky. **Securelist**, 16 fev. 2023. Disponível em: https://encr.pw/mYbzQ. Acesso em: 16 fev. 2023.
DELEUZE, Gilles. **Conversações**. Trad. Pelbart, Peter Pál. São Paulo: Ed. 34, 1992.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: direito de empresa**. São Paulo: Editora Saraiva, 2023.

EFING, Antônio Carlos. FREITAS, Cinthia Obladen de Almendra. **Direito e Questões Tecnológicas**: aplicados no desenvolvimento social. Vol. 2. Curitiba: Juruá, 2012.

EIZIRIK, Nelson. **A lei das S/A comentada**. 2. ed. São Paulo: Editora Quartier Latin, 2015.

ELLUL, Jacques. **The Technological Society**. New York, Vintage Books, 1964.

EUROPEAN DATA PROTECTION BOARD. **DPC Inquiry Reference**: IN-18-5-6. Disponível em: https://bit.ly/3LtTsqj. Acesso em: 9 abr. 2024.

EXECUTIVOS DA JBS contam como foi o ciberataque. **CISO Advisor**, 29 nov. 2021. Disponível em: https://www.cisoadvisor.com.br/executivos-da-jbs-contam-como-foi-o-ataque/#:~:text=Como%20os%20resultados%20da%20investiga%C3%A7%C3%A3o,mais%20dif%C3%ADcil%20impedir%20o%20ataque. Acesso em: 9 abr. 2024.

FEDERAL COURT OF AUSTRALIA. **Australian Securities and Investments Commission v RI Advice Group Pty Ltd Statement of Claim, 21 out. 2021**. Disponível em: https://bit.ly/3T4V5Qg. Acesso em: 9 abr. 2024.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. **Implantando a governança de TI**. 2. ed. Porto alegre: Brasport, 2008.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.

FRAZÃO, Ana. **Função social da empresa**: Repercussões sobre a responsabilidade civil de controladores e administradores de S/As. Rio de Janeiro: Editora Renovar, 2011.

GARÇON, Juliana. CVM diz que não deve baixar novas regras de segurança; entenda. **Estadão Investidor**, 13 set. 2023.

GICO JR, Ivo T. Introdução à Análise Econômica do Direito. *In*: KLEIN, Vinicius; RIBEIRO, Marcia Carla Pereira (Coord.). **O que é análise econômica do direito**: uma introdução. Belo Horizonte: Editora Fórum, 2011.

GOMES, Fábio Bellote. **Manual de Direito Empresarial**. 4. ed. São Paulo: Revista dos Tribunais, 2013.

GOMES, Irene. CABRAL, Umberlância. 84,9% das indústrias de médio grande porte utilizaram tecnologia digital avançada. **Agência IBGE notícias** 28 set. 2023. Disponível em: https://bit.ly/427s9Kc. Acesso em: 9 abr. 2024.

GONÇALVES, Oksandro. MIRÓ, Gustavo. CORNASSINO, Maria. LUCIANO, Danna. **IV Livro de resultados de pesquisa do GRAED PUCPR**. Londrina: Thoth Editora, 2023.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. Berkeley: New Riders, 2006.

GRIMES, Roger A. **Manual de proteção contra ransomware**: como criar um plano de segurança cibernética. São Paulo: Grupo A, 2022.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL. **Countering ransomware financing**. GAFI Report. 14 mar. 2023. Disponível em: https://l1nq.com/vwugN. Acesso em: 9 abr. 2024.

GUIMARÃES, Fernanda. Cerca de 11,4 milhões de brasileiros dependem de aplicativos para ter uma renda. **CNN Brasil**, 12 abr. 2021. Disponível em: https://l1nq.com/mxhA1. Acesso em: 9 abr. 2024.
HALPERÍN, Isaac. **Sociedades Anónimas**. Buenos Aires: Editora De Palma, 1974.

HAMILTON, Robert. **The law corporations***.* Saint Paul: West group, 2000.

HAN, Byung-chul. **NO ENXAME**: Perspectivas do Digital. Trad. Lucas Machado. Petrópolis, Rio de Janeiro: Editora Vozes, 2018.

HANLEY, Rob. MACPHERSON; John. VIERTMANN, Maxine. Ransomware new legislation should criminalise making ransomware payments. **Ashust**, 26 nov. 2021.

IMMUNEFI. **Top Crypto Ransomware Payments Report**, 2022. Disponível em: https://acesse.dev/CiOv8. Acesso em: 9 abr. 2024.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Big data, artificial intelligence, Machine Learning and data protection**. Disponível em: https://l1nq.com/ub8ri. Acesso em: 9 abr. 2024.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos**: evolução em governança e estratégia. São Paulo, SP: IBGC, 2017.

JBS DIZ que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. **G1 Globo**, 9 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 9 abr. 2024.

JBS PARALISA 25 unidades nos EUA e Canadá após ataque hacker. **CNN BRASIL**, 1 jun. 2021. Disponível em: 9 abr. 2024.

JBS USA CEO Andre Nogueira and Feeding America on soof supply chain. **WALL STREET JOURNAL**, 16 maio 2020. Disponível em: https://l1nq.com/3FLKF. Acesso em: 9 abr. 2024.

JOBIM, Caio. Europol e FBI prendem hackers ligados aos ataques ransomware contra JBS e Kayzea. **Cointelegraph**, 10 nov. 2021. Disponível em: https://encr.pw/JmFh8. Acesso em: 9 abr. 2024.

JONAS, Hans. **O princípio responsabilidade**: Ensaio de uma ética para a civilização tecnológica. Trad. Marijane Lisboa e Luiz Barros Montez. Rio de Janeiro: Editora Contraponto, PUCRJ, 2006.

KAHNEMAN, Daniel. **Rápido e devagar**: duas formas de pensar. Rio de Janeiro: Objetiva. 2012

KIM, David. SOLOMON, Michael. **Fundamentos de Segurança de Sistemas de Informação**. 1. ed. Editora: LTC, 2014.

KLEINA, Nilton. Erro no waze deixa trânsito de São Paulo (ainda mais) congestionado). **Tecmundo**, 25 out. 2017. Disponível em: https://encr.pw/FOVnj. Acesso em: 9 abr. 2024.

LAURINDO, Fernando José Barbin. **Gestão da tecnologia da informação**. São Paulo: Atlas, 2008.

LOJAS RENNER: os possíveis impactos do ataque hacker nas operações e nas ações da companhia. **Infomoney**, 22 ago. 2021. Disponível em:

https://www.infomoney.com.br/mercados/lojas-renner-os-possiveis-impactos-do-ataque-hacker-nas-operacoes-e-nas-acoes-da-companhia/#:~:text=S%C3%83O%20PAULO%20%E2%80%93%20A%20Lojas%20Renner,ataque%20e%20minimizar%20eventuais%20impactos. Acesso em: 9 abr. 2024.

LOPES, Miguel Maria de Serpa. **Curso de Direito Civil**. Rio de Janeiro: Freitas Bastos, 1962.

LUCAS, Lais Machado. **Programas de integridade nas sociedades anônimas**: implementação como conteúdo do dever de diligência dos administradores. Porto Alegre: Livraria do Advogado, 2021.

LUPION, Ricardo; HACKMANN, Evaldo Osorio. Cibersegurança e dever de diligência do administrador. **Revista jurídica Luso-brasileira**, ano 9, n. 2, 2023. Disponível em: https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-9-2023-n-2/289. Acesso em: 9 br. 2024.

LYNGAAS, Sean. Ciberataque força hospital dos EUA a enviar ambulâncias para outros lugares. **CNN Brasil**, 1 jun. 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/ciberataque-forca-hospital-dos-eua-a-enviar-ambulancias-para-outros-lugares/. Acesso em: 9 abr. 2024.

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

MACHADO, Léia. Alerta: ciberataque aos canais eletrônicos da Americanas e Submarino indicam sinais de aliciamento. **Security Leaders**, 21 fev. 2022. Disponível em: https://securityleaders.com.br/alerta-ciberataque-aos-canais-eletronicos-da-americanas-e-submarino-indicam-sinais-de-aliciamento/. Acesso em: 9 abr. 2024.

MACHADO, Léia. CISOs se manifestam diante de ciberataque à Renner. **Security Leaders**, 23 ago. 2021. Disponível em: https://securityleaders.com.br/cisos-se-manifestam-diante-de-ciberataque-a-renner/. Acesso em: 9 abr. 2024.

MACHADO, Léia. Um ano de guerra: Conflito envolve o ciberespaço como frente de batalha. **Security Report**, 24 fev. 2023. Disponível em: https://securityleaders.com.br/um-ano-depois-guerra-hibrida-entre-russia-e-ucrania-mostra-mudanca-na-direcao-dos-ciberataques/. Acesso em: 9 abr. 2024.

MADUREIRA, Daniele. Americanas apresenta balanço de 2022 nesta segunda. **Folha de São Paulo**, 12 nov. 2023. Disponível em: https://www1.folha.uol.com.br/mercado/2023/11/americanas-apresenta-balanco-de-2022-nesta-segunda-10-meses-apos-fraude-contabil.shtml. Acesso em: 9 abr. 2024.

MARQUES, Christopher da Costa; SOUZA, Weilan Carvalho; SOUZA, Julio Cesar Pinto de. A dependência da tecnologia na saúde mental dos adolescentes / The dependence of technology in the mental health of adolescents. **Brazilian Journal of**

Health Review, v. 4, n. 5, 2021. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJHR/article/view/38296. Acesso em: 9 abr. 2024.

MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed. São Paulo: Atlas. 2016.

MAZIERO, Carlos. **Sistemas Operacionais**: Conceitos e Mecanismos. Curitiba: Editora UFPR, 2019.

MAZZUCATO, Mariana. **O valor de tudo**: Produção e Apropriação na economia global. Trad. Camilo Adorno e Odorico Leal. 1. ed. São Paulo: Portfólio-Penguin, 2020.

MCAFEE. **Life Behind the screens of Parents, Tweens and Teens**, 2022. Disponível em: https://l1nq.com/m2vEJ. Acesso em: 9 abr. 2024.

MENDONÇA, Saulo Bichara. Função Social da Empresa – Análise Pragmática. **Revista de Estudos Jurídicos da UNESP**, v. 16, n. 23, 2012. Disponível em: https://seer.franca.unesp.br/index.php/estudosjuridicosunesp/user/setLocale/pt_BR?source=%2Findex.php%2Festudosjuridicosunesp%2Farticle%2Fview%2F479%2F0. Acesso em: 9 abr. 2024.

MIRANDA, Pontes. **Tratado de direito privado**. 3. ed. Rio de Janeiro: Borsoi, 1972.

MISUGI, Guilherme. **Tutela Jurídica das Novas Práticas Mercadológicas**: manipulação do comportamento do consumidor. Curitiba: Juruá, 2018.

MOCHON, D., & FREDERICK, S. Anchoring in sequential judgments. **Organizational behavioral and human decision processes**, v. 122, n. 1, 2013. Disponível em: https://ideas.repec.org/a/eee/jobhdp/v122y2013i1p69-79.html. Acesso em: 9 abr. 2024.

MUNCASTER, Phil. Cyber-Attacks up 37% over past months as #COVID19 bites. **Infosecurity Magazine**, 1 jun. 2020. Disponível em: https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/. Acesso em 9 abr. 2024.

MURPHY, Andrea; TUCKER, Hank. Forbes Global 2000: Quais são as maiores empresas do mundo em 2023. **Forbes**, 9 jun. 2023. Disponível em: https://forbes.com.br/forbes-money/2023/06/forbes-global-2000-quais-sao-as-10-maiores-empresas-do-mundo-em-2023/. Acesso em: 9 abr. 2024.

NALIN, Carolina; ALCÂNTARA, Camila. Americanas: Com suspensão das vendas on-line, empresa já perdeu quase R$ 3,5 bi em valor de mercado. **Jornal o Globo**, 23 fev. 2022. Disponível em: https://l1nk.dev/5aREL. Acesso em: 9 abr. 2024.

NATIONAL CYBER SECURITY CENTRE (NCSC), **Mitigating malware and ransomware attacks**, 13 feb. 2020.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATIONS CENTER. **What tis wannacry/Wannacryptor?**.Disponível em: https://encr.pw/oSRcI. Acesso em: 9 abr. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity, 12 feb. 2014**. Disponível em: https://acesse.dev/z8zpu. Acesso em: 9 abr. 2024.

NAUMANN, Saher. Now You See It, Now You Don't: Wipers in the Wild. **Virus Bulletin Conference**, Montreal, 2018. Disponível em: https://l1nq.com/sSDDH. Acesso em: 9 abr. 2024.

NEUMANN, Débora Martins Consteila; MISSEL, Rafaela Jarros. Família Digital: A Influência da Tecnologia nas Relações Entre Pais e Filhos Adolescentes. **Pensando Famílias**, v. 23, n. 2, 2019. Disponível em: http://pepsic.bvsalud.org/pdf/penf/v23n2/v23n2a07.pdf. Acesso em 9 abr. 2024.

NEVES, Edmo Colnaghi. Compliance empresarial: **o tom da liderança: estrutura e benefícios do programa**. São Paulo: Trevisan Editora, 2018.

NORONHA, Ilene Patrícia. Os ritos procedimentais de competência da CVM. *In*: SIMÃO FILHO, Adalberto; LUCCA, Newton de (Coord.). **Direito Empresarial contemporâneo**. São Paulo: Juarez de Oliveira, 2004.

NOVAS TECNOLOGIAS: tendências e o que esperar para o futuro. **CNN BRASIL**, 10 abr. 2023. Disponível em: https://www.cnnbrasil.com.br/tecnologia/novas-tecnologias/#:~:text=Realidade%20virtual%2C%20Big%20Data%20e,4D%20representam%20nomes%20do%20futuro. Acesso em: 9 abr. 2024.

O QUE se sabe sobre ataque cibernético a JBS investigado pelo FBI. **BBC News Brasil**, 2 jun. 2021. Disponível em: https://encurtador.com.br/gmvMT. Acesso em: 9 abr. 2024.

OFFICE PUBLICA AFFAIRS – U.S. DEPARTMENT OF JUSTICE. **Ukrainian Arrested and Charged with Ransomware Attack on Kaseya**, 8 nov. 2021. Disponível em: https://l1nq.com/OGqon. Acesso em: 9 abr. 2024.

OLIVEIRA, Ana Paula; ZANETTI DE OLIVEIRA, Dânton Hilário; LIMA, Flávio Santos; SAMPAIO, Themis Ortega. A Lei Geral de Proteção de Dados Brasileira na Prática Empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, v. 4, n. 1, 2019. Disponível em: https://bit.ly/306h0tZ. Acesso em: 9 abr. 2024.

OLIVEIRA, Ana Perestrelo de. **Manual de governo das sociedades**. Coimbra: Almedina, 2017.

OLIVEIRA, Dânton Zanetti de. **Big Data e a Lei Geral de Proteção de Dados Pessoais**: Diálogos necessários em prol da livre iniciativa. Rio de Janeiro: Lumen Juris, 2022b.

OLIVEIRA, Dânton Zanetti de. Big Data e Dualidade: Uma problematização entre Tecnologia e a Lei Geral de Proteção de Dados Pessoais Brasileira. *In*: FREITAS, Cinthia Obladen de Almendra; OLIVEIRA, Dânton Zanetti de (Org.). **Sociedade informacional e a Lei Geral de Proteção de Dados Pessoais**: diálogos contemporâneos entre direito e tecnologia. Rio de Janeiro: Lumen Juris, 2022a.

OLIVEIRA, Fátima Bayma de. **Tecnologia da Informação e da Comunicação**: desafios e propostas estratégicas para o desenvolvimento dos negócios. 1. ed. São Paulo: Editora Pearson Prentice Hall, 2006.

PAES, Paulo Roberto Tavares. **Responsabilidade dos administradores de sociedades**. São Paulo: Revista dos tribunais, 1997.

PANETTA, Kasey. As oito principais previsões de segurança cibernética para 2021-2022. **Gartner**, 20 out. 2021. Disponível em: https://encurtador.com.br/fuwI1. Acesso em: 9 abr. 2024.

PARENTE, Flavia. **O dever de diligência dos administradores das sociedades anônimas**. Rio de Janeiro. Editora Renovar, 2005.

PINHEIRO, Patricia Peck. LOTUFO, Larissa. Proteção de Dados Pessoais. *In*: PINHEIRO, Patricia Peck. **Segurança Digital** – Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2020.

PINTO, Mariana. As múltiplas faces do dever de diligência. **Análise editorial**, 9 dez. 2022.

PORTO, Walter. Venda de ebooks salta 83% em 2020 e revela força dos livros digitais na pandemia. **Folha de São Paulo**, 1 jul. 2021. Disponível em: https://acesse.one/k9lti. Acesso em: 9 abr. 2024.

PREJUÍZO DO ataque hacker contra JBS se estendeu à indústria de alimentos dos EUA. **Infomoney**, 11 jun. 2021. Disponível em: https://encurtador.com.br/cmvHZ. Acesso em: 9 abr. 2024.

PRIMEIRA SANÇÃO por descumprimento da LGPD é publicada pela ANPD. **Trench Rossi Watanabe**, 14 jul. 2023. Disponível em: 9 abr. 2024.

PROCON. **Notificação do Procon-SP sobre ataque cibernético, 1 out. 2021**. Disponível em: https://l1nk.dev/9LKBN. Acesso em: 9 abr. 2024.

PROOFPOINT. **2020 State of the Phish. 2020**. Disponível em: https://l1nq.com/PmMzm. Acesso em: 9 abr. 2024.

PROTEÇÃO DE Dados Pessoais agora é um direito fundamental. **Ministério da Justiça e Segurança Pública**, 14 fev. 2022. Disponível em: https://encurtador.com.br/kOQS0. Acesso em: 9 abr. 2024.

RAJAMÃKI, Ari. **Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center**. Master's thesis (Master's Degree) – Programme in Information Technology, Cyber Security, 2021.

RENNER DIZ não ter pago resgate após ataque hacker. **O Globo**, 24 ago. 2021. Disponível em: https://shre.ink/8KlB. Acesso em: 9 abr. 2024.

REQUIÃO, Rubens. **Curso de direito comercial**. 33. ed. São Paulo: Saraiva, 2014.

REZENDE, Denis Acides. **Planejamento de sistemas de informação e informática**. 3 ed. São Paulo: Atlas, 2008.

RIBEIRO, Renato Ventura. **Dever de diligência dos administradores de sociedades**. São Paulo: Editora Quartier Latin, 2006.

RICHARDSON, Ronny; NORTH, Max. **Ransomware**: Evolution, Mitigation and Prevention. International Management Review, 2017.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSS, Stephen A.; WESTERFIELD, Randolph W.; JAFFE, Jeffrey. **Administração Financeira**. Porto Alegre: Grupo AMGH, 2015.

SAAVEDRA, Giovanni Augusto; BORGES, Gabriel Oliveira de Aguiar. CONSTITUCIONALISMO DIGITAL BRASILEIRO. **Revista da AJURIS**, v. 49, n. 152, 2022. Disponível em: https://l1nq.com/OPH5s. Acesso em: 9 abr. 2024.

SACRAMONE, Marcelo Barbosa. **Administradores de sociedades anônimas**. Enciclopédia jurídica da PUC-SP. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Comercial. Fábio Ulhoa Coelho, Marcus Elidius Michelli de Almeida (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

SACRAMONE, Marcelo Barbosa. **Ato de preenchimento de órgão de administração**. Tese (Doutorado em Direito Comercial) – Universidade de São Paulo, São Paulo, 2012.

SACRAMONE, Marcelo Barbosa. **Manual de Direito Empresarial**. São Paulo: Editora Saraiva, 2023.

SALOMÃO FILHO, Calixto. Recuperação de empresas e interesse social. *In*: SOUZA JUNIOR, Francisco Satiro de; PITOMBO, Antonio Sergio A. de Moraes (Coord.). **Comentários à lei de recuperação de empresas e falências**. 2. ed. São Paulo: Revista dos Tribunais, 2007.

SANGER, David. Russia's most aggressive ransomware group disappeared. It's unclear who made that happen. **The New York Times**, 13 jul. 2021. Disponível em: https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html. Acesso em: 9 abr. 2024.

SANTINO, Renato. Americanas, Submarino e Shoptime saem do ar nesta segunda (21) após ataque. **Canaltech**, 21 fev. 2022. Disponível em: https://shre.ink/8Kla. Acesso em: 9 abr. 2024.

SCHOLLMEIER, Rüdiger. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architetures and Applications. Conference. **IEEE Internet Computing**, 2022. Disponível em: https://shre.ink/8Kln. Acesso em: 9 abr. 2024.

SCHUURMAN, Egbert. **Reflections on the Technological Society**. Ontario: Wedge Publishing Foundation, 1983.

SCHWAB, Claus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SCHWEITZER, Heike; WELKER, Robert. Competition policy for the digital era. **The Antitrust Chronicle**, v. 3. 2019. Disponível em: https://www.competitionpolicyinternational.com/wp-content/uploads/2019/12/CPI-Schweitzer-Welker.pdf. Acesso em: 9 abr. 2024.

SECURITIES AND EXCHANGE COMMISSION. **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 2022**. Disponível em: https://l1nq.com/mZxtU. Acesso em: 9 abr. 2024.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: Uma visão Executiva. Rio de Janeiro: Ed. Campus, 2003.

SHALAL, Andrea. Após ataque hacker contra JBS, EUA devem mostrar postura mais agressiva diante da Rússia. **Terra**, 2 jun. 2021. Disponível em: https://shre.ink/8KaF. Acesso em: 9 abr. 2024.

SHERSTOBITOFF, Ryan. JBS Ransomware Attack Started in March and Much Larger in Scope than Previously Identified. **Security Scorecard**, 8 jun. 2021. Disponível em: https://encr.pw/iMfk9. Acesso em 9 abr. 2024.

SILVA, Alexandre Couto. **Responsabilidade dos Administradores de S.A.** – Business Judgment Rule. Rio de Janeiro: Elsevier, 2007.

SILVA, Américo Luís Martins da. **Sociedades Empresariais**. Volume 2. São Paulo: Editora Forense, 2007.

SILVA, Michel Bernardo Fernandes da. **Cibersegurança**: uma visão panorâmica sobre a segurança da informação na internet. 1. ed. São Paulo: Freitas Bastos, 2023.

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. Dissertação (Mestrado em Ciências Jurídico Forenses) – Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

SONICWALL. **Relatório de ameaças cibernéticas 2021**, 2022. Disponível em: https://l1nq.com/m69gx. Acesso em: 9 abr. 2024.

SOPHOS. **The state of ransomware**, 2022. Disponível em: https://acesse.dev/pXygs. Acesso em: 9 abr. 2024.

STALLINGS, William. **Criptografia e Segurança de Redes**: Princípios e Práticas. 6. ed. São Paulo: Editora Pearson, 2014.

STAMP, Mark. **Information Security**: Principles and Practice. Indianapolis, USA: Wiley Publishing, 2008.

STATISTA. **Distribution of information security incidents in 2020**.

STRIPHAS, Ted. Algorithmic culture. **European Journal of Cultural Studies**, v. 18, n. 4-5, 2015. Disponível em: https://journals.sagepub.com/doi/10.1177/1367549415577392. Acesso em: 9 abr. 2024.

TEIXEIRA, Egberto Lacerda; GUERREIRO, José Alexandre Tavares. **Das sociedades anônimas no direito brasileiro**. São Paulo: Editora José Bushatsky, 1979.
URQUIAGA, Francisco Pfeffer. Deber de lealtad de directores y gerentes de sociedades anónimas al interior de un grupo de sociedades, a propósito del denominado Caso Cascadas. **Revista ACTUALIDAD JURÍDICA**, n. 32, jul. 2015. Disponível em: https://shre.ink/8Kaq. Acesso em: 9 abr. 2024.

VENOSA, Silvio de Salvo. **Direito Civil**. Responsabilidade Civil. 13. ed. São Paulo: Atlas, 2013.

VENTUROLI, Emanuele. Os 275 acordos de patrocínio da Fórmula 1 de 2023. **RTR Sports Marketing**, 24 fev. 2023. Disponível em: https://bit.ly/427rs3y. Acesso em: 9 abr. 2024.

VERÇOSA, Haroldo Malheiros Duclerc. **Curso de Direito Comercial**. Volume 1. 2. ed. São Paulo: Malheiros, 2008.

WORLD ECONOMIC FORUM. **The global risks report 2024**. 19th edition. January, 2024. Disponível em: https://l1nq.com/kvhnj. Acesso em: 9 abr. 2024.