CIBERSEGURANÇA E DEVER DE DILIGÊNCIA DO ADMINISTRADOR[1]

Ricardo Lupion[2]

Evaldo Osorio Hackmann[3]

Resumo: As corporações enfrentam, atualmente, grandes desafios à continuidade de suas atividades, quais sejam, os ataques cibernéticos. Estas ameaças têm figurado como uma das maiores preocupações dos administradores das companhias listadas em bolsa. Os prejuízos causados às companhias podem ser financeiros ou reputacionais, em ambos os casos, exigindo que seus administradores atuem para preservar as instituições e resguardar os interesses dos acionistas. O enfrentamento aos *cyber attacks* está, indubitavelmente, contido no dever de diligência do administrador, sendo fundamental à solução jurídica para esses incidentes a incorporação de medidas de técnicas de cibersegurança às boas práticas de governança corporativa. O método utilizado foi exegético para pesquisa bibliográfica e documental. Especificamente, denota-se o caráter dogmático fundamental do estudo no Direito Empresarial brasileiro.

Palavras-Chave: ataques cibernéticos – administradores – dever de diligência – cibersegurança – governança corporativa

---

[1] Tema apresentado no evento realizado em homenagem ao 8º Aniversário da Revista Jurídica Luso-Brasileira, pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa, em 16 a 20/01/2023.

[2] Pós-Doutor em Ciências Jurídico-Empresariais pela Faculdade de Direito da Universidade de Lisboa. Mestre e Doutor em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Professor Titular de Direito Empresarial na Escola de Direito da PUCRS. Advogado.

[3] Mestrando e bolsista no Programa de Pós-Graduação em Direito (PPGD) na PUCRS. Advogado.

CYBERSECURITY AND THE ADMINISTRATOR'S DUTY OF CARE

Abstract: Corporations currently face major challenges to the continuity of their activities, namely, cyber attacks. These threats have been one of the biggest concerns of listed companies administrators. The damages caused to the companies can be financial or reputational, in both cases, requiring their administrators to act to preserve the institutions and protect the interests of shareholders. The fight against cyber attacks is, undoubtedly, contained in the administrator's duty of diligence, and the incorporation of cybersecurity techniques measures to good corporate governance practices is fundamental to the legal solution for these incidents. The method used was exegetical for bibliographic and documentary research. Specifically, it denotes the fundamental dogmatic character of the study in Brazilian Corporate Law.

Keywords: cyber attacks – administrators – duty of diligence – cybersecutiry – corporate governance

1. INTRODUÇÃO

Ultimamente, pesquisas realizadas junto aos principais líderes empresariais – sobretudo aqueles responsáveis pela condução de negócios em escala global – têm revelado as maiores ameaças que tiram o sono destes administradores, demandando uma definição acerca de como encará-las de maneira eficaz.

No mês de janeiro de 2022, dados revelados pelo estudo *11º Allianz Risk Barometer*[4] indicaram que 44% das empresas

[4] Estudo disponível em: https://www.agcs.allianz.com/news-and-

com atuação global apontaram o risco cibernético como a maior preocupação à continuidade de seus negócios. Um recorte por país indicou que um total de 64% das empresas brasileiras considera os riscos de ataques cibernéticos, nas suas mais variadas modalidades, a principal ameaça aos seus negócios para o corrente ano (2022).

Outra pesquisa levada a campo pela consultoria *Roland Berger*, a pedido do jornal O Estado de São Paulo[5], divulgada em março de 2022, corrobora e sustenta como legítima a preocupação dos principais executivos brasileiros. O título da matéria, por si só, já é alarmante: "Tentativas de ataque *hacker* atingem uma empresa a cada segundo no País", principalmente, quando se percebe que o conteúdo da notícia aponta para um aumento expressivo de ataques aos sistemas de dados das empresas, capturando e criptografando as informações contidas em seus arquivos, bem como exigindo pagamento de quantia vultosa para a não destruição e o restabelecimento da posse dos dados pela empresa atacada, alçando o Brasil da 9ª para a 4ª posição, em apenas um ano, no *ranking* global de investidas de *ransomware*[6].

Salienta-se, na reportagem, que qualquer empresa de grande porte e intenso fluxo de caixa está sob a ameaça desses atacantes, bem como revela-se uma projeção acerca dos custos globais dessas ações criminosas que são estimadas em US$ 20 bilhões (vinte bilhões de dólares) em todo o mundo. Nesse sentido, a título de exemplificação, os ataques perpetrados por grupos *hackers* contra a JBS[7] (que rendeu aos criminosos um

insights/reports/allianz-risk-barometer.html. Acesso em: 15/06/2022.

[5] Disponível em: https://economia.estadao.com.br/noticias/negocios,ciberataques-hacker-ransomware-empresas-brasil,70003995784. Acesso em: 15/06/2022.

[6] Entendido como a modalidade de cibercrime na qual o atacante invade o sistema de dados da organização, captura e criptografa as informações contidas em seus arquivos e exige pagamento de quantia vultosa para a não destruição e restabelecimento da posse dos dados pela empresa atacada.

7 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.

pagamento de resgate de dados de US$11 milhões) e em desfavor da varejista Americanas[8] (cuja perda financeira estimada foi de R$ 1 bilhão) vêm a tangibilizar esta estimativa, bem como dar um colorido (sombrio e denso) ao problema que aflige conselheiros de administração e demais executivos brasileiros.

Com efeito, ao lado dos impactos financeiros, estão os que atuam sobre o aspecto reputacional da empresa vítima de um ataque *hacker*. Veja-se o caso ocorrido com um dos grandes prestadores de serviço do setor de *healthcare* nacional, o laboratório Fleury[9]. Esta organização sofreu um ataque e, com isto, teve a indisponibilidade de seus serviços por mais de uma semana, prejudicando alguns dos maiores serviços hospitalares e clínicas do país, que se mobilizaram contingencialmente para informar seus pacientes – aqueles que compartilharam seus dados de clínicos com o laboratório em destaque – sobre os resultados de exames diversos.

Noutra seara, para delinear a situação com mais clareza, pinçando exemplo que denota que o ataque cibernético não se restringe às fronteiras da nossa pátria, traz-se à baila o ataque ao oleoduto, administrado pela empresa Colonial Pipeline[10], em maio de 2021, que paralisou as atividades de fornecimento de combustível em todo o sudeste dos Estados Unidos da América, prejudicando em torno de 50 milhões de americanos e empresas locais. Destaque-se que, neste incidente, o dano provocado à infraestrutura de abastecimento e aos cidadãos atingidos pela indisponibilidade dos serviços de fornecimento de combustível

Acesso em: 15/06/2022.

8 Disponível em: https://pipelinevalor.globo.com/negocios/noticia/ataque-hacker-custou-r-1-bilhao-a-americanas.ghtml. Acesso em 15/06/2022.

9 Disponível em: https://www.correiobraziliense.com.br/brasil/2021/06/4933691-apos-ataque-hacker-a-laboratorio-hospitais-montam-forca-tarefa-para-exames.html. Acesso em 15/06/2022.

10 Disponível em: https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=3d2238773d82. Acesso em: 15/06/2022.

pode ser qualificado como imensurável; ademais, o prejuízo político ao governo norte-americano e a repentina elevação de preço em face da escassez do produto teriam o potencial de prejudicar todo o sistema econômico da maior potência mundial.

Todos os casos citados referem-se à ocorrência que tiveram como alvo empresas listadas em bolsa de valores: o que, indubitavelmente, remete o leitor a questionar sobre os reflexos nos mercados de capitais onde as empresas atacadas negociam seus papeis.

Destarte, o ataque cibernético: a ação praticada por *hackers* no intuito de violar ou desabilitar sistemas de computacionais, a partir da captura ou vazamento de dados tratados por controladores (pessoas físicas ou jurídicas), mediante utilização de credenciais obtidas de modo espúrio ou técnicas de engenharia social, tem ganhado, cada vez mais, notoriedade nos mercados mundo a fora e, por isso mesmo, deve estar na agenda estratégica de toda empresa e administrador diligente e responsável[11].

Em face à gravidade do tema em destaque, cabe indagar se os administradores das empresas – sobretudo aqueles dirigentes que se ocupam de guiar os destinos das sociedades anônimas – tem a mera discricionariedade ou, ao revés, o inadiável e inescapável dever fiduciário de enfrentar as investidas com a roupagem moderna dos ataques cibernéticos. Procurar-se-á responder a tal indagação de modo a evitar-se tergiversações, respeitando as opiniões em contrário senso, com base legal e no conceito doutrinário, fundamentos e boas práticas de Governança Corporativa que suportam a tomada de decisão estratégica, dirigem, controlam e monitoram as companhias.

Tendo situado a temática de forma introdutória, cumpre-se percorrer os conceitos de Governança Corporativa e sua

[11] Contudo, essa não parece ser a realidade encontrada nas organizações mundo a fora: https://www.techrepublic.com/article/security-executives-say-unprepared-threats-lie-ahead/. Acesso em 15/06/2022.

intrincada e – por que não ressaltar – moderna relação com a cibersegurança.

Avançando, especificamente em relação ao conteúdo do dever do administrador das sociedades anônimas, espera-se esmiuçar o entendimento com amparo legal e doutrinário. Dessa forma, quer-se convencer o leitor de que não há alternativa justificável ao comportamento desidioso e irresponsável diante do incremento e do recrudescimento dos *cyberattacks* às organizações de propriedade dispersa. Nessa linha, buscar-se-á exemplos de quanto pode custar a uma empresa o comportamento não-diligente da sua administração[12], e qual o impacto dessa conduta repreensível junto aos mercados.

Por outro lado, como consequência desse dever, indicar qual seria a conduta ou mecanismo adequado à mitigação dos riscos cibernéticos: demonstrando como deveriam se planejar estas ações, quais seriam os atores envolvidos, se necessária uma mudança estrutural dentre os agentes de governança ou mesmo de *mindset* organizacional.

De fato, cumpre ao trabalho em tela analisar o dever de diligência do administrador em razão dos potenciais riscos impostos pelos ataques cibernéticos. Para isto, utiliza-se pesquisa bibliográfica, legal e doutrinária, bem como cotejam-se resultados de pesquisas realizadas por importantes consultoria, divulgadas em meios de comunicação que gozam de boa reputação para sustentarmos a posição que se julga inarredável e mais alinhada a essência da fidúcia depositada tanto no conselho de administração, quanto na direção executiva.

Finalmente, com o intuito de colaborar com a elaboração de uma posição sobre o tema, bem como agregar argumentos de

[12] Acerca dos custos financeiros derivados dos ataques cibernéticos, leia-se: MORGAN, Steve. *Cybercrime to Cost The World $10.5 trillion annually by 2025*. CYBERCRIME MAGAZINE, 13/11/2020. Disponível em: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Acesso em 15/06/2022.

forma legítima e assertiva ao estabelecimento de um dever do administrador de enfrentamento aos ataques cibernéticos, mas sem a pretensão de exaurir a discussão que o tema suscita, concluir-se-á o presente artigo com as considerações finais sustentando a linha-mestra deste modesto contributo acadêmico.

2. GOVERNANÇA CORPORATIVA E CIBERSEGURANÇA

Antes de adentrar-se na análise do dever de diligência do administrador em face das ameaças oriundas dos ataques cibernéticos, para fins de delimitação da responsabilidade do administrador, tem-se como baliza legal o disposto no artigo 158, § 3º, da Lei das Sociedades Anônimas (nº 6.404/1976)[13], que preconiza um *standard* comportamental a ser seguido pelos dirigentes das companhias abertas.

Dito isso, é prudente que se opte por um conceito base de Governança Corporativa[14] para ter-se o mesmo como porto seguro à tese que será esposada a seguir, destacando que não há um conceito estático e definitivo, pois se trata de um tema fluido e em constante aprimoramento, que varia diante das condições culturais e socioeconômicas das nações nas quais se desenvolve.

A título de exemplos e referenciais teóricos, opta-se por destacar os conceitos emanados por duas importantes instituições promotoras da governança, no Brasil e no estrangeiro, o IBGC e a OCDE.

Para o Instituto Brasileiro de Governança Corporativa[15]:

> Governança Corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas,

[13] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6404compilada.htm . Acesso em: 16/06/2022.

[14] Notadamente, prefere-se adotar um conceito ampliado de governança, *stakeholder oriented*, como será verificado a seguir, em face da crença na conjugação entre a maximização dos lucros e os interesses de todos os demais envolvidos no entorno da corporação.

[15] IBGC – Instituto Brasileiro de Governança Corporativa. *Código das melhores práticas de governança corporativa.* 5ª edição. São Paulo: IBGC, 2015.

> envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controles e demais partes interessadas. As boas práticas de Governança Corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.

Diante desse conceito, percebe-se a clara opção do instituto por considerar que os temas de governança constituem um verdadeiro sistema de relações que direcionará, interna e externamente, a estratégia das organizações.

Por outro lado, a OCDE[16] adota um viés que busca garantir o interesse de todos os envolvidos com as atividades desempenhadas pelos entes empresariais, traduzido da seguinte forma:

A Governança Corporativa é o sistema segundo o qual as corporações de negócios são dirigidas e controladas. A estrutura da Governança Corporativa especifica a distribuição dos direitos e responsabilidades entre os diferentes participantes da corporação, tais como o conselho de administração, os diretores executivos, os acionistas e outros interessados, além de definir regras e procedimentos para a tomada de decisão em relação a questões corporativas. E oferece também as bases através das quais os objetivos da empresa são estabelecidos, definindo os meios para se alcançarem tais objetivos e os instrumentos para se acompanhar o desempenho.

Ou seja, além de contemplar o conceito de sistema de relações, a OCDE traz em sua definição sobre o tema aspectos que levam a determinar que a Governança Corporativa, igualmente, pode ser um sistema normativo e, principalmente, a guardiã de direitos dos demais *stakeholders* na continuidade dos

[16] Disponível em: OCDE–Organização para a Cooperação e Desenvolvimento Econômico. https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf. Acesso em 15/06/2022.

negócios das organizações[17].

Finalmente, é mister que se realcem as bases que alicerçam o edifício da Governança Corporativa, iluminando com destaque a responsabilidade corporativa.

2.1 FUNDAMENTO DE GOVERNANÇA: FOCO NA RESPONSABILIDADE CORPORATIVA.

Os fundamentos ou princípios de Governança Corporativa servem como guias orientativos nesse longo e importante percurso em direção à maturidade, à perenidade, ao desenvolvimento econômico e à sustentabilidade dos negócios.

A incorporação dos fundamentos deve se dar pela companhia em sua inteireza, perpassar todos os setores, as estruturas de governo da sociedade, bem como fazer parte das discussões internas, do relacionamento com terceiros prestadores de serviços e demais interessados.

Assim, o exemplo corporativo fornece a exata medida de importância dos fundamentos para a empresa. Sem o comprovado engajamento da alta direção, conselho de administração e executivos-chefes, a chance de sucesso na implantação dos conceitos é nula.

Em relação ao elenco de princípios[18] que governam as sociedades, há quase um consenso. Oriundos de interpretação de leis, doutrina e códigos de boas práticas, podem-se elencar quatro tipos fundamentais à construção desse sistema: a transparência (*disclosure*), a equidade (*fairness*), a prestação de

[17] Adota-se o conceito denominado *Stakeholder Capitalism*, cuja essência pode ser verificada, entre outras fontes, em: SCHWAB, Klaus; VANHAM, Peter. *Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet.* John Wiley & Sons: New Jersey, 2021.

[18] Para melhor entendimento sobre os fundamentos de governança, recomendamos: BLOK, Marcella. *Compliance e Governança Corporativa*. 3ª ed. São Paulo: Freitas Bastos Editora, 2020, p.2. e ROSSETI, José P. ANDRADE, Adriana. *Governança Corporativa: fundamentos, desenvolvimento e tendências*. 7. ed. – São Paulo: Atlas, 2016, p. 140.

contas (*accountability*) e a responsabilidade corporativa (*corporate liability*).

Em que pese a abordagem apartada de cada um deles, não se deve perder de vista que necessitam ser conjugados de modo harmônico e integrado à realização das atividades empresariais. Outrossim, os enunciados não se tratam de normas cogentes, ou seja, não vinculam os dirigentes das companhias no exercício de suas atividades.

Para a finalidade deste artigo, foca-se na no conceito delimitador da reponsabilidade corporativa que, entre outras funções, baliza o dever de conduta diligente dos administradores.

A responsabilidade corporativa (*corporate liability*) guarda relação com sustentabilidade do negócio, com a viabilidade econômica e financeira, numa palavra, com a continuidade da empresa. Nessa toada, deve pautar a maximização dos lucros dos acionistas na justa medida entre responsabilidade e assunção de riscos vinculados às atividades da companhia, mitigando as externalidades negativas e aumentando as positivas, levando em consideração o segmento de mercado, a comunidade na qual se insere, bem como o ordenamento jurídico que contém o desenvolvimento dos negócios da corporação.

Nesse sentido, de modo a suportar as complexas demandas de governança, surge como importante facilitador a figura do *Governance Officer* que desempenha suas funções nas dimensões estratégica, relacional e operacional[19]. Este profissional, dada a especialização e a senioridade exigidas, atua como um apoio essencial às atividades dos administradores, não apenas organizando processos internos, mas colaborando para uma tomada de decisão holística e sintonizada com os desafios impostos pelos mercados em que a empresa atua.

[19] IBGC – Instituto Brasileiro de Governança Corporativa. *Governance Officer*. São Paulo: IBGC, 2022, p.17 e ss.

A essa altura, claramente, já se percebe a relação entre a reponsabilidade corporativa e o dever de diligência do administrador. Isto, em razão da necessária conjugação dos fundamentos exemplificados acima com a inescapável conduta íntegra, tempestiva, eficiente e eficaz esperada dos responsáveis pela continuidade negocial. Este dever perpassa a necessária observância da conformidade legal pelas corporações, bem como determina a atuação preventiva ou mitigatória frente aos riscos que se apresentam às atividades empresariais, o que enseja a abordagem do próximo item, a Cibersegurança.

2.2 CIBERSEGURANÇA: CONCEITO E IMPACTOS DE VIOLAÇÃO.

Diante da expansão das frentes de comércio internacional e da transformação digital que caracteriza a Quarta Revolução Industrial[20], existe uma tendência de que a chamada hiper conectividade seja cada vez mais acentuada, exigindo-se um nível superior de compreensão de Segurança da Informação e maturidade de governança nos mais diversos mercados. Assim, as empresas e os governos devem implementar políticas e ações voltadas à mitigação de riscos e ataques cibernéticos a partir da decisão fundamental de seus administradores[21].

Desse modo, revela-se imprescindível a compreensão conceitual da Cibersegurança, sendo definida como um conjunto de ações e técnicas para a proteção de sistemas, programas, redes, bancos de dados e equipamentos computacionais de violações e vazamentos de dados corporativos ou pessoais.[22]

---

[20] SCHWAB, Klaus. *The Fourth Industrial Revolution*. New York: Currency Books, 2017.

[21] Veja-se a definição do governo norte-americano ao priorizar a Cibersegurança como política estratégica nacional: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/, Acesso em 16/06/2022.

[22] O conceito em destaque é elaborado pelos autores, tendo como fundamento fontes doutrinárias e legais. No ordenamento jurídico pátrio, recomenda-se a leitura do

Nos últimos anos, tornou-se comum a preocupação com a segurança das informações tratadas por meio digital. Neste sentido, resguardar os dados tratados pelas companhias não mais se revela uma opção, e sim uma inadiável conformidade legal.

Diante disto, é que resplandece o valor estratégico da Cibersegurança para as companhias abertas, não apenas para que protejam seus segredos industriais, mas para que tratem os dados de seus clientes finais em conformidade com os mandamentos das leis gerais de proteção de dados e privacidade às quais estão subordinadas, evitando violações e vazamentos que podem render-lhes prejuízos tremendos no campo financeiro ou reputacional.

De um lado, observa-se que os ataques de *hackers* têm sido mais ousados, causando grandes entraves ao regular funcionamento de diversas empresas. De outra parte, como dito anteriormente, percebe-se que está se tornando mais usual falar sobre Cibersegurança, e como pode ser prejudicial a ausência de investimentos em medidas protetivas.

Nessa seara, o 17ª Relatório do Custo de uma Violação de Dados[23], baseado em pesquisa conduzida pelo Instituto Ponemon e a IBM Security, denota um incremento dos custos de incidentes cibernéticos em quase todos os setores investigados: o custo médio de violação foi de US$ 4,24 milhões (2021) para US$ 4,35 milhões (2022), um aumento de 2,6%.

Para além dos impactos financeiros, a depender do porte da empresa, um vazamento ou violação de dados pode contaminar a credibilidade das relações estabelecidas no mercado de capitais como um todo, pois, a confiança das

Decreto federal nº 10.222, de 05 de fevereiro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm, Acesso em: 17/06/2022.

[23] A pesquisa foi conduzida de forma independente pelo Instituto Ponemon e os resultados foram patrocinados, analisados, relatados e publicados pela IBM Security. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em 28/07/2022.

sociedades é diretamente proporcional à segurança jurídica das interações entre os investidores e as companhias neles listadas.

Assim, em caso de algum incidente cibernético, o órgão regulador deve agir com celeridade e rigor para garantir a continuidade das transações no mercado de capitais. Nesta linha, em caso de comprovada ausência de medidas técnicas e administrativas relacionadas à Cibersegurança, o mesmo pode impingir sanções financeiras e, em casos mais graves, determinar à descontinuidade das atividades do ente empresarial atacado no mercado, impactando não somente o caixa, mas promovendo dano reputacional à instituição.

Nesse momento, após a conceituação dos institutos basilares acima referidos, bem como a demonstração dos custos, tangíveis e intangíveis, que envolvem os ataques cibernéticos, emerge imperiosa e necessária a conduta exigida dos líderes das companhias, mais ainda, daquelas que possuem ações listadas em bolsa. Assim, passa-se ao dever de diligência dos administradores como objeto central do próximo ponto deste artigo.

3. DEVER DE DILIGÊNCIA: CONCEITO E ELEMENTO CENTRAL.

A administração de uma sociedade compreende atos de gestão coordenados e direcionados à obtenção da maximização dos lucros dos investidores precipuamente, bem como à promoção do interesse dos indivíduos, demais empresas e sociedade interessados no sucesso da organização.

O conteúdo desses atos, em sua maioria, não se encontra exaustivamente determinados em documentos internos, leis ou regulamentos a serem observados pelos administradores. Ao contrário, tais tomadas de decisões advêm da reflexão obtida a partir das situações que se impõem pelo dinamismo das atividades empresariais, sopesadas com as situações já

vivenciadas em suas experiências pessoais e trajetórias corporativas, contendo – essencialmente – inequívoca parcela de discricionariedade.

Dessa forma, em que pese as amarras impostas pela regulação e pelos estatutos sociais *lato sensu*, na maior parte do tempo, caberá ao dirigente eleger a melhor alternativa à continuidade exitosa dos negócios dentre todas aquelas que se apresentam ao seu alvedrio.

Nesse sentido, descortina-se o dever de diligência como como uma norma geral e abstrata[24], um *standard* jurídico que exige do administrador uma conduta orientada em direção ao cumprimento de uma obrigação. Diante disto, revela-se que a avaliação da conformidade deverá ser levada a efeito a partir da verificação de um caso concreto, onde a ação perpetrada pelo agente[25] será escrutinada em razão da tomada de decisão por ele efetivada, ou seja, do que comportamento que dele se esperava[26].

Inobstante a configuração de uma norma geral e abstrata,

---

[24] ÁVILA, Humberto. *Teoria dos Princípios*. 16.ª ed. São Paulo: Malheiros, 2015, p. 109.

[25] Aqui, há opção pela clássica definição do poder transmitido pelo principal (outorgante) ao agente (outorgado) que embasa a renomada Teoria da Agência: "We define an agency relationship as a contract under which one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision making authority to the agent. If both parties to the relationship are utility maximizers, there is good reason to believe that the agent will not always act in the best interests of the principal. JENSEN. Michael C. MECKLING. William H. *Theory of the firm: managerial behavior, agency costs and ownership structure*. Journal of Financial Economics, October, 1976, V. 3, No. 4, p. 310.

[26] A CVM – Comissão de Valores Mobiliários indica as características do dever de diligência: "Assim, o Relator, ainda que tenha feito reparo à falta da descrição de eventuais discussões ocorridas, entendeu não haver indícios e nem menção pela Acusação de qualquer interesse particular dos conselheiros na decisão e reconheceu que a mesma foi tomada de maneira informada, refletida e desinteressada, dentro do padrão de diligência esperado para administradores das companhias abertas, votando pela absolvição dos acusados." Voto do Diretor Relator Carlos Rebello, Caso OGX IV – PAS CVM nº RJ2016/7197. (grifou-se). In: LORIA, Eli; KALANSKY, Daniel. *Processo sancionador e Mercado de Capitais V: Estudo de Casos e Tendências: Julgamentos da CVM.* São Paulo: Quartier Latin, 2021, p.121 e ss.

a Lei das Sociedades Anônimas (lei nº 6.404/1976), em seu artigo 153[27], define o dever de diligência da seguinte forma:

> 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.

Sem, aqui, querer avançar-se numa análise doutrinária extensiva sobre o disposto no artigo em comento, impende destacar qual a intenção do legislador, ainda que sumariamente, que será fundamental para a verificação, por exemplo, de elemento central ao dever de diligência, bem como para demonstrar que este conceito não deve ser compreendido numa quadra estática, mas demandante de adequada e necessária atualização profissional.

Note-se a clara opção do legislador pela utilização do conceito do homem médio, qualificado como aquele ativo e probo, ancorado na figura jurídica oriunda do Direito Romano, o *bonus pater familias*. Notadamente, um conceito que deve ser superado quando se está a analisar a conduta do agente em relação às exigências corporativas modernas, bem como em face do Direito Societário hodierno.

No mesmo sentido, a doutrina salienta o inadiável câmbio do paradigma do bom pai de família pelo do competente administrador de empresas[28]. Isto, pois é notória e necessária a

---

[27] Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6404compilada.htm. Acesso em: 16/06/2022.

[28] Ao encontro do exposto, destaca-se: "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 em vista as profundíssimas alterações na distribuição social de trabalho entre os sexos e as novas estruturas familiares. De outro lado, o atual estágio de desenvolvimento da "ciência" da administração — nascida do pioneiro trabalho de Frederick Taylor, no fim do século XIX — permite à doutrina jurídica deitar ao lado as já gastas fórmulas do direito romano. Em suma, o paradigma do administrador competente deve substituir o do bom pai de família. O administrador diligente é aquele que emprega na condução dos negócios sociais as cautelas, métodos, recomendações, postulados e diretivas da "ciência" da administração de empresas." COELHO, Fabio Ulhoa. *Curso de Direito Comercial*, volume 2, direito de empresa. São Paulo: Saraiva, 2012, p. 313-314.

conjugação de qualificações técnicas ao administrador contemporâneo, não sendo suficiente a opção por um dirigente com conduta ilibada e retidão de caráter tão-somente; mormente, em mercados de alta complexidade negocial e intensa competitividade entre empresas.

Em linha, não há como se ostentar a pretensão de que seria suficientemente válida a conjugação adjetiva proposta pela Lei das Sociedades Anônimas para a eleição de um administrador. A escolha deste agente pelos principais deverá ser amplificada, sobretudo, conjugando a diligência buscada com a experiência corporativa do escolhido (*background*), isto é, levando em consideração as atividades a serem desenvolvidas, o setor ao qual pertence a companhia e, sobretudo, a sua qualificação[29]; tendo a lei fixado, salvo melhor juízo, um padrão mínimo de exigência.

Com efeito, a avaliação da conformidade do dever de diligência, em face das ações perpetradas pelo administrador, deverá levar em consideração o caminho percorrido ao longo do processo de tomada de decisão, ou seja, todas as variáveis que cercaram este percurso: independentemente, como ressalta a doutrina, da obtenção de uma vantagem econômica para a companhia ao final da jornada decisória[30].

Reforça-se que a imposição do referido dever aos

[29] Nesse sentido: "Em relação a este dever, durante muito tempo imperou a ideia de que o sucesso de uma empresa não estava necessariamente vinculado à formação técnica de seus administradores, existindo inúmeros exemplos de empreendedores com baixa escolaridade que construíram impérios empresariais. Talvez por esse motivo, a Lei de Sociedades Anônimas não tenha exigido qualificações técnicas ou formação específica para o cargo de administrador, até mesmo para que isso não gerasse qualquer entrave ao desenvolvimento da livre-iniciativa. No entanto, as exigências atuais do mercado não comportam mais um profissional que não tenha competências desenvolvidas, pelo menos no que tange à gestão." LUCAS, Lais. *Programas de integridade nas sociedades anônimas: implementação como conteúdo do dever de diligência dos administradores* Porto Alegre: Livraria do Advogado, , 2021, p. 145.

[30] ADAMEK, Marcelo Vieira von. *Responsabilidade Civil dos Administradores de S/A e as ações correlatas*. São Paulo: Saraiva, 2009, p. 132.

conselheiros e aos diretores visa à promoção do fim social da empresa. Neste sentido, revelam-se incompatíveis e injustificáveis quaisquer condutas culposas ou dolosas por eles praticadas.

Fixada a compreensão do dever de diligência, é necessário que se perquira qual o seu elemento normativo central. Dito de outra forma, aquilo que determina – dentro de uma considerável margem de discricionariedade como já exposto ao longo deste texto – que se admitida como adequado o comportamento do administrador em vista do caso concreto[31].

A resposta para tal indagação está amparada na coleção de dados e informações relevantes para a proteção do negócio obtidas pelo agente, sendo que pouco importa se as mesmas provêm dos diferentes setores internos à organização, se resultantes de um aprofundado estudo ou mesmo da contratação de consultoria especializada.

Portanto, gize-se, não se está a exigir do administrador, e nem seria cabível, um grau apurado de tecnicidade em toda matéria. Ao encontro da otimização do processo decisório, em que pese o fato de comprovada insuficiência de conhecimento, por isto mesmo, ele deverá buscar o melhor auxílio técnico possível para embasar a tomada de decisão[32].

---

[31] Nesta linha, julgado da CVM: "O dever de diligência é um dos deveres expressos sob a forma de uma cláusula geral. A lei societária se refere genericamente a um standard de conduta, deixando ao intérprete e ao aplicador ampla margem de discricionariedade na delimitação do conteúdo específico do dever de diligência. Quando bem utilizada, essa flexibilidade mostra-se de suma importância, na medida em que permite que o conteúdo do dever de diligência seja aferido à luz das circunstâncias do caso concreto." COMISSÃO DE VALORES MOBILIÁRIOS. Processo Administrativo Sancionador CVM nº 05/2016. Apurar possível inobservância de deveres fiduciários de administradores da Petrobras na construção da Refinaria Abreu e Lima. Infrações aos artigos 153, 154, §2º, "c", 155, e 163, I, da Lei n° 6.404/1976. Voto Diretor Gustavo Machado Gonzales, julgado em 03 de novembro de 2020, p.22. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/noticias/anexos/2020/20201103_PAS_CVM_SEI_19957_010647_2019_97_05_2016_voto_diretor_gustavo_gonzalez.pdf-4796a160193148b2a835fb6458616c1c. Acesso em 08 de setembro de 2022.

[32] Uma vez mais, veja-se o entendimento da autarquia anteriormente citada ao tratar

Assim, é cristalino que o elemento central do dever de diligência é o dever de informar-se, pois, o administrador deve conhecer a sociedade, o segmento de mercado, bem como os riscos associados à sua atividade[33]. Inclusive, buscando dirimir eventuais incertezas junto a *experts* sobre a matéria objeto da decisão como outrora afirmado.

Com base na diversidade e na qualidade das informações buscadas, o agente poderá firmar seu juízo e realizar o processo de tomada de decisão, ético, seguro e eficaz, direcionado aos resultados esperados pelo principal e demais interessados.

Essa decisão deverá ser sedimentada não apenas sob a observância de um dever de atuação diligente, mas também pelo estatuto social e pela regulamentação a ser observada pelo ente empresarial. Neste sentido, retomar-se-á o elemento nuclear do

---

do dever do administrador de informar-se: "Em linhas gerais, o dever de se informar requer que o administrador busque informações capazes de suportar as decisões negociais. O administrador não pode se esquivar das decisões negociais, alegando falta de competência ou de conhecimento. Todavia, não é razoável esperar que os membros do conselho de administração tenham expertise ou experiência para lidar com todos os assuntos da companhia que são levados à apreciação do conselho. Assim, reconhece-se que a melhor forma do administrador que se depara com um assunto que não domina dar concretude ao seu dever de se informar é por meio da consulta a um terceiro com expertise na área – advogado, economista ou contador, para citar apenas alguns exemplos – e capaz de lhe aconselhar a respeito da melhor decisão
acerca da matéria." COMISSÃO DE VALORES MOBILIÁRIOS. Processo Administrativo Sancionador CVM nº RJ2014/8013. Exercício abusivo do direito de voto e desvio de poder de administradores da HRT Participações em Petróleo S.A. Infração aos arts. 154, caput e art. 115 c/c o 159, §1 da Lei nº 6.404/76. Infração ao art. 12, caput, II e §5º da Instrução CVM nº 358/02. Multas. Absolvição. Voto Diretor Gustavo Machado Gonzales, julgado em 28 de agosto de 2018. Disponível em: https://conteudo.cvm.gov.br/sancionadores/sancionador/2018/20180731_PAS_RJ20148013.html. Acesso em 08 de setembro de 2022.

[33] Cabe ao administrador informar-se com o objetivo de qualificar-se. Assim, ensina a doutrina: "(...) o administrador deve ter ou adquirir os conhecimentos mínimos sobre as atividades da companhia e a competência necessária ao desempenho de suas funções, com capacidade técnica para tomar decisões de maneira refletida e responsável. Assim, se o administrador não possui conhecimentos mínimos que lhe permitam dirigir os negócios sociais, não deve aceitar o cargo." EIZIRIK, Nelson. *A Lei das S/A Comentada*. 2ª ed., vol. II. São Paulo: Quartier Latin, 2015, pág. 353.

presente estudo para demonstrar a existência de modernas normas, em nosso ordenamento e no estrangeiro, que determinam um dever de diligência frente às ameaças cibernéticas.

4. ATAQUES CIBERNÉTICOS: REGULAÇÃO E DEVER DE DILIGÊNCIA.

O ambiente no qual se encontram essas organizações impõe verdadeiros testes de resiliência empresarial[34], isto é, algo que poderia equivaler à seleção natural desses entes em face da adaptação ao meio em que transacionam serviços ou produtos.

A Comissão de Valores Mobiliários (CVM), , em 26 de maio de 2021, editou a Resolução CVM nº35[35], estabelecendo normas e procedimentos sobre a intermediação de operações sob sua tutela.

Assim, os intermediários[36] deverão adotar e implementar regras e procedimentos para o cumprimento da resolução: as condutas deverão ser escritas, comprováveis e disponíveis para consulta da autarquia e instituições autorizadas. Veja-se, existe um comando inequívoco do regulador que condiciona a atuação diligente do administrador.

Seguindo, a CVM impõe que o intermediário destaque, dentre seus quadros, dois diretores estatutários para, respectivamente, responsabilizarem-se pelo cumprimento das determinações estabelecidas, bem como para supervisionar os procedimentos e controles internos com vistas ao disposto na resolução em comento. Note-se que a resolução é direta no sentido de que se tratam de diferentes diretores, ampliando o

[34] Sobre desafios impostos às firmas e resiliência empresarial, ver: GARCIA, Ricardo Lupion. *O sonho da liberdade econômica, o pesadelo da pandemia do COVID-19 e a empresa resiliente.* Revista Jurídica Luso-brasileira, Ano 6, nº 4, 2020.

[35] Disponível em: https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html. Acesso em: 17/06/2022.

[36] Conforme disposto na Res. CVM nº35, art. 2º, inciso VII.

compromisso institucional pela aderência aos dispositivos no seio da alta direção corretamente.

Nessa quadra, faz-se necessário indicar quais os deveres impostos pelo regulador aos administradores da organização que atua como intermediária das operações reguladas pela CVM. A autarquia determina a necessidade de constituição de um plano de contingência negocial, indicando qual os critérios e procedimentos que nele deverão constar, i.e., com o objetivo de manutenção da continuidade negocial, proteção dos clientes e bom funcionamento do mercado.

A elaboração do mencionado plano de contingência é um dever do administrador, que terá de observá-lo em razão dos riscos associados às atividades que a organização intermediária desenvolve.

Os processos e sistemas críticos não podem sofrer interrupção para o bom funcionamento e credibilidade do mercado de capitais. Com isso, fazendo-se uma leitura sistemática do conteúdo deste artigo, nota-se que os ataques cibernéticos – visto tratarem-se da maior ameaça aos negócios segundo os administradores conforme demonstrado pelas pesquisas colacionadas na parte introdutória – devem ser contemplados no plano de contingência exigido pela CVM.

Não indiferente à realidade que se impõe, qual seja, a iminência de um ataque cibernético que interrompa as atividades do mercado de capitais nacional, a resolução manda que que implemente uma política de Segurança da Informação.

A preocupação da entidade reguladora do mercado de valores mobiliários brasileiro não está descolada da realidade, ao contrário, entende como inadiável a implantação de medidas que afastem ou mitiguem os riscos cibernéticos aos seus intermediários, mercado e clientes finais.

O movimento dos reguladores com vistas ao enfrentamento aos incidentes cibernéticos não ocorre, apenas, em território pátrio.

Neste ano, um dos marcos históricos da Governança Corporativa, a Lei Sarbannes-Oxley (SOx) completa 20 anos de edição. Numa síntese apertada, o diploma em destaque, segundo a doutrina[37]:

> "(...) promoveu ampla regulação da vida corporativa, fundamentada nas boas práticas de governança. Seus focos são, exatamente, os quatro valores que há duas décadas vinham sendo enfatizados pelo ativismo pioneiro. Vale repeti-los: 1. Compliance, conformidade legal; 2 accountability, prestação de contas; 3. Disclousure, mais transparência; e 4. Fairness, senso de justiça."

Notável a contribuição da SOx no sentido de não apenas reafirmar, mas de exigir a necessidade de comprovação de boas práticas de governança às companhias, seja em relação à conformidade legal, seja em face das demonstrações contábeis. Numa palavra, são emanados comandos à alta administração, impondo que respeitem e guardem observância aos princípios estabelecidos na legislação.

Nessa linha, em março do corrente ano, a *SEC – Security Exchange Comission*, o órgão regulador do mercado de valores mobiliários norte-americano, abriu consulta pública[38] a uma série de disposições que visam atualizar as demonstrações e condutas diligentes exigidas dos administradores em face dos riscos cibernéticos associados às atividades dos mercados de capitais. O procedimento consultivo encerrou-se em 09 de maio de 2022.

A SEC verificou um incremento exponencial dos riscos associados ao mercado regulado e, por isso, as medidas que padronizariam os relatórios de Cibersegurança trariam benefícios a todos os envolvidos[39].

---

[37] ROSSETI, José P. ANDRADE, Adriana. *Governança Corporativa: fundamentos, desenvolvimento e tendências*. 7. ed. – São Paulo: Atlas, 2014, p. 181.

[38] Disponível em: https://www.sec.gov/news/press-release/2022-39. Acesso em 16/06/2022.

[39] Conforme o SEC Chairman Gary Gensler ressaltou na oportunidade de divulgação da consulta pública: "Today, cybersecurity is an emerging risk with which public

Dessa forma, como feito há 20 anos com a SOx em relação às demonstrações contábeis e à conformidade legal, a SEC pretende exigir que às companhias comprovem que a alta direção detém habilidades em segurança cibernéticas. Essa comprovação padronizada não será baseada na quantidade ou nomenclatura de cargos, e sim na educação formal, especialização e experiência prática nesse tema.

Com base nesses dois movimentos regulatórios, CVM e SEC, fica nítido que os administradores têm o dever de atuar de modo diligente na prevenção e no enfrentamento dos ataques cibernéticos: de um lado, criando e promovendo políticas de Segurança da Informação; de outro, informando-se, qualificando-se e apropriando-se de *cyber skills*.

Provavelmente, o reflexo dessas medidas espalhar-se-ão em todas as economias desenvolvidas e emergentes, o que resultará numa acelerada promoção da cultura de Cibersegurança nas grandes empresas, agregando valor às marcas, credibilidade junto aos clientes, higidez aos mercados e maior resiliência empresarial[40].

Finalmente, resta investigar quais seriam as tendências em Cibersegurança para os próximos tempos, e como a governança poder fornecer uma solução jurídica para a atuação diligente do administrador frente a essa temática em constante evolução.

---

issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."

[40] Há quem entenda que elas deveriam ser ampliadas. Nesta linha, recomenda-se o texto de autoria de Shiva Rajgopal Professor de Contabilidade e Auditoria na Columbia Business School e Alex Sharpe fundador da Sharpe Consulting LLC, no *Harvard Law School Forum on Corporate Governance*, de 03/06/2022. Disponível em: https://corpgov.law.harvard.edu/2022/06/03/the-secs-cyber-disclosures/, Acesso em 18/06/2022.

5. CIBERSEGURANÇA COMO PARTE DA SOLUÇÃO JURÍDICA DA GOVERNANÇA: VISÃO GERAL E TENDÊNCIAS.

Em nossas vidas, as mudanças ocasionadas pela transformação digital vinculada às Tecnologias da Informação e Comunicação (TIC's) nos brindam com conveniência, escalabilidade, velocidade e, não se pode esquecer, graves riscos cibernéticos.

Como demonstrado ao longo do estudo, a implantação de medidas preventivas e protetivas de Segurança da Informação e governança devem ser conjugadas, aumentando com isto, significativamente, a esfera de atuação dos administradores no que guarda relação com o seu dever de diligência.

Na esteira dessa proposta, algumas ações se revelam mais importantes que outras, demandando atenção à listagem (não-exaustiva) que será destacada de modo a facilitar a sua implantação pelos administradores e, potencialmente, ajudar-lhes a cumprir com as exigências do seu dever de diligência.

A composição da alta administração, conselho e diretoria executiva, deve conter, pelo menos um, especialista em Cibersegurança. Evidentemente, está-se a falar de posição estratégica, levando-se em consideração o porte, o mercado e os riscos associados à atividade empresarial. Uma boa prática recomendada é a de que o CISO (Chefe de Segurança da Informação) tenha lugar de fala junto ao *Executive Board*[41], ocupando assento no conselho ou em comitê de enfrentamento aos riscos cibernéticos[42].

---

[41] Veja-se a previsão da consultoria Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-. Acesso em 18/06/2022.

[42] Especialistas defendem a criação de um Cyber Hub, algo como um comitê multidisciplinar dedicado ao tema da Cibersegurança institucional. Leia-se: BROOKS, Chuck. *A Cybersecurity Risk Management Strategy for the C-Suite*. HS Today, 11/05/2022. Disponível em: https://www.hstoday.us/featured/a-cybersecurity-risk-management-strategy-for-the-c-suite/. Acesso em 18/06/2022.

Outro ponto fundamental é que a Cibersegurança deve ser parte da estratégia organizacional: não é admissível que a companhia tenha uma visão restritiva, definindo que as questões relativas aos riscos cibernéticos sejam de exclusiva responsabilidade da área de Segurança da Informação. Ao revés, para que a estratégia tenha sucesso, é necessário que se tenha uma visão holística do tema, encarando-o como um problema da corporação.

Ao encontro do acima exposto, é imprescindível que sejam destinados recursos financeiros e humanos suficientes o bastante para fazerem frente às ameaças verificadas numa prévia avaliação de riscos vinculados ao setor e atividades exercidas pela sociedade. Estes recursos devem ser direcionados à promoção da política de segurança da informação, a treinamentos de todos os colaboradores da companhia, bem como da cadeia de fornecedores: onde, muitas vezes, pode estar o elo mais fraco da rede de proteção aos ataques cibernéticos[43]. Ademais, invista-se na realização de testes periódicos e, a partir dos resultados, os indicadores-chave para a área responsável pela gestão de riscos cibernéticos.

Finalmente, devem ser considerados os pilares fundamentais de uma adequada estratégia de Cibersegurança, quais sejam: *security by design*, defesa profunda e *zero trust*.

O *security by design* realiza com perfeição a interface entre a governança e a gestão de riscos de segurança cibernéticas, fazendo com o que os responsáveis pelo tema na organização previnam, detectem e eliminem as principais ameaças à continuidade dos negócios. Trata-se de uma forma de avaliação de risco antecipada, que busca integrar a empresa como um todo, de forma contínua e gerenciada.

A defesa profunda se refere à máxima proteção das

[43] Exemplifica-se: *Ex-NSA hacker says a supply chain cyberattack is one of the things that keeps him up at night*. Disponível em: https://www.cnbc.com/2021/10/25/ex-nsa-hacker-says-a-supply-chain-cyberattack-is-one-of-the-things-that-keeps-him-up-at-night.html. Acesso em 19/06/2022.

estruturas de tecnologia da informação, concebida em diversas camadas relativas à arquitetura de segurança, aos serviços em nuvem, à integridade do banco de dados e demais áreas estratégicas sensíveis aos potenciais incidentes cibernéticos.

O conceito *zero trust* pressupõe a ausência de confiança em usuários, ativos e recursos envolvidos com a companhia. Sua aplicação pode influenciar na autenticação dos usuários, na manutenção de arquivos em locais fora da sede das empresas, protegendo os recursos em sua integralidade, e não apenas as redes corporativas.

Todos os pilares mencionados anteriormente devem ser combinados conforme o porte, o segmento de atuação e o mercado onde a empresa se insere. Isto, como de forma a entregar a mais robusta defesa cibernética à organização, fazendo parte de uma decisão fundamental dos administradores, lastreada no impositivo dever de diligência e, ao mesmo tempo, integrada à solução jurídica de Governança Corporativa.

6. CONSIDERAÇÕES FINAIS

Ao transcorrer do presente artigo, buscou-se trazer o atento leitor à realidade que se impõe, qual seja, o ambiente empresarial está sob ataque: iniciativas desleais, a partir de um inimigo sem rosto e que não se prende a determinadas fronteiras. Atualmente, estas investidas silenciosas e, muitas vezes, imperceptíveis às organizações trazem consigo a falsa impressão de que o problema não existe, revelando aparente calmaria e tranquilidade: um erro crasso, e que pode custar a própria continuidade dos negócios do ente empresarial.

As pesquisas colacionadas ao longo do trabalho já indicam que os ataques cibernéticos ocupam posição destacada entre os principais desafios impostos aos administradores das companhias. Entretanto, mais que identificar esta informação, deve o administrador atuar – diligentemente – para prevenir que

sua companhia seja atingida, bem como preparar-se para mitigar os efeitos de um incidente cibernético que a estrutura protetiva empresarial não consiga deter.

Dessa feita, em face da exponencial quantidade, bem como em razão do recrudescimento desses incidentes, exige-se o necessário e inadiável enfrentamento deste assunto pelos administradores. O dever de diligência ao qual se submetem demanda que assim o façam, evitando a um só tempo os prejuízos tangíveis e os intangíveis relacionados a esse tipo de ataque. Muitas vezes, o este último pode decretar uma perda de credibilidade e relação ao ente empresarial alvo dos *hackers*, o que pode minar, para sempre, a sua atuação junto ao mercado e à sociedade.

Não por menos, órgãos de regulação – nos principais mercados globais – têm se ocupado de exigir das companhias a elaboração e a implantação comprovada de medidas técnicas e administrativas que evitem esse tipo de ocorrência ou, ao menos, que garantam um elevado nível de proteção aos seus negócios, isto é, de modo a evitar prejuízos sistêmicos ao mercado no qual desenvolvem suas atividades o que, a depender do porte e da larga influência da companhia, pode ocorrer sem maiores dificuldades.

Com isso, assevera-se a conjugação inescapável de esforços no sentido de indicar a impreterível atuação sinérgica entre as boas práticas de Governança Corporativa e as políticas de Segurança da Informação. Este somatório de condutas orientadas em direção à prevenção e à manutenção da continuidade dos negócios deve ser componente de uma solução jurídica eficaz, partindo da decisão informada, devidamente sopesadas as características de cada companhia, dos seus conselhos de administração e executivos-chefes.

Finalmente, pretende-se sublinhar que existe importante tarefa a ser cumprida pelos atuais administradores, e o enfrentamento a esta dura e indesviável ameaça está – de fato e

por imposição legal – contida na roupagem do dever de diligência dos dirigentes das sociedades abertas.

7. REFERÊNCIAS

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

ALLIANZ GROUP. *Allianz Risk Barometer 2022*. Disponível em: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. Acesso em: 15/06/2022.

ÁVILA, Humberto. *Teoria dos Princípios*. 16.ª ed. São Paulo: Malheiros, 2015.

BLOK, Marcella. Compliance e Governança Corporativa. 3ª ed. São Paulo: Freitas Bastos Editora, 2020.

BRASIL. CVM – Comissão de Valores Mobiliários. Resolução CVM nº 35, 2021.

_____. CVM – COMISSÃO DE VALORES MOBILIÁRIOS. *Processo Administrativo Sancionador CVM nº RJ2014/8013*.

_____. CVM – COMISSÃO DE VALORES MOBILIÁRIOS. *Processo Administrativo Sancionador CVM nº 05/2016*.

BRASIL. Decreto federal nº 10.222, de 05 de fevereiro de 2022.

BRASIL. Lei das Sociedades Anônimas nº 6.404/1976.

BROOKS, Chuck. *A Cybersecurity Risk Management Strategy for the C-Suite. HS Today*, 11/05/2022. Disponível em: https://www.hstoday.us/featured/a-cybersecurity-risk-management-strategy-for-the-c-suite/ . Acesso em 18/06/2022.

CNBC. *Ex-NSA hacker says a supply chain cyberattack is one of the things that keeps him up at night.* Disponível em: https://www.cnbc.com/2021/10/25/ex-nsa-hacker-says-a-supply-chain-cyberattack-is-one-of-the-things-that-keeps-him-up-at-night.html . Acesso em 19/06/2022

COELHO, Fabio Ulhoa. *Curso de Direito Comercial*, volume 2, direito de empresa. São Paulo: Saraiva, 2012.

EIZIRIK, Nelson. *A Lei das S/A Comentada*. 2ª ed., vol. II. São Paulo: Quartier Latin, 2015.

ESTADOS UNIDOS DA AMÉRICA. SEC – Security and Exchange Comission. Disponível em: https://www.sec.gov/news/press-release/2022-39. Acesso em 16/06/2022.

_____. NSA – National Security Agency. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/. Acesso em 16/06/2022.

GARCIA, Ricardo Lupion. *O sonho da liberdade econômica, o pesadelo da pandemia do COVID-19 e a empresa resiliente.* Revista Jurídica Luso-brasileira, Ano 6, nº 4, 2020.

GARTNER GROUP. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated- . Acesso em 18/06/2022.

HARVARD LAW SCHOOL. *Forum on Corporate Governance*, de 03/06/2022. Disponível em: https://corpgov.law.harvard.edu/2022/06/03/the-secs-cyber-disclosures/ . Acesso em 18/06/2022.

IBGC – Instituto Brasileiro de Governança Corporativa. *Código das melhores práticas de governança corporativa.* 5ª edição. São Paulo: IBGC, 2015.

IBGC – Instituto Brasileiro de Governança Corporativa.

Governance Officer. São Paulo: IBGC, 2022

IBM Security. *Cost of a data breach report 2022*.

JENSEN. Michael C. MECKLING. William H. *Theory of the firm: managerial behavior, agency costs and ownership structure*. Journal of Financial Economics, October, 1976, V. 3, No. 4.

LORIA, Eli; KALANSKY, Daniel. *Processo sancionador e Mercado de Capitais V: Estudo de Casos e Tendências: Julgamentos da CVM*. São Paulo: Quartier Latin, 2021.

LUCAS, Lais. *Programas de integridade nas sociedades anônimas: implementação como conteúdo do dever de diligência dos administradores*. Porto Alegre: Livraria do Advogado, 2021.

MORGAN, Steve. *Cybercrime to Cost The World $10.5 trillion annually by 2025*. CYBERCRIME MAGAZINE, 13/11/2020.

OCDE – Organização para a Cooperação e Desenvolvimento Econômico. Corporate Governance Principles, 2015.

ROSSETI, José P. ANDRADE, Adriana. *Governança Corporativa: fundamentos, desenvolvimento e tendências*. 7. ed. – São Paulo: Atlas, 2014.

SCHWAB, Klaus; VANHAM, Peter. Stakeholder Capitalism: A Global Economy that Works for Progress, People and Planet. John Wiley & Sons: New Jersey, 2021.

SCHWAB, Klaus. The Fourth Industrial Revolution. New York: Currency Books, 2017.