PRISMA JURÍDICO
COPE Member since 2020 JM14464
e-ISSN: 1983-9286
ISSN: 1677-4760

Recebido em: 11 maio 2024 / **Aprovado em:** 29 ago. 2024
Editor: Prof. Dr. José Fernando Vidal de Souza
Processo de Avaliação: *Double Blind Review*
http://doi.org/10.5585/2024.26656
Artigo

Check for updates

Distopia cibernética e meio ambiente digital

Cybernetic dystopia and digital environment

Willian Ryutaro Kobe

Mestrando pelo Programa de Pós-Graduação em Direito (PPGD) da Pontifícia Universidade Católica do Paraná (PUCPR)

Pontifícia Universidade Católica do Paraná (PUCPR)

Curitiba, PR – Brasil

willian.kobe@pucpr.edu.br

Heline Sivini Ferreira

Mestrando em Direito
Doutora em Direito pela UFSC. Mestre em Direito pela UFSC.

Pontifícia Universidade Católica do Paraná (PUCPR)

Curitiba, PR – Brasil

Cinthia Obladen de Almendra Freitas

Professora Titular da Escola de Direito da PUCPR e Professora Permanente do Programa de Pós-Graduação (Mestrado/Doutorado) em Direito (PPGD) da PUCPR.
Mestre em Engenharia Elétrica e Informática Industrial pela Universidade Tecnológica Federal do Paraná (1990)

Pontifícia Universidade Católica do Paraná (PUCPR)

Curitiba, PR – Brasil

Resumo: A exploração excessiva de dados no meio digital perturba o equilíbrio do meio ambiente digital, gerando riscos concretos conforme a Teoria de Beck. A pesquisa abordou exemplos de vazamentos de dados, como os do Grupo Meta em 2018, da Microsoft em junho de 2023 e do programa Auxílio Brasil do Governo Federal em 2022. Isso cria uma distopia cibernética onde a segurança do ciberespaço e das pessoas que a ele se vinculam é comprometida. A pesquisa investiga se esses riscos podem ser mensurados e mitigados juridicamente. A hipótese é que a nocividade desses riscos é imensurável, mas pode ser contida

pelo Direito. Conclui-se que a legislação deve promover o debate e a regulamentação para proteção de dados, visando combater os riscos concretos mencionados.

Palavras-chave: sociedades; novas tecnologias; meio ambiente digital; riscos; dados.

Abstract: The excessive exploitation of data in the digital realm disrupts the balance of the digital environment, generating concrete risks according to Beck's Theory. The research addressed examples of data leaks, such as those from Meta Group in 2018, Microsoft in June 2023, and the Federal Government's Auxílio Brasil program in 2022. This creates a cybernetic dystopia where cyberspace security and the people connected to it are compromised. The research investigates whether these risks can be legally measured and mitigated. The hypothesis is that the harmfulness of these risks is immeasurable but can be contained by law. It is concluded that legislation should promote debate and regulation for data protection, aiming to combat the mentioned concrete risks.

Keywords: societies; new technologies; digital environment; risks; data.

Para citar este artigo

ABNT NBR 6023:2018

KOBE, William Ryutaro; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. Distopia cibernética e meio ambiente digital. *Prisma Jurídico,* São Paulo, v. 23, n. 2, p. 315-335, jul./dez. 2024. http://doi.org/10.5585/2024.26656

1 INTRODUÇÃO

O meio ambiente, apesar de ser uno e indivisível, abrangendo todos as suas espécies em um único sistema organizado e equilibrado, doutrinariamente pode ser classificado para melhor compreensão e esquematização do conhecimento. Neste contexto, surgiram classificações como o meio ambiente digital, hoje expressado principalmente pela Internet. Na Internet, a principal expressão do ciberespaço, os dados são os componentes basilares desse ecossistema e tem elevado valor, tal como se observa em práticas de publicidade direcionada de acordo com as preferências pessoais a partir do perfilamento do titular de dados.

Esse valor dos dados atrai interesses mercadológicos que buscam explorar esse recurso, e com a exploração excessiva, surgem os riscos, na acepção da Teoria de Beck (2002) que norteia o presente artigo, como frutos de intervenções humanas neste meio ambiente digital,

vez que toda forma de meio ambiente se encontra em um perfeito equilíbrio e se mostra sensível às mudanças, como um verdadeiro sistema caótico. Esses riscos podem ser enxergados tanto de forma abstrata, representando a sociedade do risco sob a perspectiva do ciberespaço, mas, também, se manifestam de forma concreta em situações que envolvem o tratamento inadequado de dados, em especial o vazamento de dados que é o foco do presente artigo.

Logo, buscou-se exemplificar tais riscos concretos por meio de três casos de vazamento de dados que ocorreram recentemente e afetaram milhões de pessoas, sendo representativos de riscos concretos que assolam o meio ambiente digital e amplamente divulgados na mídia. São eles a) o vazamento de dados relativo ao grupo Meta em 2018; b) Vazamento de 38 terabytes de dados internos da Microsoft em 2023; e c) vazamento de dados pessoais vinculado ao programa Auxílio Brasil do Governo Federal em 2022.

Todo esse contexto indica, preliminarmente, que o meio ambiente digital passa por uma situação distópica ao estilo Cyberpunk abordado na obra Neuromancer (Gibson, 1991), ou seja, uma distopia cibernética em que os riscos, gerado pela exploração excessiva dos dados, minam a segurança do próprio ciberespaço e das pessoas que se conectam a ele.

Diante de todo esse cenário, surge a seguinte pergunta de pesquisa: a nocividade dos riscos gerados pelas companhias e entes estatais no ciberespaço é mensurável, bem como seus efeitos podem ser contidos ou mitigados de alguma forma pelo Direito? Com base neste panorama, formulou-se a seguinte hipótese: a nocividade dos riscos concretos gerados pelas companhias e entes estatais no meio ambiente digital são imensuráveis, mas ainda podem ser contidos com o enfrentamento adequado pelo Direito.

Em relação à metodologia, cabe destacar que o artigo, a ser desenvolvido, pode ser classificada, quanto à abordagem do problema, como qualitativa, visto que busca analisar o fenômeno do meio ambiente digital e os riscos que o cercam. Quanto aos objetivos, se trata de pesquisa descritiva, com foco na compreensão e estudo do meio ambiente digital buscando descrever suas características, as correlacionando com outras teorias, tal como a de risco. Em relação aos procedimentos técnicos, a pesquisa pode ser classificada como bibliográfica, vez que busca se estruturar teoricamente a partir de livros, artigos e demais materiais sobre a temática.

Por fim, com base nessas premissas de pesquisa, espera-se como resultado que a nocividade dos riscos é de fato imensuráveis, ao passo em que existem meios de enfrentamento desses riscos, e seus efeitos, pelo Direito. Feitas considerações introdutórias, passa-se ao desenvolvimento do artigo.

2 MEIO AMBIENTE DIGITAL, RISCO E DADOS

O meio ambiente, apesar de ser uno e indivisível, abrangendo todos as suas espécies em um único sistema organizado e equilibrado, doutrinariamente pode ser classificado para melhor compreensão e esquematização do conhecimento.

Diante deste contexto, concebeu-se o conceito de meio ambiente digital, sendo definido por Coutinho (2014, p. 223) da seguinte maneira:

> Junte-se a este ponto a ideia de existência do meio ambiente digital como manifestação da criação humana e parte integrante do patrimônio imaterial, sobretudo representado pela tecnologia do espectro eletromagnético (ondas de rádio, TV, celular e internet) que deve estar a serviço do desenvolvimento (sustentável) e, portanto, lucro e desenvolvimento aliado à preservação do meio ambiente (art. 218, CF).

Analisando a referida definição, extrai-se que o meio ambiente digital é uma faceta imaterial do meio ambiente, sendo este o ponto que interessa ao presente estudo. Justamente por seu caráter imaterial, intangível e virtual, o referido ecossistema digital acaba por se instituir e se difundir com extrema facilidade, superando fronteiras e alcançando um número avassalador de sujeitos, estes últimos, evidentemente, intimamente conectados com este meio ambiente, tornando-se indissociáveis.

Neste ponto, e partindo da premissa de que a Internet é a principal expressão atual do meio ambiente digital, a definição de Castells (2003, p. 87) de que a cultura da Internet é caracterizada por uma fé na progressão humana por meio da tecnologia, impulsionada por comunidades que valorizam a liberdade criativa tecnológica integrada em redes virtuais que buscam transformar a sociedade e este cenário, por sua vez, atrai empreendedores motivados pelo lucro na economia digital emergente, se torna visível o surgimento da intenção exploratória deste potencial emergente. Neste sentido, pondera Capra (2006, p. 8) que o advento tecnológico proporcionou a reformulação do próprio capitalismo, que, por sua vez, modificou severamente o meio ambiente digital, visto que o valor da informação passa impactar o mercado que percebe uma oportunidade de sua exploração. Logo, já neste ponto se torna perceptível que neste espaço cibernético que surgiu diante do avanço e integração tecnológicos, surgiu, também, uma exploração deste espaço, o qual passa despercebido pelas pessoas que integram o referido ambiente, vez que a liquidez, na acepção de mudança constante, da Internet atrofia o sentido dos sujeitos que ali se inserem, fazendo com que na maioria das vezes, não perceba a exploração que ocorre por trás dos serviços que utilizam, ou dos conteúdos que consomem. E nesta direção,

frisa-se que o alcance amplo e a fluidez das tecnologias digitais, certamente, remetem ao conceito de liquidez defendida por Bauman (2001, p. 7), em especial a ideia de que "os fluidos não se atêm muito a qualquer forma e estão constantemente prontos (e propensos) a mudá-la".

Por sua vez, essa fluidez também se relaciona com a versatilidade da Internet, bem como de sua capacidade de conectar pessoas e seus dispositivos, praticamente, ignorando as distâncias físicas, esta tecnologia se difundiu rapidamente, se tornando praticamente onipresente na sociedade atual, como bem definido por Cavedon et al. (2015. p. 201): "a informática torna-se onipresente no cotidiano das pessoas, congregando uma variedade de riscos que não podem ser facilmente percebidos ou identificados".

Ademais, neste contexto, se extrai da literatura acerca da temática que os dados são componentes essenciais desse ecossistema. Nos ensinamentos de Doneda (2011, p. 94), têm-se que os dados são componentes basilares dessa estrutura imaterial, sendo elemento primário no referido ambiente, estando associado "a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração". Em convergência à ideia de que os dados são componentes basilares do meio digital, cabe apresentar a ideia de Devenport (1998, p. 19), o qual, primeiramente, define os dados como "observações sobre o estado do mundo. Por exemplo: 'existem 697 unidades no armazém'. A observação desses fatos brutos, ou entidades quantificáveis, pode ser feita por pessoas ou por uma tecnologia apropriada." Por sua vez, ainda de acordo com Davenport (1998, p. 19), os dados podem ser processados para se tornarem informações, a qual, ao seu turno, também pode ser aprimorada para se tornar conhecimento, criando uma relação piramidal, na qual o conhecimento se encontra na parte superior e os dados na parte inferior, refletindo o caráter constitutivo dos dados em meio a esse ecossistema. Outrossim, neste mesmo sentido assevera Freitas (2022, p. 238), acerca dos dados que existe um: "ecossistema de dados (data ecosystems), envolvendo organizações complexas de relações sociais dinâmicas por meio das quais dados e informações se movem e se transformam."

Desta forma, se observa o caráter essencial, ou basilar, dos dados, ainda que estes não sejam necessariamente o destino ou forma final das operações realizadas no meio ambiente digital, certamente embasam todas as práticas ocorridas no referido ambiente, tal como a publicidade direcionada, sendo constantemente coletados, inseridos e processados, com ou sem finalidade econômica, por motivos lícitos ou ilícitos, sendo inegável que os dados formam a base de um verdadeiro ecossistema digital (Zuboff, 2020, p. 154). Oportuno destacar que os dados, por constituírem o meio ambiente digital, desempenham papel semelhante às riquezas encontradas na natureza, denominadas pelo Capital como "recursos naturais", sofrendo a

mesma destinação, isto é a exploração econômica, muitas vezes, excessiva e que afeta o equilíbrio do sistema, conforme será explorado nos capítulos seguintes deste artigo.

Logo, em análise conjunta das ideias de Devenport, Doneda e Freitas, supracitados, verifica-se que os dados são componentes essenciais do meio ambiente digital. Assim, compilando todas essas informações, extrai-se que o meio ambiente digital, hoje expressado massivamente pela Internet, ostenta as seguintes características: a) imaterialidade, vez que se compõe em um espaço intangível fisicamente; b) fluidez, pois, diante da conexão, permite tráfego rápido de informações e se encontra em constante mudança, e c) dados como componentes essenciais, vez que se constitui a partir da menor unidade desse sistema que, por sua vez, é injetado em quantidade imensa a todo momento.

Uma vez fixada a ideia de que o meio ambiente digital é um sistema complexo, bem estruturado e com características próprias, cabe, então, explorar a referida complexidade.

Nitidamente, o referido ambiente digital se trata de um sistema caótico, não no sentido pejorativo do termo, como se difunde no senso comum, e sim no contexto científico, ou seja, a ciência do caos. Para Gleick (1987, p. 16-17) alguns sistemas são extremamente sensíveis às alterações das condições iniciais, ou seja, sensíveis às oscilações e mudanças, de modo que uma modificação, aparentemente insignificante, nos termos iniciais, provoca uma deturpação ao longo dos desdobramentos observáveis, tornando praticamente impossível a sua previsão ou levando a resultado totalmente diverso daquele esperado. A título exemplificativo, pode ser compreendido como oscilações a indução ao aumento de tráfego de dados, tal como ocorre com a disponibilização de serviços “gratuitos” como redes sociais e conteúdo de streaming que mantém os usuários entretidos por horas em uma plataforma, bem como a coleta excessiva desses dados para fins mercadológicos. Essa coleta excessiva, poderá deturpar o equilíbrio digital, gerando riscos em torno de incidentes de segurança, tal como o vazamento de dados.

Ou seja, refletindo acerca deste caráter caótico entorno do ecossistema de dados, como acabou de se destacar, percebe-se que as referidas oscilações podem ser compreendidas como os riscos gerados pela ação humana, visto que, tanto a indução ao aumento do tráfego de dados, bem como a sua exploração, ocorre por ações e interesses humanos, seja pelo emprego de tecnologias desenvolvidas para tal finalidade ou por tomada de decisões inadequadas envolvendo o tratamento dos aludidos dados. Assim, partindo da premissa de que esses riscos se originam a partir da intenção de exploração excessiva dos dados, percebe-se aqui a aplicabilidade da teoria de Ulrich Beck, normalmente utilizada ao conceito de meio ambiente clássico, natureza, e catástrofe global.

Na medida em que se compreende e se enxerga o meio ambiente digital como uma das facetas do conceito amplo e abrangente de meio ambiente, verifica-se que o ambiente digital também está vulnerável aos riscos induzidos pelo ser humano, como se destacou anteriormente com a coleta e exploração excessiva de dados. Neste sentido, para melhor correlacionar os riscos digitais com a teoria do risco, faz-se necessário elencar alguns conceitos do autor. Em primeiro momento, cabe destacar que, para Beck (2002, p. 78) os "perigos" se distinguem fundamentalmente dos "riscos" devido a origem daquele não estar ligada a escolhas deliberadas deste, ou seja, escolhas que visam benefícios e oportunidades econômicas e tecnológicas, enquanto encaram as ameaças como inerentes à face sombria do avanço. Diante deste primeiro ponto, têm-se que os fatores indicados no parágrafo anterior não se confundem com meros perigos, vez que não se originam naturalmente. Por sua vez, ainda de acordo com o autor (2002, p. 84), os riscos perdem sua delimitação no tempo e no espaço e, com isso, seu significado, tornando-se um evento com começo, mas sem fim, um verdadeiro evento progressivo de destruição. Ao seu turno, Beck (2002, p. 86) sustenta que a rotina diária não percebe os riscos que a circundam e, assim, nas escolhas pessoais, confia em "especialistas", não se limitando apenas ao possível dano decorrente dos riscos, mas também à ideia de que essa privação sensorial causada pelos riscos globais torna a vida incerta.

Em suma, é possível sintetizar e estruturar as principais ideias da teoria do risco, segundo o autor, da seguinte forma: a) os riscos não se originam naturalmente, sendo criação humana a partir de tomada de decisões; b) não se delimitam no tempo e no espaço, podendo se proliferar para além do local em que foi produzido e extrapolar os efeitos temporais de sua origem; e c) ocorrem no contexto de privação sensorial, de modo que são praticamente imperceptíveis àqueles que estão vulneráveis aos seus efeitos, isto é toda a sociedade.

Portanto, fixadas as principais ideias acerca da teoria do risco, cabe correlacioná-las ao meio ambiente digital. Diante da análise das bases teóricas acerca do ambiente digital, se constatou se tratar de uma faceta do grande conceito de meio ambiente, o qual é uno e indivisível, sendo dividido somente para fins de estudo. Logo, uma vez enxergado como uma dimensão desse grande conceito, o meio ambiente digital, também, demonstrou manter um equilíbrio próprio por meio de seu ecossistema de dados, evidenciando sua complexidade inerente à interconexão mundial e sua formação por inúmeros aparelhos eletrônicos conectados, contendo uma rede essencialmente caótica, ou seja, um sistema complexo e sensível, estando vulnerável às intervenções humanas.

Partindo-se desta premissa, subsome-se a teoria do risco de Ulrich Beck ao meio ambiente digital quando se observa que: a) os riscos no meio ambiente digital são criados a

partir de vontade humana, em especial com intenção de exploração econômica, principalmente por empresas, em especial as Big Techs, de modo que até mesmo os Estados e seus Governos podem contribuir com esses riscos, sendo oportuno consignar que segundo Freitas (2022, p. 228) o "tratamento de dados pessoais está (ou pode estar) vinculado ao surgimento de riscos capazes de comprometer a qualidade de vida do homem (titulares de dados)"; b) não se restringem no tempo e no espaço em que se originou, justamente pelo caráter de interconexão global da Internet que permite integrar os pontos mais remotos do planeta, fazendo com que os riscos produzidos se difundam por todo o meio ambiente; e c) ocorrem num contexto em que os usuários e titulares de dados não são cientificados, muitas vezes sofrendo com coleta de dados clandestinamente ou de forma obscura, eivando o seu consentimento ao passo que nem sempre os dados extraídos são tratados de forma segura, se mostrando como verdadeira privação sensorial.

Desta forma, considerando que o risco está presente no meio ambiente digital, surge a necessidade de mitigação desses riscos, visto que, conforme explicado por Freitas (2022, p. 244), têm-se que "a proteção de dados pessoais pode ser um evento dentro da análise de riscos, visto que quando os dados pessoais" e no momento em que esta proteção não ocorre, como em casos de vazamentos, "tal evento leva à violação potencial de todos os direitos fundamentais dos titulares dos dados afetados por operações de tratamento de dados."

Portanto, extrai-se que os riscos, na acepção de Beck (2002), possuem uma dimensão abstrata na medida em que são representativos da sociedade de risco e se refletem na liquidez de Bauman (2001) e aqui consubstanciado na ideia de exploração excessiva do meio ambiente digital, mas, também, contam com uma dimensão concreta, comumente manifestada no ciberespaço por meio de incidentes de segurança, em especial os vazamento de dados que serão abordados e exemplificados adiante.

Assim, encerra-se a presente seção com a exploração e diálogo das teorias apresentadas que permitem constatar que o meio ambiente digital existe, tem sua importância como qualquer outra faceta da natureza e está suscetível a riscos, merecendo tutela, formando, assim, a base teórica para o presente artigo, na qual será erigida toda tentativa de resposta à pergunta inicialmente formulada. Outrossim, na seção seguinte serão abordados os riscos concretos, ou casos reais, envolvendo exploração indevida de dados no meio ambiente digital, buscando se analisar a extensão da nocividade dos riscos.

3 RISCOS CONCRETOS GERADOS NO MEIO AMBIENTE DIGITAL

É imperioso revisitar a forma como o conceito de risco é introduzido e explorado nas análises propostas. Ao discernir entre o risco concreto e o risco abstrato, Beck utiliza este último como uma representação da sociedade de risco. Essa abstração, assim como a noção de liquidez de Bauman (2001) mencionada no parágrafo supra, ressalta a complexidade e a mutabilidade dos desafios enfrentados em um mundo em constante transformação.

A distinção entre risco concreto e risco abstrato, como proposta por Ulrich Beck, revela uma perspectiva fundamental para compreensão das dinâmicas contemporâneas da sociedade. Enquanto os riscos abstratos envolvem incertezas difusas e interconectadas, como as relacionadas à tecnologia, meio ambiente e economia globalizada e ressoa com a teoria da liquidez de Bauman (2001), como foi explicado anteriormente, e que descreve a natureza fluida e evanescente das estruturas sociais e individuais na era contemporânea e não estão densificados para aplicação num cenário real, os riscos concretos tomam rumo distinto. Os riscos concretos podem ser identificados de forma tangível e mensurável, como desastres naturais, pandemias, ou falhas de segurança em infraestruturas críticas. Estes eventos têm impactos diretos e imediatos no meio ambiente, material ou digital, bem como nas pessoas a eles interligadas. Reconhecer e abordar esses riscos demanda estratégias específicas de mitigação, preparação e resposta. É crucial uma gestão eficaz desses riscos concretos para proteger indivíduos e seus direitos, diante de tais adversidades. Nesse sentido, entender a natureza e a dinâmica desses riscos é fundamental para promover políticas públicas e práticas de segurança adequadas às necessidades e realidades locais e globais. Deste modo, indicar a existência desses riscos é o primeiro passo para seu enfrentamento.

Logo, para que seja possível propor eventual forma de mitigação dos riscos concretos, necessário verificar como estes riscos concretos se manifestam. Aqui se elegeu três casos de vazamentos como representativos de riscos concretos. A escolha ocorreu em razão de dois dos vazamentos terem partido de duas companhias gigantes do ramo da tecnologia (Big techs), aqui se referindo e um dos casos ter partido do ente estatal. O primeiro caso diz respeito ao vazamento de dados vinculado ao grupo Meta no ano de 2018, responsável pela gestão e manutenção de redes sociais notoriamente populares como Facebook, Instagram, e WhatsApp, indicando que um vazamento oriundo desta empresa afetaria inúmeros usuários. Ao seu turno, o segundo caso de vazamento partiu da empresa Microsoft, responsável pela oferta e manutenção de um dos sistemas operacionais mais utilizados no mundo (Steiw, 2023), conectando diversos dispositivos e usuários, de modo que um incidente de segurança gerado

por uma empresa deste porte, igualmente afetaria uma quantidade elevada de titulares de dados. Por fim, o terceiro caso de vazamento decorreu do Governo Federal, quando dados pessoais vinculados ao programa Auxílio Brasil foram violados, sendo a demanda, dada a relevância, judicializada e amplamente divulgada, indicando que os riscos no meio ambiente digital podem surgir até mesmo por parte de entes estatais. Em suma, os três exemplos foram eleitos diante da relevância e repercussão, sendo oportunos para possibilitar um estudo mais acurada.

Feitas conceituações e estabelecidas premissas teóricas, passa-se a explorar os exemplos de riscos concretos que impactam o meio ambiente digital.

No ano de 2018 ocorreu o vazamento de dados relativo ao grupo Meta, no qual, de acordo com jornal Globo (Zuba, 2023), "invasores acessaram as contas de cerca de 29 milhões de brasileiros". Diante do ataque, dados pessoais de milhões de usuários acabaram sendo obtidos indevidamente pelos invasores, dados como "gênero, localidade, idioma, status de relacionamento, religião, cidade natal, data de nascimento, dispositivos usados para acessar o Facebook, educação, trabalho e os últimos dez locais onde estiveram ou foram marcadas". O caso ocorreu em razão de "vulnerabilidade do sistema também permitiu que hackers instalassem de maneira remota um tipo de software espião em alguns telefones, para ter acesso a dados dos aparelhos".

Conforme sedimentado anteriormente, o meio ambiente digital é formado pelo tráfego de dados, dentre eles os dados pessoais, objeto de tratamento, no presente caso, por uma empresa de porte gigante, com a finalidade de exploração econômica, já que seus serviços não são normalmente remunerados de forma direta pelo usuário, sendo necessário o tratamento dos dados coletados para venda a terceiros, os quais os utilizarão para atender às suas pretensões mercadológicas, como direcionar a publicidade ao grupo certo e aumentar as chances de venda de um produto ou serviço.

Neste contexto, se faz evidente a gravidade da falha pelo grupo Meta, visto que produziu concretamente um risco ao meio ambiente digital, consistente em concentrar um grande fluxo de dados sem lhes oferecer uma proteção adequada, permitindo seu vazamento e maculando o equilíbrio do ambiente digital.

Recapitulando os conceitos anteriormente abordados, uma vez que o ambiente digital é formado pelo tráfego de dados, e que seu adequado tratamento está intimamente ligado com segurança e equilíbrio do meio ambiente digital e as pessoas conectadas a si, evidente que um incidente de violação dos dados se traduz na violação ao meio ambiente ecologicamente equilibrado, rompendo o estado natural do espaço digital e o contaminando com dados que deveriam estar devidamente acondicionados, pois a sua dispensação imprópria afeta a

privacidade dos usuários titulares, um dos pressupostos para manutenção do equilíbrio digital, pois cabe a cada ser humano conectado decidir onde e quando seus dados deverão ser inseridos.

Logo, o incidente se mostra como um típico exemplo de risco concreto produzido no meio ambiente digital, consubstanciado no vazamento, o qual demonstra a falta de transparência por parte dos operadores de dados e seus especialistas que sempre garantem a plena segurança da privacidade, negando qualquer risco, até que estes se com concretizem, minando qualquer argumento negacionista de que os riscos inexistem, ou, então, criando situações paradoxais em que os riscos, até então inexistentes, passam a existir, quando se concretizam em incidentes específicos, forçando o reconhecimento pelos especialistas, exatamente como explanado por Beck (2010, p. 87).

Por sua vez, apresenta-se outro episódio de vazamento de dados oriundo de mais uma Big Tech, uma das maiores empresas do mundo, a Microsoft. Ocorrido em meado do mês de junho de 2023, o caso, de acordo com o portal de notícias Mundo Conectado (Carbone, 2023) se tornou público quando a uma empresa de cyber segurança, denominada Wiz, descobriu que "38 terabytes de dados internos da Microsoft foram expostos acidentalmente por erro humano. A falha ocorreu quando a equipe de pesquisa em IA da empresa disponibilizou dados de treinamento em um repositório do GitHub".

A situação se torna alarmante quando parte de uma empresa responsável por fornecer um dos sistemas operacionais mais utilizados do mundo, com enorme alcance de usuários, de acordo com o portal Insper (Steiw, 2023). Inobstante o próprio incidente ser grave, outro fator alarmante se evidencia com a causa do vazamento, segundo o portal de notícias fornecer os pesquisadores da empresa disponibilizaram as informações, acerca de código-fonte e técnicas empregadas no desenvolvimento de IA, à comunidade científica em uma plataforma conhecida como GitHub, "no entanto, um link incluído nos arquivos deu acesso a backups de computadores de funcionários da Microsoft. Esses backups continham informações sensíveis, incluindo senhas e chaves secretas".

Indagada acerca do incidente, e empresa "garantiu que nenhum dado de cliente foi exposto devido a este incidente. A empresa também afirmou que nenhum outro serviço interno foi comprometido. O problema estava na permissividade do link, que dava acesso a toda a conta de armazenamento." Esta afirmação da Microsoft faz evidenciar o negacionismo inerente aos riscos, de modo que os causadores sempre os negam, tratando as críticas como teorias conspiracionistas. No presente caso, se observa o evidente intuito de contenção de danos à imagem da empresa, no entanto, por trás da atitude da Big Tech é inegável a negação de que o risco existiu e foi produzido, visto que a falha permitiu acesso, por qualquer pessoa, bem ou

mal-intencionada, no ambiente digital, minando qualquer segurança que poderia circundar os referidos dados pessoais.

Referido incidente evidencia, novamente, como os riscos são frequentemente concretizados no meio digital por intermédio das falhas de segurança, e que, no presente caso, somente se tornou público em razão da atuação de um terceiro que realizou observações das atividades da Microsoft, evidenciando que, apesar de os riscos serem bem reais, muitas vezes permanecem na clandestinidade, nem sempre se tornando públicos e confirmando a fala de Beck (2010, p. 87) no sentido de que os riscos só "existem" quando são reconhecidos pelos especialistas, caso contrário, permanecem em um estado de sobreposição de realidades que só se confirmam com a observação e se tornam públicos, neste sentido. Aludido incidente demonstra, mais uma vez, a falta de transparência, apesar da existência de mecanismos legais, ao redor do planeta e inclusive nos Estados Unidos onde ocorreu o incidente, fica evidente a ocultação dos riscos, os quais, por sua vez, impactam todo o meio ambiente digital conectado mundialmente pela Internet.

Inegavelmente, o referido incidente da Microsoft se mostra como mais um risco concreto perpetrado no meio ambiente digital, afetando o equilíbrio e segurança ambiental, causando danos tanto ao espaço cibernético quanto aos usuários que estão interligados com este.

O último exemplo de risco concreto a ser apresentado demonstra que os riscos são gerados até mesmo por entes estatais, consistente no vazamento de dados pessoais vinculado ao programa Auxílio Brasil do Governo Federal. A situação envolveu o programa, então denominado, Auxílio Brasil, sendo que "o vazamento ocorreu a partir de bancos de dados mantidos pela Caixa, União e Dataprev." (UOL, 2023) De acordo com o Ministério Público Federal, "dados pessoais foram divulgados ilegalmente a correspondentes bancários, que usaram as informações para oferecer empréstimos e outros produtos financeiros". O diferencial do referido caso se consubstancia justamente no fato de a demanda ter sido judicializada e, com o julgamento em primeiro grau, tornou certo a existência dos riscos perpetrados, inclusive delimitando o seu dano, visto que "a Justiça Federal fixou em R$ 15 mil o valor da indenização para cada uma das pessoas afetados pelo vazamento", tornando certo o dano e delimitando sua extensão.

Ao seu turno, apesar de a questão já ter sido solucionada judicialmente, ao menos em primeira instância, demonstra que nem mesmo os entes estatais estão isentos de produzir riscos no meio ambiente digital. Os riscos aludidos, certamente, não se limitam geograficamente, dado ao poder de conexão da Internet, bem como não se limitarão em um período temporal, podendo

gerar efeitos nocivos a qualquer momento no futuro próximo ou distante, como bem destacou a Procuradora da República Karen Louise Jeanette Kahn "esses dados violados pairam no registro e no banco de dados de incontáveis instituições, assim como em poder de terceiros que, facilmente, poderão fazer uso maléfico e fraudulento dessas informações". Logo, se torna nítido que, por uma falha, desta vez estatal, se produziu mais um risco que macula o meio ambiente digital.

Portanto, a análise deste incidente permitiu a constatação de que os riscos podem ser produzidos, praticamente, por qualquer sujeito envolvido no meio ambiente digital, seja companhias ou o Estado, visto que o ser humano, como integrante e indissociável do meio em que vive, promove mudanças, não raramente nocivas, ao espaço em que está inserido, o que, normalmente, no ambiente digital, costuma se manifestar em forma de falhas de segurança que acarretam esses vazamentos de dados supracitados.

Desta forma, foram apresentados exemplos de riscos concretos que demonstram efetivamente a existência de riscos, nos ditames da teoria de Beck (2002), que impactam o meio ambiente digital, os quais, pela análise dos próprios casos citados indicam que são imensuráveis, na medida em que afeta não somente o direito dos titulares de dados, mas maculam o ciberespaço por meio da dispensação de dados de forma inadequada que não deveriam ser simplesmente difundidos pela Internet, acarretando uso mal intencionado desses dados para diversas finalidades ilícitas que podem se converter novamente em práticas nocivas ao meio ambiente digital. Logo, neste momento, a pergunta inicialmente formulada fica parcialmente respondida, vez que se confirmou que a nocividade dos riscos concretos no ciberespaço é imensurável.

Outrossim, resta perquirir, a partir deste momento, sobre a possibilidade de sua contenção ou mitigação pelo Direito, buscando averiguar a procedência integral da hipótese inicialmente formulada, no sentido de que os riscos concretos gerados pelas companhias de grande porte, Big Techs e entes estatais no meio ambiente digital são significativamente nocivos, na medida em que afeta bilhões de seres humanos conectados, mas ainda podem ser contidos com o enfrentamento adequado, conforme se explicará na próxima seção.

4 A DISTOPIA CIBERNÉTICA E O PAPEL DO DIIREITO PARA SEU ENFRENTAMENTO

Até este momento, observou-se que os riscos concretos se manifestam frequentemente e afetam inúmeras pessoas interligadas ao ciberespaço, bem como se observou que os riscos concretos, como aqueles citados anteriormente, criam um cenário distópico, onde o direito dos titulares de dados é constantemente violado sem o conhecimento destes, causado por um verdadeiro meio ambiente desequilibrado e doente que se origina a partir do tratamento inadequado de dados pessoais. E este cenário, caso se mantenha, será extremamente tóxico ao ser humano, ou seja, um cenário de opressão digital, ressalvadas devidas proporções, ao estilo Cyberpunk abordado na obra Neuromancer de William Gibson (Gibson, 1991), indicando que a exploração excessiva de dados está causando, e continuará a causar, a deturpação do ciberespaço, prejudicando a todos que nele se conectam.

A relação entre a Teoria da Sociedade de Risco do Beck e o meio ambiente digital, explorados na primeira seção deste artigo, ganhou uma dimensão concreta por meio da demonstração de casos reais, frutos do risco, na segunda seção deste artigo. E com base nessas premissas, se abordará como o Direito, dentro da sua atribuição, pode contribuir ao enfrentamento deste problema, buscando averiguar a procedência da parte final da hipótese de pesquisa.

Em primeiro lugar, necessário expor acerca da incerteza sobre a Ciência, geradora da tecnologia que compõe o meio ambiente digital e foco central deste artigo, certamente cria uma espécie de caixa-preta que ofusca a percepção dos riscos que circundam o espaço cibernético, e acerca dessa questão, assevera Beck (2002, p. 95) que a produção precede a pesquisa, no sentido de que as tecnologias disponibilizadas no mercado, não raramente, deixam de ser testadas e serem devidamente analisadas se atingem um padrão de segurança bom, de modo que a ciência paira cegamente no limite das ameaças e impede que o conhecimento dos riscos, mesmo os concretos, cheguem ao conhecimento das pessoas. Quando ocorre essa privação sensorial, por parte da Ciência não transparente, a qual gera as tecnologias que determinam o rumo da humanidade, surge um sério problema indicado por Beck (2002, p. 96), no sentido de que um monopólio da tecnologia se torna um monopólio da mudança social encoberta, que deve ser repreendido por vozes discordantes, especialistas discordantes e diversidade interdisciplinar, e que evidenciar a incerteza científica e tecnologia é fundamental para a democratização do debate acerca desses riscos, permitindo uma contramedida e seu enfrentamento.

Extrai-se da referida lição que a Ciência, essencialmente, pressupõe o debate, a contraposição de teses, possibilitando a reformulação de um modelo predominante sempre que metodologicamente comprovado e empiricamente constatável, pautando-se em evidências. Logo, nada mais oportuno do que afastar o caráter absoluto e possibilitar questionamentos por meios que admitem uma participação social, visto ser a sociedade a final destinatária dos frutos da ciência e, eventualmente vítima de seus erros. Quando se debate acerca do enfrentamento dos riscos, imperioso salientar algumas lições de Beck (2002, p. 110), a se iniciar pela extensão ecológica da democracia para o desenvolvimento da harmonia entre várias vozes e autoridades, promovendo a autonomia política, legal e social em contraposição à ilusória segurança de uma sociedade concebida de maneira abstrata, envolvendo dois princípios complementares: primeiro, estabelecimento de uma divisão de poderes; segundo, a criação de um espaço público para o debate, vez que apenas um debate público vigoroso e embasado em argumentos científicos pode distinguir entre conhecimento válido e pseudocientífico, permite que as instituições responsáveis pela tecnologia, política e justiça recuperem o controle com base em critérios próprios.

Percebe-se, a este ponto, que a chave para enfrentamento dos riscos é, em primeiro lugar, a extirpação da privação sensorial, afastando a falta de transparência que circundam os bastidores do meio ambiente digital. A nebulosidade ao redor dos agentes de tratamento de dados reflete justamente a função simbólica da Ciência, Política e Direito. Nos dizeres de Ferreira (2016, p. 136-144) cabe conceituar as funções simbólicas como: a) para a ciência: romper a neutralidade e imparcialidade da ciência para produzir conhecimento enviesado que induza à conclusão pela normalidade dos riscos; b) para a política: adotar medidas governamentais que carecem de efetividade, seja pelo estabelecimento de metas que não serão atingidas ou pela falha, proposital, na obtenção do resultado (a exemplo do Plano de Ação para a Prevenção e Controle do Desmatamento na Amazônia Legal, o qual buscou efetivar internamente o compromisso assumido internacionalmente, mas sem sucesso); c) e para o Direito: criar normas jurídicas com a finalidade de efetivar o avanço descontrolado da ciência enviesada e/ou legitimar a política simbólica (pela sua ação ou omissão), de modo a chancelar os problemas criados pelas duas vertentes anteriores, de modo a completar o círculo vicioso da normalização do risco e irresponsabilidade organizada. Verifica-se que os diversos usos simbólicos se interligam, a ciência simbólica pode ser má utilizada para exercer uma política simbólica, que, por sua vez, pode produzir normas jurídicas simbólicas, a qual, por fim, pode efetivar as práticas anteriores, instituindo sistema de irresponsabilidade organizada.

Aludida falta de transparência aliada à função simbólica do Direito e da Ciência, no mundo digital, se mostra como a principal causa dos riscos, em um geral, visto que em seu âmago permite se instalar a função simbólica da ciência, produzindo tecnologias sem a devida análise de risco e permitindo práticas que carecem de segurança, o que se observa pelos dispositivos que constantemente vigiam as pessoas integradas no meio ambiente digital, coletando seus dados em grande quantidade, e, ao mesmo tempo, não adotando mecanismos que confiram efetiva segurança ao tratamento dos referidos dados, ocasionando frequentes vazamentos que, por sua vez, contaminam o meio ambiente digital e embasam novas práticas congêneres, ao tornar a situação "normal" e permitir que os dados vazados alicercem novos ataques cibernéticos ou causem novos incidentes de segurança, constituindo um verdadeiro ciclo desvirtuoso que se renova a cada falha. Acerca desta temática, oportuno destacar as lições de Freitas (2022, p. 244):

> Nesse entendimento, a proteção de dados pessoais pode ser um evento dentro da análise de riscos, visto que quando os dados pessoais não são protegidos de forma adequada, ou seja, quando as disposições e obrigações de proteção de dados não são cumpridas, não se tem conformidade, tal evento leva à violação potencial de todos os direitos fundamentais dos titulares dos dados afetados por operações de tratamento de dados.

Referidas lições de Beck, Ferreira e Freitas permitem concluir que a participação social é fundamental para deliberar sobre os rumos de uma sociedade, inclusive em matéria de prevenção de risco e formas de lidar com tal problemática. No entanto, para viabilizar deliberações desta ordem, se faz necessário a contribuição da comunidade científica que, por sua vez, também deve respeitar a dialética interna para emitir posicionamentos não enviesados. Indispensável, também, a atuação do Direito para regular as deliberações e proporcionar forma de solução de conflitos e regulamentar a proteção adequada dos dados pessoais. Ou seja, para enfrentamento dos riscos sob a perspectiva do Direito, é imprescindível, em suma, a estrutura social adequada ao debate além de uma regulamentação precisa e eficaz da proteção de dados.

Quanto à estrutura social para promoção do debate, o Direito deve incentivar práticas de ampla divulgação e debate sobre os riscos, tal como, a título exemplificativo, obrigar juridicamente os agentes de tratamento de dados mantenham uma plataforma para publicização dos riscos, permitindo críticas, sugestões, indagações e avaliações por terceiros, utilizando o próprio ciberespaço para discutir os riscos que o circundam. Neste ponto, é notável observar que a própria tecnologia, que apresenta os riscos mencionados, pode também ser utilizada para sua resolução ou, pelo menos, mitigação, ao proporcionar um ambiente onde bilhões de usuários se conectam e compartilham informações em uma verdadeira ciberdemocracia discutida por

Levy (1999, p. 188). A interconexão dos indivíduos pela Internet pode dar origem a uma abordagem inovadora para políticas de planejamento, além de trazer benefícios por meio das oportunidades oferecidas no ciberespaço, o que pode fomentar a revitalização do tecido social e explorar novos métodos democráticos. Nesse sentido, a tecnologia demonstra sua capacidade de unir pessoas dentro do espaço digital, reconhecido anteriormente como o ambiente digital, permitindo a efetivação de uma democracia participativa. Esta concepção de democracia digital remete às ideias apresentada por Castells (2013) em sua obra ao analisar movimentos de protesto social impulsionados pelas redes, onde é destacada a noção de que as redes possibilitam uma nova forma de mobilização, denominada conectividade. Neste sentido, visibilidade dos riscos e o debate acerca destes fenômenos é essencial ao seu enfrentamento, visto que a sociedade de risco se enxerga nesse novo paradigma e passa a permitir a discussão acerca dos seus problemas, o internalizando em sua essência, como afirmado por Beck (2012, p. 22). Logo, incumbe ao Direito, neste contexto, fomentar tais práticas, seja pela imposição de manutenção de plataformas destinadas à exposição e ao debate dos riscos pelos próprios agentes de tratamento, ou pela criação e manutenção de plataforma, pelo próprio Estado, destinado à idêntica finalidade, e devem ser implementados para que o Direito possa cumprir com o seu dever de proporcionar uma estrutura social para o debate destinado ao enfrentamento dos riscos ambientais no ciberespaço.

Por sua vez, quanto à regulamentação da proteção de dados, atualmente no cenário jurídico, já existem notórios atos normativos como a Lei Geral de Proteção de Dados (BRASIL, 2018), que incentiva boas práticas (art. 46, da LGPD), mas que carece de uma definição precisa do que seriam essas boas práticas. A lacuna normativa acaba por ser suprida, na prática, por normas técnicas que buscam estabelecer padrões de segurança adequados, tal como as normas ISO da família 27000 (ISO/IEC, 2018). As normas desta família abordam os requisitos do Sistema de Gestão de Segurança da Informação (SGSI) para toda a empresa, seguindo o princípio de "Plan-Do-Check-Act" e estabelecem práticas para garantir a Segurança da Informação, alinhada com a LGPD, em 11 seções de controles de segurança, prevendo requisitos de privacidade de dados para proteger os dados pessoais identificáveis e garantir o direito à privacidade dos titulares. Assim, tais normas, atualmente de adoção facultativa, deveriam ser obrigatórias perante disposições legais ou regulamentação delegada do poder Executivo, ou suas autarquias, obrigando os agentes de tratamento de dados que operam no espaço digital a adotarem mecanismos eficazes de proteção de dados e, consequentemente, de mitigação dos riscos. Portanto, se torna evidente que existem normativas facultativas que buscam proteger os dados pessoais coletados, estabelecendo condutas que garantam a

segurança no tratamento desses dados, de modo que incumbe ao Direito, neste ponto, obrigar a adoção de tais normas nos casos em que os riscos são elevados. O que se mostra plenamente possível quando se considera que LGPD, em seu art. 5º, XVII, prevê a necessidade de um relatório de impacto à proteção de dados pessoais que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, de modo que os agentes de tratamento podem mensurar o risco e adotar práticas de segurança proporcionais a estes, tal como as citadas normas ISO/IEC (2018).

Portanto, observa-se que o Direito pode, e deve, contribuir com o enfretamento dos riscos concretos no ciberespaço procedendo desta forma. No entanto, evidentemente, somente o Direito não é capaz de cumprir tal tarefa, visto que referido feito demanda um trabalho interdisciplinar, mas se o Direito não se mobilizar e conferir uma resposta adequado ao problema vislumbrado, se limitará à sua função simbólica, o que deve ser evitado a todo custo, vez que a degradação do meio ambiente digital implica a degradação do ser humano, e um consequente dano irreparável às gerações presentes e futuras.

Assim, percebe-se que, para real contenção dos riscos, o Direito deve superar sua função simbólica e permitir a transparência dos riscos que afetam o meio ambiente digital, restabelecendo seu equilíbrio e o protegendo de práticas nocivas, sob pena de se condenar um meio ambiente inteiro ao destino abissal e distópico, um cenário em que nem as pessoas e nem o espaço são respeitados. Logo, nesta seção se observou que mesmo que existam mecanismos legais e normas infralegais que subsidiam o enfrentamento dos riscos concretos produzidos no meio ambiente digital, para o efetivo combate aos riscos se faz necessária a participação democrática, o reconhecimento dos riscos e um debate informado destinado ao atingimento de soluções que possam reestabelecer o equilíbrio ambiental rompido, devendo o Direito exercer sua atuação nestas duas formas de enfrentamento.

5 CONCLUSÃO

Pela breve exposição das ideias no presente artigo, permitiu-se observar que o meio ambiente, apesar de ser uno, possui, para fins de estudos, sua dimensão digital, o qual se mantém em um delicado equilíbrio e, por esta razão, é vulnerável às oscilações denominadas como risco.Referido meio ambiente digital, hoje expressado principalmente pela Internet, é composto, em sua essência, por dados, os quais desempenham funções semelhantes aos átomos na física.

Por sua vez, os riscos se manifestam concretamente por meio de incidentes de segurança, em especial os vazamentos de dados que foi como foco deste artigo, ao passo em que sua nocividade é imensurável, afetando bilhões de pessoas, direta ou indiretamente.

Diante deste cenário, no qual os riscos são inegáveis e seus efeitos imensuráveis, surge a discussão acerca do papel do Direito na sua contenção, chegando ao resultado de que o Direito deve superar sua função simbólica, promovendo a publicização do debate e regulamentar com mais rigor a proteção dos dados. Caso contrário, o meio digital está fadado à exploração exacerbada e se continuará sendo uma distopia cibernética, no qual os riscos, ainda que ocultos aos olhos leigos, são devastadores.

Ao longo do trabalho, observou-se que os efeitos dos riscos gerados no contexto do meio ambiente digital não podem ser mensurados, visto que se trata de um espaço interconectado com ligações de bilhões de dispositivos ao redor do planeta, criando um verdadeiro espaço cibernético que se mostra, verdadeiramente como uma realidade paralela, e que abriga toda uma cultura gerada por bilhões de usuários que ali estão conectados.

Referidos efeitos nocivos, imensuráveis, se apresentam de diversas formas, seja um vazamento de dados, seja a vigilância, seja a exploração excessiva, mas se destinam ao mesmo ponto, a maculação do meio ambiente digital, rompendo e deturpando o equilíbrio desse ecossistema, obrigando uma reflexão acerca de como restaurá-lo.

Frente a necessidade de restauração do equilíbrio, novamente, ressurge a reflexão acerca do papel das instituições, o que se traduz no debate acerca do papel do direito, remetendo à função simbólica do Direito e as formas de como superá-la, sendo este o ponto chave para mitigação dos riscos que permeiam o espaço digital.

A partir do momento em que o Direito superar sua submissão aos interesses mercadológicos e passar a tutelar o bem jurídico, da forma com que este relevantíssimo bem jurídico merece, estar-se-á diante do início da mudança, adotando regulamentação mais precisa e promovendo a transparência e o debate, como foi explorado na seção anterior.

Logo, diante desses fatores expostos, observa-se a confirmação da hipótese, no sentido de que a nocividade dos riscos é imensurável, mas passíveis de contenção com base na ampliação do debate informado como representativo da participação democrática e respeito às normas de boas práticas que buscam proporcionar maior segurança ao processo de tratamento de dados.

Por fim, a produção de conhecimento sobre o presente tema ainda não se esgotou, ensejando discussão constante que permitirá a elaboração de outros estudos complementares,

vez que o meio ambiente digital está em constante mudança, assim como os problemas que o circundam.

REFERÊNCIAS

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001

BECK, Ulrich. **A reinvenção da política: rumo a uma teoría da modernidade reflexiva**. In: GIDDENS, Anthony; LASH, Scott; BECK, Ulrich. Modernização reflexiva: política, tradição e estética na ordem social moderna. São Paulo: UNESP, 2012.

BECK, Ulrich, **Sociedade de Risco: rumo a uma outra modernidade**. São Paulo: Editora 34, 2010.

BECK, Ulrich. **La sociedad del riesgo global**. España: Siglo Veintiuno, 2002.

CAPRA, Fritjof. **As conexões ocultas**. São Paulo: Cultrix, 2006.

CARBONE, Felipe. **Pesquisadores da Microsoft vazam sem querer 38 TB de dados da empresa**. Mundo Conectado, 19/09/2023, Disponível em: https://www.mundoconectado.com.br/corporativo/vazamento-38-tb-dados-microsoft/ Acesso em: 10 maio 2024

CASTELLS, Manuel. **A galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade**. São Paulo: Zahar, 2003

CASTELLS, Manuel. **Redes de indignação e esperança: movimentos sociais na era da internet**. Tradução de Carlos A. Medeiros. Rio de Janeiro: Zahar, 2013.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. O meio ambiente digital sob a ótica da Teoria da Sociedade de Risco: os avanços da informática em debate. **Revista Direito Ambiental e sociedade.** v. 5, n. 1. pp. 194-223. 2015. Disponível em: https://sou.ucs.br/etc/revistas/index.php/direitoambiental/article/view/3912. Acesso em: 10 maio 2024

COUTINHO, Ricardo Silva. **O meio ambiente digital e a tutela dos bens culturais.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, São Paulo, v. 1, n. 1, p. 221-244, 2014.

DAVENPORT, Thomas H.; tradução Bernadette Siqueira Abrão. **Ecologia da informação – porque só a tecnologia não basta par o sucesso na era da informação**. São Paulo: Futura, 1998.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL],** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315 Acesso em: 10 maio 2024

DONEDA, Danilo. Reflexões sobre proteção de dados pessoais em redes sociais. **Revista Internacional de Protección de Datos Personales.** universidad de los Andes. Facultad de Derecho. Bogotá. No. 1. Jul-Dez. de 2012. Disponível em:

https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/10_Danilo-Doneda_FINAL.pdf.pdf Acesso em: 10 maio 2024

FERREIRA, Heline Sivini. **A dimensão ambiental da teoria da sociedade de risco.** In: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). Direito Socioambiental e Sustentabilidade: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016.

FREITAS, Cinthia Obladen de Almendra. Riscos e Proteção De Dados Pessoais. **Revista Rede de Direito Digital, Intelectual & Sociedade.** Curitiba. v. 2. n. 4. p. 1-319. 2022. Disponível em: https://revista.ioda.org.br/index.php/rrddis/article/view/74 Acesso em: 10 maio 2024

GIBSON, William, **Neuromancer**, São Paulo: Editora Aleph, 1991.

GLEICK, James. **Chaos-making a new science**. New York: Viking, 1987.

ISO/IEC. **Information technology — Security techniques — Information security management systems — Overview and vocabulary,** ISO/IEC 27000:2018.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

STEIW, Leandro. **O que é um sistema operacional e quais são os principais?** Insper. 21/03/2023. Disponível em: https://www.insper.edu.br/noticias/o-que-e-um-sistema-operacional-e-quais-sao-os-principais/ Acesso em: 10 maio 2024

UOL. **Auxílio Brasil: Justiça manda indenizar em R$ 15 mil quem teve dado vazado**. 21/09/2023. Disponível em: https://economia.uol.com.br/noticias/redacao/2023/09/21/justica-manda-indenizar-beneficiarios-do-auxilio-que-tiveram-dados-vazados.htm?cmpid=copiaecola Acesso em: 10 maio 2024

ZUBA, Fernando. **Justiça de MG condena Facebook a pagar R$ 20 milhões por vazamento de dados de brasileiros.** Globo. 25/07/2023. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2023/07/25/justica-de-mg-condena-facebook-a-pagar-r-20-milhoes-por-vazamento-de-dados-de-brasileiros.ghtml Acesso em: 10 maio 2024

ZUBOFF, Shoshana. **A ERA DO CAPITALISMO DE VIGILÂNCIA: A luta por um futuro humano na nova fronteira do poder**; Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2020.