

DESASTRES CIBERNÉTICOS: ESTAMOS PREPARADOS PARA A GESTÃO DESTES RISCOS?

Larissa Cerqueira de Oliveira^{*}

Luciana Ziglio^{**}

Fernanda Guedes Queiroz de Lira^{***}

RESUMO

Em 19 de julho de 2024 ocorreu um apagão cibernético de proporções globais que paralisou sistemas essenciais à vida contemporânea, como saúde, finanças, transportes e comunicações. No contexto brasileiro, os eventos cibernéticos também têm sido uma preocupação ao longo das últimas décadas, sendo instituída a Rede Federal de Gestão de Incidentes Cibernéticos e a Política Nacional de Cibersegurança. Tais eventos desafiam a capacidade institucional do Estado e impulsionam reflexões sobre seu enquadramento jurídico e os mecanismos de resposta diante destes riscos tecnológicos. Dessa forma, este trabalho propõe-se a investigar, sob a ótica do Direito dos Desastres, se, e de que forma, incidentes cibernéticos podem ser enquadrados como desastres no ordenamento jurídico nacional, considerando a potencialidade de causar perturbações sistêmicas relevantes à ordem pública e social. A metodologia adotada é qualitativa, com abordagem dedutiva, fundamentada em revisão bibliográfica interdisciplinar e análise crítica do arcabouço normativo vigente. A análise revela a insuficiência do modelo institucional atual para lidar com eventos dessa natureza, indicando a fragilidade de estratégias integradas de prevenção e mitigação. Conclui-se que a construção de uma abordagem jurídica e institucional mais robusta e adaptada aos riscos contemporâneos, especialmente no que tange à cibersegurança, é essencial para o fortalecimento da resiliência institucional e para a proteção da sociedade frente aos riscos emergentes, sobretudo diante de um contexto de desconhecimento dos riscos cibernéticos por grande parte da população.

Palavras-chave: desastres; riscos; direito dos desastres; cibersegurança; ataque cibernético.

Data de submissão: 15/05/2025

Data de aprovação: 02/09/2025

^{*} Doutoranda e Mestra em Direito pela USP/FDRP. Pós-graduada em Direito Processual Civil pela Universidade Federal da Bahia. Juíza Auxiliar no Tribunal de Justiça do Estado de São Paulo.

^{**} Professora e pesquisadora da Faculdade Latino-americana de Ciências Sociais (FLACSO/Brasil). Observadora acadêmica pela FLACSO-Brasil da Convenção de Basiléia.

^{***} Mestre em Direito pela UFRN. Integrante do Grupo de Pesquisa "Acesso à Justiça, Desastres e Mudanças Climáticas" da FGV/SP. Graduada em Direito pela UNIRN.

CYBER DISASTERS: ARE WE PREPARED FOR RISK MANAGEMENT?

Larissa Cerqueira de Oliveira
Luciana Ziglio
Fernanda Guedes Queiroz de Lira

ABSTRACT

On July 19, 2024, a cyber blackout of global proportions paralyzed systems essential to contemporary life, including healthcare, finance, transportation, and communications. In the Brazilian context, power outages and incidents of cyberattacks have also intensified over recent decades. Such events challenge the institutional capacity of the state and prompt critical reflection on its legal framework and response mechanisms in the face of technological risks. This paper, therefore, aims to investigate, from the perspective of Disaster Law, whether and how cyber and energy-related incidents can be classified as disasters under the national legal system, considering their potential to trigger systemic disruptions that significantly impact public and social order. The study adopts a qualitative methodology with a deductive approach, grounded in an interdisciplinary literature review and critical analysis of the current regulatory framework. The analysis reveals the inadequacy of the existing legal model in addressing events of this nature, highlighting the fragility of integrated prevention and mitigation strategies. It concludes that developing a more robust legal framework tailored to contemporary risks (particularly concerning cybersecurity and energy security) is essential for enhancing institutional resilience and safeguarding society against emerging threats.

Keywords: disasters; technological risk; disaster law; cybersecurity; energy.

Date of submission: 15/05/2025

Date of approval: 02/09/2025

INTRODUÇÃO

O conceito de desastre cibernético está associado a um evento catastrófico, que devido à pane ou a falha de sistemas tecnológicos venha a causar danos intensos e repentinos (ScienceDirect, 2001). Nesse sentido, o presente trabalho tem por escopo analisar o arcabouço normativo brasileiro aplicado à gestão de desastres, com foco específico nos incidentes cibernéticos e suas consequências, a fim de avaliar a capacidade de resposta do sistema jurídico diante da crescente complexidade desses eventos, bem como investigar a possibilidade de sua caracterização como desastres no contexto nacional.

Os primeiros estudos sobre o conceito de desastres remontam à década de 1920, através do pesquisador Samuel Prince. Todavia, é na década de 1950 que integrantes da Universidade de Chicago buscaram estabelecer uma definição de desastres, avançando a partir daí para o aprimoramento do conceito, levando-se em consideração outros elementos, como o contexto social e riscos socio estruturais, com Dombrowsky (Andrea, 2023, p. 173).

Daniel Farber (2019, p. 25), por sua vez, aponta o Direito dos Desastres como uma área emergente de estudo tangenciada pelo conceito de gerenciamento de riscos, partindo de um modelo circular de tratamento dos desastres (ciclo), que abarcam as funções de prevenção e mitigação, resposta emergencial, compensação, reconstrução e mitigação dos riscos futuros.

No Brasil, especialmente a partir de 2010, despontaram alguns marcos normativos sobre a temática dos desastres, quais sejam:

- a) a Lei 12.340/10: que dispõe sobre as transferências de recursos para a execução de ações de prevenção em áreas de risco de desastres e de resposta e de recuperação em áreas atingidas por desastres;
- b) o Decreto 7257/2010, que trouxe a conceituação de desastres;
- c) a Lei 12.608/2012, que institui a Política Nacional de Proteção e Defesa Civil e dispõe sobre o Sistema Nacional e sobre o Conselho de Proteção e Defesa;
- d) a Lei 12.983/14: que alterou alguns dispositivos da Lei nº 12.340/2010; e e) a Lei 14.750/2023 que alterou as Leis nº 12.608/2012 e 12.340/2010, para aprimorar os instrumentos de prevenção de acidentes ou desastres e de recuperação de áreas por eles atingidas, as ações de monitoramento de riscos de acidentes ou desastres e a produção de alertas antecipados.

Por outro lado, embora apartada da normatização voltada para desastres, a partir do ano de 2021, foi instituída a Rede Federal de Gestão de Incidentes Cibernéticos, por meio do Dec. 10.748/21 e, em dezembro de 2023, a Política Nacional de Cibersegurança – PNCiber, pelo Dec. 11.856/23, após um longo caminho de incorporação oficial dessa temática nos principais documentos brasileiros de defesa desde 2005, com a publicação da Política de Defesa Nacional e, posteriormente, com a Estratégia Nacional de Defesa de 2008.

Nessa perspectiva, o presente estudo revisitou de forma crítica o arcabouço normativo brasileiro destinado à gestão de desastres, com ênfase nos incidentes cibernéticos e em sua interdependência com riscos energéticos, com o principal objetivo de avaliar se, diante de um colapso de energia e internet superior a 72 horas, nosso sistema jurídico estaria apto a tratar esses eventos como “desastres”. Delimitou-se o escopo às normas promulgadas entre 2010 e 2023, bem como às regulamentações setoriais da ANEEL e do ONS, confrontando-as com a hipótese de um “apagão virtual” global inspirado em eventos de julho de 2024 e nas diretrizes de sobrevivência francesa de março de 2025.

A problemática central partiu da pergunta “como um incidente cibernético pode consistir em um desastre e quais medidas preventivas e mitigadoras podem ser aplicadas?”. Para respondê-la, este trabalho foi organizado em cinco capítulos: (i) introdução ao conceito histórico e ao Direito dos Desastres; (ii) definição de risco; (iii) mapeamento do panorama normativo brasileiro; (iv) construção da hipótese de desastre cibernético e sua compatibilidade com as definições legais de desastre; e (v) propostas de gerenciamento de riscos.

Diante desse contexto, a pesquisa adotou uma abordagem metodológica baseada em três estratégias principais: a revisão narrativa da literatura especializada, a análise documental e a modelagem de situação hipotética. A revisão narrativa foi utilizada com o objetivo de reunir e interpretar criticamente o conhecimento produzido sobre o tema, permitindo identificar lacunas, convergências e controvérsias teóricas. Em outra perspectiva, a análise documental consistiu na coleta e exame sistemático de documentos oficiais, normativos e institucionais, buscando embasamento empírico e normativo para a compreensão do objeto de estudo. Já a modelagem de situação hipotética foi empregada como instrumento de simulação teórica, possibilitando projetar cenários e refletir sobre as possíveis implicações e consequências práticas associadas à problemática analisada.

Embora soe como algo pouco factível, não se trata de “teoria da conspiração” ou adivinhação, mas o mero desenvolvimento de análise ponderativa, pautadas no elemento risco (Beck, 2010, p. 11)² exemplificando com recentes eventos ocorridos no panorama europeu.

² À propósito, ainda em 1986, o mencionado autor, quando tratou dos propósitos da sua obra “Sociedade de Risco: rumo a uma outra modernidade” vislumbrou eventos que se concretizaram muitos anos depois, como o advento da pandemia da Covid-19: “Só precisamos nos perguntar uma única vez o que é que de fato poderia ter sido feito diferente se houvesse ocorrido uma contaminação do ar, da água, da fauna e dos seres humanos que alcançasse, também segundo parâmetros oficiais, uma proporção acentuadamente perigosa. Nesse caso, a vida – respirar, comer, beber – seria interrompida ou restrita por uma medida oficial? O que acontece com a população de um continente inteiro que, em diferentes graus (de acordo com variáveis “fatalistas” como vento, condições atmosféricas, distância em relação ao local do acidente, etc), é irreversivelmente contaminada? Podem (grupos de) países ser mantidos em quarentena? Desencadeia-se o caos interno? Ou então, mesmo num caso desses, tudo acabaria precisando acontecer como aconteceu em Chernobyl?” (Beck, 2010, p. 11). Sobre a Pandemia de Covid-19 indica-se a leitura da obra: RIBEIRO, Wagner Costa. COVID-19: passado, presente e futuro.

Portanto, ao propor uma análise crítica da normatização brasileira frente aos desafios impostos pelos desastres cibernéticos, o presente estudo busca não apenas identificar lacunas normativas, mas também fomentar reflexões sobre a necessidade de um marco regulatório mais sensível à realidade tecnológica contemporânea. Dessa forma, ao reconhecer a natureza complexa, sistêmica e potencialmente disruptiva desses eventos, pretende-se contribuir para o fortalecimento de estratégias de prevenção, mitigação e resposta, que sejam compatíveis com os riscos emergentes da sociedade hiperconectada e energeticamente dependente.

2 DOS RISCOS

Como definição inicial, risco é a probabilidade de estar em perigo (Aurélio, 2025). É a incerteza associada a um evento com o potencial de gerar consequências negativas. Como componentes essenciais do risco, consideram-se: a probabilidade, compreendida como a chance de um evento ocorrer, que pode ser expressa em porcentagem, fração ou em gradiente (como por exemplo: baixo, médio e alto risco) e o impacto, explicado como o resultante do risco que se traduz, a título de exemplo em termos financeiros (perda de dinheiro), operacionais (interrupção de atividades), reputacionais (danos à imagem) ou até mesmo em termos de saúde e segurança.

Todavia, existem diversos tipos de risco e ao analisá-los, deve-se considerar como o meio ambiente foi abordado ao longo do tempo, com base nas características específicas de cada sociedade” (Valencio et al., 2009; Zanirato et al., 2008; García-Tornel, 2001).

Tratando do conceito de risco voltado para a temática dos desastres, o Marco Sendai para a redução do Risco de Desastres 2015-2030 (UNDRR, 2015), adotado na Terceira Conferência Mundial sobre a Redução destes riscos, realizada em março de 2015, em Sendai, Miyagi, no Japão, descreve sete metas e quatro prioridades de ação para prevenir novos riscos de desastres e reduzir os existentes: (i) compreender o risco de desastres; (ii) fortalecer a governança de risco de desastres para gerenciar o risco de desastres; (iii) investir na redução de desastres para resiliência e; (iv) melhorar a preparação para desastres para uma resposta eficaz na recuperação, reabilitação e reconstrução.

Este marco aprofunda as diretrizes lançadas pelo Marco de Ação de Hyogo (2005). Segundo Andréa (2023, p. 168-169, apud Oliveira, 2024), foi justamente durante a vigência desse instrumento que o Brasil passou a criar legislação específica para desastres e a reorganizar sua estrutura administrativa, deixando claro o peso que tal documento internacional exerceu na orientação das políticas de redução de riscos em diversos países.

Universidade de São Paulo. Faculdade de Filosofia, Letras e Ciências Humanas, 2020. DOI: Disponível em: www.livrosabertos.abcd.usp.br/portaldelivrosUSP/catalog/book/552 . Acesso em 5 maio. 2025.

Na atualidade, vivenciamos o contexto de sociedade contemporânea marcada não apenas pela adoção de máquinas inteligentes e sistemas interconectados, mas, sobretudo, pela integração de diferentes tecnologias e disciplinas em um ecossistema altamente dependente da digitalização. Essa interdependência potencializa riscos sistêmicos, pois inovações que antes eram tratadas como projeções teóricas, tornaram-se parte concreta do cotidiano (Schwab; Davis, 2018).

Seguindo por essa perspectiva e considerando esta interdependência tecnológica crescente, as estruturas sociais contemporâneas têm se reorganizado em redes, impulsionadas pela globalização e pelo fluxo contínuo de dados e comunicações em escala global, característica da chamada “Era da Informação” (Castells, 1999, p. 39-66). Contudo, ainda que essa lógica de rede já tenha emergido em momentos anteriores da história, a atualidade se diferencia pela abrangência e velocidade com que a tecnologia da informação permite sua expansão, promovendo transformações inéditas tanto em sua escala quanto em seu impacto sociopolítico (Menezes Neto, 2016, p. 65–66).

No entanto, essa dependência tecnológica impõe elevados custos sociais e ambientais. A demanda por energia elétrica destinada à manutenção de *data centers*, inteligências artificiais e transações com criptomoedas é crescente e já representa uma parcela significativa do consumo global. A Agência Internacional de Energia (IEA) alerta para uma tendência de forte aumento dessa demanda, uma vez que segundo ela, o gasto energético em 2026, poderá dobrar no mundo, em relação a 2022, superando inclusive o consumo anual de países inteiros, como o Brasil (Vasconcelos, 2025, p. 12-21).

As transformações estruturais recentes vêm reconfigurando as dinâmicas sociais, econômicas e energéticas em redes digitais globais, nas quais os riscos cibernéticos, interligados aos riscos energéticos, despontam como vulnerabilidades sistêmicas centrais. Segundo o Fórum Econômico Mundial (2021), à medida que o setor energético passa por uma transição multifacetada (do analógico ao digital, do centralizado ao distribuído e do fóssil ao baixo carbono), a gestão dos riscos cibernéticos torna-se essencial para a resiliência e a sustentabilidade das cadeias de valor. O relatório *Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers*, fruto de debates entre mais de 40 executivos do setor, destaca que a integração entre tecnologias operacionais e redes de informação (com uso de *big data*, inteligência artificial e automação) é central para a construção de um modelo operacional mais eficiente, resiliente e de baixo carbono. Nesse contexto, cabe aos executivos, conselhos e gestores de segurança promover um diálogo contínuo e adotar medidas que garantam que a mitigação dos riscos cibernéticos acompanhe o ritmo da inovação tecnológica (Fórum Econômico Mundial, 2021, p. 3).

Isso porque, a complexificação das infraestruturas digitais e a crescente sofisticação dos agentes mal-intencionados tornam o setor elétrico particularmente vulnerável a ameaças cibernéticas com potencial disruptivo. Nesse sentido, a Agência Internacional de Energia (IEA) alertou que os ataques cibernéticos estão se tornando mais frequentes, destrutivos e estratégicos,

explorando com maior precisão as vulnerabilidades críticas dos sistemas elétricos. A IEA destacou que o aumento da conectividade e da automação em toda a rede elétrica, impulsionado pela digitalização e pela integração de dispositivos conectados, como medidores inteligentes e sistemas de controle remoto, amplia a superfície de ataque. A adoção crescente de tecnologias como veículos elétricos, geração distribuída e armazenamento de energia também aumenta o risco cibernético, pois essas tecnologias conectam diretamente a infraestrutura elétrica à rede digital, criando novos pontos de vulnerabilidade (IEA, 2020).

Seguindo por essa linha de raciocínio, o aumento da conectividade e da automação em toda a infraestrutura elétrica, embora traga ganhos em eficiência e flexibilidade, também potencializa a exposição a ameaças cibernéticas, tornando esses sistemas mais suscetíveis a ataques. Nestes termos, um ataque cibernético bem-sucedido pode resultar na perda de controle sobre dispositivos e processos críticos, ocasionando danos físicos consideráveis e interrupções no fornecimento de energia. Além dos efeitos diretos nos serviços essenciais e nos consumidores que dependem da eletricidade, tais incidentes podem acarretar perdas financeiras substanciais para as concessionárias de energia, incluindo custos com a detecção, investigação, contenção e recuperação do ataque, bem como as consequências econômicas da interrupção das operações, perda de dados, redução de receitas e danos aos equipamentos. (IEA, 2020).

Os incidentes registrados nos últimos anos confirmam essa realidade, evidenciando que a segurança cibernética não é apenas uma preocupação técnica, mas uma questão de resiliência estrutural que exige resposta integrada dos setores público e privado, sob risco de impactos significativos à ordem social, econômica e ambiental (Georgiadou; Michalitsi-Passarrou; Askounis, 2023).

Sendo assim, as indagações aqui inseridas pautam-se na pura e simples suscetibilidade objetiva do risco diante de uma sociedade inserida em um contexto de transformações socioeconômicas, culturais, tecnológicas e políticas, de modo que, ainda que os efeitos se revelem pouco prováveis e fortemente hipotéticos, impõe-se a condução de investigações, materializadas nos estudos de impacto ambiental, sempre que houver a possibilidade de danos de natureza catastrófica (Carvalho; Damacena, 2013).

3 DO PANORAMA NORMATIVO BRASILEIRO

Inicialmente, ao traçar o panorama normativo sobre a temática e suas respectivas regulamentações, bem como analisar as implicações de eventos cibernéticos e as suas conexões com o conceito de desastre, o artigo utilizará numa primeira abordagem, a nomenclatura incidente, entendido como um acontecimento imprevisto e não desejado, com potencial de causar dano, dissociado do conceito de desastre, que será trabalhado mais adiante.

Com essa distinção, será possível considerar a ocorrência de incidentes cibernéticos fora ou dentro de um contexto de desastres.

No que tange aos incidentes cibernéticos³, existe um amplo debate quanto à conceituação preliminar de espaço cibernético, soberania estatal⁴ e suas relações com incidentes. A ausência de consenso sobre o que exatamente constitui o espaço cibernético, ressaltada por Oliveira e Portela (2017), tem levado autores a propor modelos que deem conta de sua complexidade.

Posto isso, entre tais modelos, Ventre (2012) aponta que reduzir o ciberespaço à Internet é equivocado: trata-se de um domínio multicomponente que combina, de um lado, uma infraestrutura física - material — satélites, drones, dispositivos RFID, sistemas industriais e computadores conectados ou não — e, de outro, camadas lógicas de software e, acima delas, uma dimensão cognitiva onde a informação é produzida e interpretada. Por atravessar simultaneamente os domínios terrestre, marítimo, aéreo e espacial, essa ecologia tecnológica desafia as categorias tradicionais de territorialidade e, conseqüentemente, a aplicação linear de soberania estatal na prevenção e na resposta a incidentes cibernéticos (Oliveira; Portela, 2017; Ventre, 2012).

O espaço cibernético, sob uma perspectiva abrangente indicada por Ventre (2012), é composto por três camadas complementares: *hardware*, *software* e *peopleware*, englobando não apenas os dispositivos e sistemas tecnológicos, mas também os usuários que os operam e interagem com eles.

No contexto brasileiro, a inserção formal dessa temática nos documentos de defesa ocorreu de forma relativamente recente, nos principais documentos brasileiros de defesa ocorreu somente em 2005, com a publicação da Política de Defesa Nacional e, em seguida, com a Estratégia Nacional de Defesa de 2008 (Oliveira; Portela, 2017).

Também houve a previsão da edição do Livro Branco de Defesa Nacional (LBDN) a partir de 2012, que previu quatro ações para o projeto de defesa cibernética, abarcando:

a construção da sede definitiva do Centro de Defesa Cibernética e aquisição da infraestrutura de apoio, aquisição de equipamentos e capacitação de recursos humanos, aquisições de soluções de *hardware* e *software* de defesa cibernética e implantação dos projetos estruturantes do Setor Cibernético, a fim de ampliar a capacidade de resposta às ameaças. Esses

³ Traçando um panorama dos ataques cibernéticos mundiais, Sara Martins Ibrahim Paz (2019) em dissertação de mestrado pela Escola de Guerra Naval, elencou ao menos cinco ataques cibernéticos internacionais desde 1982, contra a União Soviética; em 2007 na Estônia e Síria; em 2008, na Geórgia; em 2009, contra o Irã e em 2015: contra setores público e privado norte-americanos (p. 66/83).

⁴ A despeito de relações de Estados, soberania e regulação de internet Pires afirma que “A história recente da criação de dois Estados Nacionais para a promoção de mecanismos que estabeleçam uma jurisprudência normativa para a regulação do ciberespaço e da Internet no século XX tornou-se ideologicamente justificada pela crescente influência da Internet na soberania e na vida cotidiana de suas relações sociais” (2012, s.p.). In: Pires, Francisco, Hindenburgo. Estados Nacionais, soberania e regulação da internet. Revista Scripta Nova, vol.16,2012. Disponível em: <https://revistes.ub.edu/index.php/ScriptaNova/article/view/14861> Acesso em: 05.05.2025.

projetos tiveram previsão de curto prazo pelo LBD e abarcam todas as três camadas do espaço cibernético: *hardware*, *software* e *peopleware*. Para o projeto de defesa cibernético, o LBD prevê gastos de R\$ 839,9 milhões até 2031, com período de execução até 2035 (Oliveira e Portela, 2017, p. 88).

Ainda, no que diz respeito à segurança cibernética, o Livro Verde é um documento que tem como objetivo reunir propostas e diretrizes básicas sobre o tema, visando fomentar o debate social, econômico, político e técnico científico sobre a segurança cibernética.

A partir do ano de 2020 (pós-pandemia) há um incremento legislativo no Brasil sobre a temática. Em 2021, foi instituída a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) por meio do Decreto nº 10.748, de 16 de julho de 2021, que tem como finalidade o fortalecimento da cooperação e parceria do Governo Federal com os entes federativos, a sensibilização dos órgãos e da população em geral para a necessidade de segurança cibernética e elevação da maturidade da Sociedade Brasileira em segurança da informação e cibernética.

Ao analisar o Decreto nº 10.748 de 16 de julho de 2021, especificamente, em seu art. 4º, inciso VI, é possível encontrar a conceituação de *incidente cibernético* como a:

ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso.

Ainda em 2021, a ANEEL editou a Resolução Normativa nº 24 dispondo sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica⁵. Isso porque, o aumento da conectividade digital das infraestruturas do setor elétrico, aliado à crescente sofisticação das ferramentas de ataque cibernético, tem ampliado significativamente a vulnerabilidade dos sistemas a incidentes maliciosos. Dentre os riscos mais recorrentes estão os ataques com uso de *ransomwares*, voltados a pedidos de resgate e ações de ciberterrorismo (ANEEL, 2021, p. 5).

⁵ No Estado de São Paulo, em decorrência dos episódios recentes de interrupções no fornecimento de energia elétrica, que em determinados casos afetaram mais de um milhão de pessoas (Folha de São Paulo, 2024), encontra-se em tramitação o Projeto de Lei nº 1562/2023, que tem por objetivo estabelecer mecanismos de proteção aos consumidores em situações de blecaute, vendavais e outras ocorrências caracterizadas como calamidade pública (Assembleia Legislativa do Estado de São Paulo, 2023). Verifica-se, portanto, a recorrência de episódios similares no que se refere a incidentes relacionados ao setor energético, o que evidencia a necessidade de medidas preventivas e corretivas por parte do poder público.

Essa Resolução veio em complemento à Resolução Normativa nº 846, de 11 de junho de 2019 da Agência, estabelecendo procedimentos, parâmetros e critérios para a imposição de penalidades aos agentes do setor elétrico. A norma dispõe que as medidas de fiscalização visam “prevenir práticas irregulares e estimular a melhoria contínua da prestação dos serviços de energia elétrica”, bem como, “atuar na busca da correção de práticas irregulares e da reparação ou minimização de eventuais danos à prestação dos serviços de energia elétrica ou aos seus usuários”. Todavia, embora não traga definições sobre o que seriam “práticas irregulares”, a nomenclatura induz à ideia de falhas de atuação humana, não havendo menção a outras externalidades (ANEEL, 2019).

Em reforço, dois anos depois do Decreto nº 10.748/21, em dezembro de 2023, foi instituída a Política Nacional de Cibersegurança (PNCiber), por meio do Decreto nº 11.856/23, que tem como um dos princípios (art. 2º, III): a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade. Ainda, são objetivos da PNCiber, dentre outros (art. 3º, V): estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos.

Nessa perspectiva, observa-se, que, nos últimos cinco anos, houve um avanço significativo na atenção dedicada às questões de proteção cibernética no Brasil, o que reflete não apenas as crescentes demandas internas, mas também a ampliação de uma preocupação global em relação a essa temática. Este movimento acompanha as tendências internacionais, que indicam a cibersegurança como uma prioridade estratégica para a proteção das infraestruturas críticas e a mitigação de riscos associados ao ambiente digital.

Por outro lado, de acordo com o Guia de Defesa Cibernética da América do Sul (2017, p. 69), o Brasil é o país que mais sofreu ataques cibernéticos na América Latina nos últimos anos, sendo o terceiro país que mais faz ataques cibernéticos no mundo. Todavia, estes ataques estiveram relacionados ao acesso de informações e mensagens sigilosas, não havendo repercussão no comprometimento da instabilidade operacional de serviços em nível nacional ou regional.

Diferentemente do evento ocorrido em julho de 2024, ponto de partida deste trabalho, consistente no apagão virtual que colapsou sistemas de computadores no mundo, atingindo setores relevantes como hospitais, bancos, transportes e comunicação. Neste caso específico, indicou-se como causa, uma falha em um sistema de segurança de uma empresa americana chamada CrowdStrike (BBC News, 2024), a qual afetou computadores que usam o sistema operacional Windows, da Microsoft.

Percebe-se, portanto, que os incidentes cibernéticos podem decorrer de ataques cibernéticos, propriamente ditos, ou de colapsos nos sistemas operacionais ou de segurança, ocasionado por fatores internos (atos intencionais ou falhas humanas) ou externos (questões climáticas, acidentes nos satélites, etc).

Tendo em vista este arcabouço normativo aliado ao elemento risco das sociedades modernas, anteriormente analisado, questiona-se: como um incidente cibernético pode vir a consistir em um desastre e quais as medidas preventivas e mitigadoras podem ser aplicadas?

4 DA INSTABILIDADE DO SISTEMA SOCIAL COMO REFERENCIAL TEÓRICO BRASILEIRO E AS PRINCIPAIS CONTRIBUIÇÕES PARA A CONSTRUÇÃO DE HIPÓTESES NO CASO DE DESASTRES CIBERNÉTICOS

Partindo do aporte teórico de Carvalho e Damacena (2013), este capítulo inaugura a análise dos incidentes cibernéticos à luz do Direito dos Desastres, para verificar em qual contexto um incidente desta natureza pode passar a consistir em um desastre.

Atualmente, a construção de um sentido jurídico dos desastres e sua conceituação passa por uma relação entre causas, consequências e capacidade de comprometimento da estabilidade do sistema social. Classificam-se, portanto, quanto às causas em: a) desastres naturais (ex.: vulcões, terremotos); b) antropogênicos (decorrentes de fatores humanos), que podem ser tecnológicos (ex.: contaminações químicas) ou sociopolíticos (ex.: refugiados de guerra, extermínio de civis) ou c) desastres híbridos (sinergia de fatores naturais e antropogênicos).

Embora o aparato para a conceituação dos desastres também possa levar em consideração as consequências do evento lesivo, como perda de vidas e propriedade, existem aspectos de comprometimento de funções ambientais que muitas vezes são subestimados (Carvalho; Damacena, 2013, p. 29).

Assim, uma análise sistêmica que leve em consideração múltiplos fatores, “privilegia a análise da perda da estabilidade do sistema atingido” (Carvalho; Damacena, 2023, p. 32). Dessa forma, quanto ao comprometimento da estabilidade do sistema social, os desastres estariam relacionados a eventos com capacidade de desestabilizar rotinas coletivas das comunidades, gerando uma incapacidade de rápida recuperação.

No Brasil, o Decreto 10.593/2020 dispõe no seu art. 2º, VII, que desastre é o resultado de evento adverso decorrente de ação natural ou antrópica sobre cenário vulnerável que cause danos humanos, materiais ou ambientais e prejuízos econômicos e sociais⁶.

Em sentido similar, a Lei 12.608/2021, alterada pela Lei 14.750, de 2023, dispõe que desastre é o “resultado de evento adverso, de origem natural ou induzido pela ação humana, sobre ecossistemas e populações vulneráveis que causa significativos danos humanos, materiais ou ambientais e prejuízos econômicos e sociais”.

⁶ A UNISDR (2016) da ONU define desastre como uma séria perturbação da ordem social causada pela interação entre um evento perigoso e condições de exposição, vulnerabilidade e capacidade de reação das pessoas e comunidades atingidas por esses eventos.

Há que se considerar que há o potencial de risco e este, eventualmente, se materializa em cenário de desastre. Assim, embora não haja um consenso sobre todas as implicações do conceito de desastres, estes podem ser considerados eventos que causam graves interrupções no funcionamento de uma sociedade, envolvendo (ou não⁷) perdas humanas, materiais, econômicas ou ambientais que excedem a capacidade da sociedade afetada de gerenciá-los. Estes podem assumir uma tipologia antrópica e, conforme afirma Valêncio *et. al*, resultar em sociedades “produtoras de alterações nos sistemas atmosférico, hídricos e demais que constituem o suporte integrado da vida no globo, produzindo cenários pouco alvissareiros segundo reportam os últimos relatórios do *Intergovernmental Panel on Climate Change - IPCC*” (2009, pp. 4).

Assim, mudanças ambientais, como por exemplo, eventos climáticos e disponibilidade hídrica podem ter grandes impactos nas populações. Segundo Young *et. al* “esses impactos, muitas vezes são inter-relacionados e, particularmente graves quando vários eventos ocorrem ao mesmo tempo (Anderson *et al.*, 2021; Leonard *et al.*, 2014) ou em sucessão (Haile *et al.*, 2019). Há que se considerar, portanto, que existe uma vulnerabilidade com relação a localização destas populações (Young *et al.*, 2023).

Partindo da instabilidade do sistema social como referencial teórico para construção do sentido de desastres aliado ao conceito adotado, no Brasil, pelo Decreto 10.593/2020 e pela Lei 12.608/2021, levando em consideração não apenas as consequências do evento, mas também uma análise sistêmica, pautada na capacidade deste de desestabilizar rotinas, entendemos pela possibilidade de um incidente cibernético ser enquadrado, também, como um desastre a depender do contexto em que ocorra.

De acordo como Relatório de Análise de Impacto Regulatório (AIR) nº 2/2021, da ANEEL, que aborda de forma detalhada o risco crescente de incidentes de segurança cibernética no setor elétrico brasileiro, este é um dos setores mais suscetíveis a ataques devido à crescente conectividade e à sofisticação dos cibercriminosos (ANEEL, 2021). Ainda, de acordo com a Agência, os principais atores e grupos potencialmente impactados por incidentes de segurança cibernética no setor elétrico brasileiro incluem os agentes responsáveis pelas infraestruturas críticas do setor, como os prestadores de serviços de geração, transmissão, distribuição e comercialização de energia elétrica, bem como os consumidores e o Operador Nacional do Sistema Elétrico (ONS). Além desses, também são afetados os órgãos institucionais do setor, o governo em geral, a sociedade civil e os fornecedores de tecnologia (ANEEL, 2021).

Considerando as explicações acima, diante de um incidente cibernético que acarrete o comprometimento destes serviços, podemos vislumbrar, exemplificativamente, a interrupção: a) dos sistemas de segurança, gerando a incomunicabilidade da população com esses sistemas; b) dos serviços de transporte e produção, com paralisação dos transportes que dependam das

⁷ Seguindo a linha de Daniel Farber e Délton Winter de Carvalho, as perdas humanas não são um elemento essencial para a definição de desastres.

redes de energia e comunicação, como metrô e sistema aéreo; c) de toda a comunicação via celular, como redes sociais, *whatsapp* e o próprio telefone, e qualquer rede que dependa dos serviços que gravitam no espaço cibernético; d) dos serviços hospitalares e centros médicos que dependem de sistemas de UTI, ventilação e monitoramentos eletrônicos, com a paralisação de equipamentos essenciais, perdas de prontuários médicos e resultados dos exames; e) de acesso a serviços bancários, como saques, pix, ou utilização de cartões de crédito; f) dos sistemas de aquecimento, refrigeração e iluminação das residências e instituições, dentre outros.

Para melhor elucidar, no último 28 de abril de 2025, um apagão massivo atingiu países da Europa (Péchy, 2025), gerando caos no transporte público, no sistema de saúde e na indústria, além de não haver sinal nos celulares por mais de 1 hora. Este curto espaço de tempo foi suficiente para gerar pânico e o desabastecimento de alguns supermercados. Por conta do fato, o Incibe (Instituto Nacional de Cibersegurança da Espanha) foi acionado para verificar as causas. Embora não tenha sido confirmado como ataque cibernético, verifica-se que, neste episódio de apenas poucas horas, houve o desabastecimento de alimentos na cidade de Portugal (G1, 2025).

Por outro lado, como efeitos posteriores a um incidente de longa duração, vislumbra-se não só a escassez e o desabastecimento de itens alimentares e medicamentos, por exemplo, mas também a elevação súbita dos preços bastante comum em fases de pós-desastres, além da retirada de valores das contas bancárias, em dinheiro, para estoque pessoal.

Assim sendo, os desastres cibernéticos transcendem os danos imediatos às infraestruturas digitais, reverberando em esferas sociais e econômicas de forma profunda e prolongada. A instabilidade gerada por tais incidentes compromete a confiança nas instituições financeiras, provoca escassez de bens essenciais e eleva os custos de vida, afetando desproporcionalmente as camadas mais vulneráveis da sociedade. Logo, compreender os efeitos sistêmicos dos desastres cibernéticos é fundamental para o desenvolvimento de políticas públicas eficazes que integrem segurança digital, proteção social e resiliência econômica.

5 DO GERENCIAMENTO DOS RISCOS

Uma vez reconhecida a hipótese de desastre, o capítulo passa a explorar caminhos para prevenir e atenuar riscos. A severidade dos efeitos de um desastre depende das vulnerabilidades e desigualdades já presentes nas áreas atingidas. Partindo desse entendimento, as iniciativas de prevenção ou de reparação devem ser construídas em conjunto com as comunidades locais, assegurando que elas exerçam papel de protagonismo, tenham acesso a informações claras e disponham de mecanismos realmente adequados para proteger seus direitos (Asperti; Zufelato; Garcia, 2020).

Daniel Farber (2019) nos aponta para um modelo circular de tratamento dos desastres, que abarcam as funções de prevenção e mitigação, resposta

emergencial, compensação e reconstrução e mitigação dos riscos futuros (ciclo dos desastres).

Tem-se, portanto, que a fase de prevenção e mitigação de riscos (*risk mitigation*) antecede a ocorrência do desastre, sendo essencial para a redução dos danos potenciais. Nesse sentido, Farber (2012, p. 6 e 7) destaca que os riscos não estão totalmente fora do controle humano e que, por meio de um planejamento adequado, é possível minimizá-los de forma significativa. Por outro lado, a fase de resposta emergencial (*emergency response*) é considerada pelo autor como a mais crítica, pois envolve a atuação imediata diante das condições de emergência já estabelecidas, exemplificada pela mobilização de militares e autoridades civis na execução das ações de resposta.

Por sua vez, a fase da compensação (*compensation*) compreenderia aquela destinada à indenização das vítimas, onde cada sistema jurídico oferece métodos públicos ou privados nesta composição. Já a fase de reconstrução (*rebuilding and restoration*) estaria relacionada aos espaços danificados e a necessidade de reconstrução e manutenção das atividades e serviços seja nos mesmos locais, quando possível, ou o remanejamento para outra localidade.

Ao tratar da resposta aos desastres, o art. 1º, parágrafo único, XII, da Lei 12.608/2012, incluído pela Lei nº 14.750, de 2023, dispõe, dentre outras medidas, que a resposta consistiria em ações imediatas com o objetivo de socorrer a população atingida e restabelecer as condições de segurança das áreas atingidas, incluídas ações de busca e salvamento de vítimas e atendimento médico, sem prejuízo da atenção aos problemas crônicos e agudos da população, de provisão de alimentos e meios para sua preparação e abrigo.

O primeiro ponto que se observa quando tratamos do gerenciamento dos riscos de desastres cibernéticos, é a absoluta ausência de informação da população sobre esses riscos, o que dificulta qualquer possibilidade de mobilização ou de apoio caso este cenário se concretize. Uma população desinformada não possui meios de se preparar e de colaborar para a mitigação dos próprios riscos. De forma semelhante, observa-se que as instituições também falham na divulgação de medidas preventivas, o que agrava ainda mais a vulnerabilidade diante desses eventos. Um exemplo elucidativo pode ser observado a seguir.

Em novembro de 2024, a Organização Mundial de Saúde emitiu um alerta sobre o aumento alarmante de ataques de *ransomware* nas infraestruturas de saúde no mundo (Mishra, 2024). De acordo com a página da ONU, estes ataques são uma forma de ataque cibernético em que um agente malicioso “assume” ou “bloqueia” arquivos em um único computador ou em uma rede inteira, exigindo pagamento em troca de acesso.

Em termos práticos, o ataque cibernético compromete o acesso aos prontuários digitais e serviços de diagnósticos essenciais, como os resultados dos exames, perdendo-se o histórico de cada paciente e o acesso à simples consulta dos prontuários, o que inviabiliza a realização de cirurgias e outros procedimentos médicos. Neste contexto, as unidades de terapia intensiva e todos os tratamentos que possam depender de aparelhos, também podem ser

diretamente afetados, colocando em risco a saúde e a vida de milhares de pacientes.

Por esta razão, como mitigação e gerenciamento de riscos, nos casos envolvendo as infraestruturas de saúde, sugere-se que a manutenção de arquivos, prontuários e resultados de exames em papéis físicos, ao menos durante o tempo da internação dos pacientes, podem servir de baliza para a redução dos riscos, por exemplo.

Já para a população em geral, a elaboração de cartilhas regionais e estaduais podem servir de guia prático, atendendo especificamente às necessidades e estruturas de cada localidade, com indicações não só dos itens básicos de manutenção, mas também de eventuais pontos físicos de apoio dos governos locais, especialmente os grupos mais vulneráveis.

Em proposta similar, o Protocolo “Acesso à Justiça e Desastres”: Recomendações Elaboradas para o Sistema de Justiça para Atuação em Casos de Desastres (FGV, 2023), traz na Recomendação de nº 15, a criação de Sistemas de Alerta, nos seguintes termos:

15.1. Criação e instalação de sistemas de alerta: Exigir de empresas e municípios a instalação de sistemas de alerta próximo a infraestruturas com risco de colapso ou áreas de risco em geral. Tais sistemas podem incluir: instalação de sirenes, criação de sistemas de alerta via SMS ou plataformas similares.

15.2. Simulações e manutenção: Exigir a realização de manutenção contínua e simulados periódicos dos sistemas de alerta.

15.3. Treinamento e divulgação: Realizar conjuntamente com empresas e municípios ou exigir a realização de treinamentos com a população para publicizar e preparar as pessoas em áreas de risco sobre o funcionamento dos sistemas de alerta e dos planos de ação e emergência.

15.3. Fiscalização e monitoramento: Exigir a prestação periódica de informações, pelas empresas e municípios, sobre os sistemas de alerta instalados e realizar monitoramento contínuo.

15.4. Mecanismos adicionais de alerta: Manter canais de diálogo com a população para informação sobre riscos, incluindo páginas na internet e mídias sociais, e publicização de planos de ação e emergência.

Por sua vez, no tange ao sistema jurídico, partindo da estrutura normativa apresentada ao longo do trabalho, avança-se, ao lado do direito material dos desastres, nas ferramentas processuais para o tratamento adequado destes pelo sistema de justiça para fins de redução das vulnerabilidades e dos riscos, o que se convencionou denominar de direito processual dos desastres.

No dizer de Carvalho; Zaneti Jr (2023, p. 02):

a evolução do Direito dos Desastres, no Brasil, “está saindo de uma primeira fase de *Law in the Books* e conscientização de sua existência pelos operadores e teóricos do Direito, para uma fase

de *Law in Action*, isto é, de sua aplicação para a obtenção de uma solução justa e equitativa em casos práticos.

Acompanhando o ciclo dos desastres de Farber, as medidas processuais cabíveis atuariam especificamente em cada uma das fases, aplicando-se tutelas inibitórias ou de remoção de ilícito para a fase preventiva e de mitigação de desastres; tutelas de urgência para a fase de resposta emergencial; tutelas ressarcitórias para a fase de compensação e tutelas ressarcitórias específicas para a fase de reconstrução pós desastre (Andrea, 2023, p. 240).

Todavia, o que chama a atenção nos casos de desastres cibernéticos é que o Poder Judiciário será igualmente atingido em seus sistemas. Isso porque, sem o funcionamento dos sistemas de energia e internet, as operações do judiciário ficarão suspensas. O cenário é mais alarmante do que o ocorrido no período da pandemia em que, ao menos virtualmente, as audiências e tutelas provisórias de urgência eram emitidas. Já no cenário aqui levantado, não haverá sequer acesso aos sistemas dos Tribunais, inviabilizando, inclusive, as audiências de custódia, pois, mesmo presencialmente, não haveria comunicação entre os sistemas das Delegacias e do Judiciário e nem da população com os sistemas de emergência e segurança.

Nestes casos, é válida a Recomendação nº 02 da FGV (2023), quanto ao incentivo (ou exigência) para que agentes públicos realizem cursos de capacitação sobre gestão de riscos e desastres, com cursos voltados para diferentes níveis hierárquicos e áreas de atuação dos agentes públicos, abordando temas como prevenção, resposta a emergências, coordenação de operações, entre outros.

No que diz respeito ao setor elétrico, a ANEEL orienta uma política de segurança cibernética para o setor, válida para todas as geradoras, distribuidoras e transmissoras de energia no país, incluindo procedimentos de resposta rápida para contenção de incidentes, recomendando a promoção junto aos funcionários, de uma conscientização acerca dos riscos cibernéticos por meio de exercícios cibernéticos (ANEEL, 2021).

Isso porque, a ausência de uma política robusta de segurança cibernética no setor elétrico aumenta significativamente os riscos de interrupções no fornecimento de energia, além de ampliar as vulnerabilidades relacionadas ao acesso não autorizado a dados sensíveis. Nesse cenário, ataques cibernéticos tornam-se uma ameaça concreta à estabilidade e à confiabilidade do sistema, com potencial para provocar apagões de grande escala e consequências severas para a população e a economia. Reconhecendo essa vulnerabilidade, a segurança cibernética passou a ser tratada como uma questão estratégica de segurança nacional (Branquinho; Leal, 2022).

Nessa perspectiva, é salutar ressaltarmos que a publicação da Rotina Operacional RO-CB.BR.01 pelo Operador Nacional do Sistema Elétrico (ONS) marcou uma mudança significativa na forma como a segurança cibernética é tratada no setor elétrico brasileiro. Dentre os principais requisitos estabelecidos pela RO-CB.BR.01 estão: a nomeação de gestores responsáveis pela segurança cibernética, a elaboração de políticas de governança claras e o inventário

detalhado e seguro de todos os ativos conectados ao ARCiber. Essas e outras diretrizes visam fortalecer a resiliência cibernética do setor e evitar que vulnerabilidades individuais comprometam a estabilidade de todo o sistema elétrico nacional (ONS,2021).

Verifica-se, portanto, que as estratégias de gestão de riscos constituem um elemento fundamental para garantir uma margem de ação, sobretudo em cenários inesperados, sendo ainda mais deficitária a gestão dos riscos cibernéticos no Brasil. Do ponto de vista institucional, o aparato preventivo ainda é incipiente e demanda esforços para avançar nas medidas de mitigação, bem como de preparo da população para esses eventos extremos.

Em arremate, entende-se que é fundamental a compreensão de que, na sociedade contemporânea, os riscos cibernéticos não apenas coexistem com os riscos tradicionais, mas frequentemente os amplificam, criando cenários de desastres híbridos que desafiam as estruturas normativas e operacionais existentes. A crescente interdependência dos sistemas digitais e físicos torna as infraestruturas críticas vulneráveis a falhas sistêmicas desencadeadas por incidentes cibernéticos.

Nesse contexto, a integração dos conceitos de risco e desastre é essencial para o desenvolvimento de políticas públicas eficazes que abordem a complexidade dos desafios contemporâneos. Logo, a construção de uma resiliência sistêmica requer não apenas a atualização dos marcos legais e regulatórios, mas também a promoção de uma cultura de prevenção e resposta coordenada entre os diversos setores da sociedade.

CONCLUSÃO

Como resultado das análises empreendidas ao longo deste artigo, temos que esta é uma contribuição que permite diversas abordagens sobre a temática dos desastres cibernéticos que, certamente, não se encerram nas observações aqui trazidas, que constituem apenas um ponto de partida para o desenvolvimento do tema.

Na sociedade de risco Beck (2010) o único cenário que podemos esperar é o inesperado, portanto, é necessário ponderar sobre a construção institucional de margens de segurança para eventos extremos, uma vez que diante deste contexto social a única certeza é a incerteza, e o inesperado torna-se uma constante. Diante disso, torna-se imperativo refletir sobre a construção de diretrizes que possam mitigar os impactos de eventos extremos, como os desastres cibernéticos. Consequentemente, tais nortes devem ser entendidas não apenas como medidas técnicas, mas como construções sociais que envolvem a participação ativa da sociedade, a cooperação entre diferentes setores e a adaptação contínua às novas ameaças que emergem em um mundo cada vez mais interconectado e digitalizado.

Com base nesse aparato normativo e outros assinalados ao longo do trabalho, o artigo foi estruturado em seis partes, abarcando: introdução, desenvolvimento em quatro capítulos sobre os riscos, o aprofundamento do panorama normativo brasileiro, a construção da hipótese de desastre

cibernético e o gerenciamento dos riscos e conclusão. A metodologia é revisão narrativa de literatura articulada com a construção de uma situação hipotética, com base no evento ocorrido em 19 de julho de 2024 e nas medidas de sobrevivência emitidas pela França, em março de 2025, para questionar se estamos preparados para o enfrentamento dos riscos de um desastre cibernético de nível global que implique em ausência de funcionamento das redes de energia e internet por período superior a 72 horas.

Assim, retomando a hipótese levantada na introdução, caso o evento ocorrido em 19 de julho de 2024 se repita e perdure por 72 horas, marco pautado nas medidas de sobrevivência emitidas pelo governo da França (Euronews, 2025), entendemos que um incidente cibernético desta proporção, pode se enquadrar na hipótese de desastre, com capacidade de desestabilizar rotinas e gerar impactos sociais e econômicos de grandes proporções. Isso porque, tais eventos podem comprometer serviços essenciais, como energia, saúde e finanças, resultando em impactos comparáveis aos de desastres naturais de grande magnitude.

Seguindo por essa linha de raciocínio, os objetivos propostos foram alcançados de forma que primeiro, mapeou-se a evolução normativa nacional, evidenciando que, embora o Brasil disponha de dispositivos robustos para eventos naturais e antrópicos tradicionais, carece de articulação formal entre Defesa Civil e cibersegurança. Em seguida, demonstrou-se que um incidente cibernético de 72 horas, enquadra-se nos requisitos legais de “desastre”, por comprometer a estabilidade social e a capacidade de recuperação rápida. Por fim, apresentaram-se medidas concretas: inclusão expressa de incidentes cibernéticos na Política Nacional de Proteção e Defesa Civil, planos setoriais de continuidade (energia, internet, saúde, Judiciário).

Portanto, o presente estudo oferece uma contribuição ao debate jurídico-institucional ao expor a formulação de um marco regulatório alinhado às transformações da sociedade contemporânea, profundamente marcada pela intensificação das tecnologias digitais e pela crescente dependência de infraestruturas críticas. Tal marco é concebido com base em uma abordagem sistêmica e integrada, capaz de articular, em um único ciclo normativo, as fases de prevenção, resposta emergencial, compensação e reconstrução diante de eventos disruptivos, especialmente no contexto de riscos cibernéticos e energéticos. Ao adotar uma visão global, essa proposta busca não apenas responder a desastres, mas também fortalecer a capacidade institucional de antecipar e mitigar ameaças, contribuindo para a construção de um arcabouço jurídico mais resiliente e adaptativo.

Nesse sentido, recomenda-se que estudos futuros aprofundem análises comparativas com experiências internacionais consolidadas, de modo a identificar boas práticas regulatórias e aprimorar o desenho institucional brasileiro. Além disso, recomenda-se o desenvolvimento de indicadores específicos de resiliência legislativa e institucional, os quais podem subsidiar políticas públicas mais eficazes e sustentáveis, reforçando a capacidade do Estado brasileiro de enfrentar, com maior preparo, os riscos emergentes de uma

sociedade hiperconectada, que demanda matrizes energéticas e cibersegurança.

REFERÊNCIAS

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL. *Resolução nº 24, de 20 de setembro de 2021*. Dispõe sobre diretrizes para a contratação de reserva de capacidade de energia elétrica. Brasília, DF: ANEEL, 2021. Disponível em: <https://www2.aneel.gov.br/cedoc/res2021024cnpe.pdf>. Acesso em: 6 maio 2025.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL. *Resolução Normativa nº 964, de 14 de dezembro de 2021*. Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Brasília, DF: ANEEL, 2021. Disponível em: <https://www2.aneel.gov.br/cedoc/ren2021964.html>. Acesso em: 7 abr. 2025.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). *Relatório de Análise de Impacto Regulatório nº 2/2021*. Brasília: ANEEL, 2021. Disponível em: <https://www2.aneel.gov.br/cedoc/air2021002srt.pdf>. Acesso em: 25 abr. 2025.

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). *Resolução Normativa nº 846, de 11 de junho de 2019*. Aprova procedimentos, parâmetros e critérios para a imposição de penalidades aos agentes do setor de energia elétrica e dispõe sobre diretrizes gerais da fiscalização da Agência. Diário Oficial da União, Brasília, DF, Seção 1, p. 37, 18 jun. 2019. Disponível em: <https://www2.aneel.gov.br/cedoc/ren2019846.html>. Acesso em: 14 mar. 2025.

ANDERSON, W. et. al. Violent conflict exacerbated drought-related food insecurity between 2009 and 2019 in sub-Saharan Africa. *Nature Food*, v. 2, p. 603-615, 2021. DOI: 10.1038/s43016-021-00327-4.

ANDREA, G. F. M. *Processo estrutural dos desastres: dever estatal de prevenção a partir do paradigma das calamidades hidrológicas*. Londrina: Thoth Editora, 2024.

ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO. *Projeto de Lei nº 1562, de 8 de novembro de 2023*. Autoria: Rafa Zimbaldi. Disponível em: https://www.al.sp.gov.br/spl/2023/11/Propositura/1000537007_1000677101_Propositura.pdf. Acesso em: 14 mar. 2025.

BBC NEWS. *CrowdStrike e Microsoft: o que se sabe sobre a pane global de TI*. 19 jul. 2024. Disponível em: <https://www.bbc.com/portuguese/articles/cjr4l9nndd4do>. Acesso em: 22 abr. 2025.

BECK, U. *Sociedade de risco: rumo a uma nova modernidade*. Tradução de Sebastião Nascimento. São Paulo: Ed. 34, 2010.

BRANQUINHO, M.; LEAL, R. *Capítulo VII – Ambiente regulatório de segurança cibernética para empresas de energia no Brasil*. O Setor Elétrico, 16 mar. 2022. Disponível em: <https://www.osetoelettrico.com.br/capitulo-vii-ambiente-regulatorio-de-seguranca-cibernetica-para-empresas-de-energia-no-brasil/>. Acesso em: 7 abr. 2025.

CADIP – CENTRO DE APOIO AO DIREITO PÚBLICO. *Catástrofes urbanas e o Direito dos Desastres*. TJSP, 2024.

CARVALHO, D. W. *A natureza jurídica da pandemia covid-19 como um desastre biológico*. Revista dos Tribunais, v. 1017, jul. 2020. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/CEJUR%20%20PGM/CEJUR%20Clipping/5%C2%AA%20Edi%C3%A7%C3%A3o/Artigos/9.pdf>. Acesso em: 23 out. 2024.

CARVALHO, D. W. Direito Internacional dos Desastres: da centralidade na resposta humanitária à formação do dever internacional de redução de riscos de desastres. *Revista Brasileira de Políticas Públicas e Internacionais*, v. 5, n. 2, 2020. Disponível em: <https://periodicos.ufpb.br/index.php/rppi/article/view/52677>. Acesso em: 21 out. 2024.

CARVALHO, D. W. *O que devemos urgentemente aprender com o novel Direito dos Desastres*. Disponível em: <https://www.conjur.com.br/2019-jan-29/delton-winter-devemos-aprender-direito-desastres>. Acesso em: 10 out. 2024.

CARVALHO, D. W.; DAMACENA, F. D. L. *Direito dos Desastres*. Porto Alegre: Livraria do Advogado Editora, 2013.

CARVALHO, D. W.; ZANETI JR., H. O Direito Processual dos Desastres e o Papel das Cortes Judiciais na Prevenção e no Preparo aos Desastres. *Revista de Processo*, v. 346, p. 167-194, 2023.

CASTELLS, M. *A sociedade em rede*. Tradução de Roneide Venâncio Majer; atualização para a 6ª ed. de Jussara Simões. São Paulo: Paz e Terra, 1999.

FARBER, D. Disaster Law and Emerging Issues in Brazil. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)*, v. 4, n. 1, p. 2-15, jan-jun. 2012. Disponível em: <https://webcache.googleusercontent.com/search?q=cache:bCLRuNRtpdEJ:https://dialnet.unirioja.es/descarga/articulo/5007566.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 21 out. 2024.

FGV. *Desastres ambientais: experiências nacionais e internacionais*. Disponível em:

https://fgvprojetos.fgv.br/sites/fgvprojetos.fgv.br/files/publicacao_desastres_ambientais_miobilingue_final-web.pdf. Acesso em: 28 out. 2024.

FGV. *Parâmetros para uma Abordagem Baseada em Direitos Humanos para a Resposta e Reconstrução de Desastres Envolvendo Empresas*. Fundação Getúlio Vargas. Rio de Janeiro; São Paulo: FGV, 2019.

FGV. *Protocolo Acesso à Justiça e Desastres: Recomendações elaboradas para o sistema de justiça para atuação em casos de desastres* / Fundação Getúlio Vargas. – São Paulo: FGV, 2023.

FOLHA DE SÃO PAULO. *Depois de 24 horas, SP tem 1,35 milhão sem luz e revive pesadelo de apagão*. Folha de São Paulo, São Paulo, 12 out. 2024. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2024/10/depois-de-24-horas-sp-tem-135-milhao-sem-luz-e-revive-pesadelo-de-apagao.shtml>. Acesso em: 14 mar. 2025.

FÓRUM ECONÔMICO MUNDIAL. *Cyber resilience in the oil and gas industry: playbook for boards and corporate officers*. 2021. Disponível em: <https://www.weforum.org/publications/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers/>. Acesso em: 25 abr. 2025.

G1. *Jornalista brasileira relata falta de mantimentos em mercado após apagão; sensação de 'fim de mundo'*. G1 Pará, 28 abr. 2025. Disponível em: <https://g1.globo.com/pa/para/noticia/2025/04/28/jornalista-brasileira-relata-falta-de-mantimentos-em-mercado-apos-apagao-sensacao-de-fim-de-mundo.ghtml>. Acesso em: 28 abr. 2025.

GARCÍA-TORNEL, F. C. *Sociedades y territorios en riesgo*. Barcelona: Ediciones del Serbal, 2001.

GEORGIADOU, A.; MICHALITSI-PSARROU, A.; ASKOUNIS, D. A security awareness and competency evaluation in the energy sector. *Computers & Security*, v. 129, 2023. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404823001098>. Acesso em: 07 abr. 2025. <https://doi.org/10.1016/j.cose.2023.103199>.

HAILE, G. G.; TANG, Q.; SUN, S.; HUANG, Z. Liu Droughts in East Africa: Causes, impacts and resilience. *Earth-Science Reviews*, v. 193, 2019, p. 146-161, DOI 10.1016/j.earscirev.2019.04.015.

IEA – INTERNATIONAL ENERGY AGENCY. *Power systems in transition*. Paris: International Energy Agency, 2020. Disponível em: <https://www.iea.org/reports/power-systems-in-transition>. Licença: CC BY 4.0. Acesso em: 25 abr. 2025.

LEONARD, M. et al. A compound event framework for understanding extreme impacts. *Wiley Interdisciplinary Reviews: Climate Change*, v. 5, p. 113-128, 2014. DOI 10.1002/wcc.252.

MENEZES NETO, E. J. *Surveillance, democracia e direitos humanos: os limites do Estado na era do big data*. 2016. 293 f. Tese (Doutorado em Direito) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2016. Disponível em: https://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/5530/Elias%20Jacob%20de%20Menezes%20Neto_.pdf?sequence=1&isAllowed=y. Acesso em: 9 abr. 2025.

MISHRA, V. *Cyberattacks on healthcare: A global threat that can't be ignored*. UN News, 8 nov. 2024. Disponível em: https://news-un-org.translate.google/en/story/2024/11/1156751?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 05 maio 2025.

OLIVEIRA, L. C. *Participação direta no litígio coletivo: reflexões a partir da análise do Caso Braskem*. 2024. 231 p. Dissertação (Mestrado em Ciências) – Programa de Pós-Graduação em Direito, Faculdade de Direito de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2024.

OLIVEIRA, M. A. G. et al. *Guia de Defesa Cibernética da América do Sul*. Recife: Ed. UFPE, 2017.

OLIVEIRA, M. A. G.; PORTELA, L. S. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. *Revista Brasileira de Estudos de Defesa*, v. 4, n. 2, jul./dez. 2017, p. 77-99 DOI: 10.26792/RBED.v4n2.2017.75014.

OPERADOR NACIONAL DO SISTEMA ELÉTRICO (ONS). *Manual de Procedimentos da Operação*: Módulo 5 – Submódulo 5.13: Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético – RO-CB.BR.01. Revisão 00. Rio de Janeiro: ONS, 2021. Disponível em: https://www.ons.org.br/AcervoDigitalDocumentosEPublicacoes/RO-CB.BR.01_Rev.00.pdf. Acesso em: 9 abr. 2025.

PAZ, S M. I. *Ciência, Tecnologia e Inovação na Guerra: Reflexões para a Defesa Cibernética Brasileira a partir do Estudo De Casos Internacionais*. Dissertação de Mestrado pela Marinha do Brasil, Escola de Guerra Naval, 2019.

PÉCHY, A. *Apagão massivo atinge Portugal e Espanha: outros países europeus reportam falha*. VEJA, São Paulo, 28 abr. 2025. Disponível em: <https://veja.abril.com.br/mundo/apagao-massivo-atinge-portugal-e-espanha-outros-paises-europeus-reportam-falha/>. Acesso em: 22 abr. 2025.

RIBEIRO, W. C. *COVID-19: passado, presente e futuro*. Universidade de São Paulo. Faculdade de Filosofia, Letras e Ciências Humanas, 2020. DOI: Disponível em: www.livrosabertos.abcd.usp.br/portaldelivrosUSP/catalog/book/552. Acesso em 5 maio 2025.

SCHWAB, K.; DAVIS, N. *Aplicando a quarta revolução industrial*. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SCIENCEDIRECT. *Technological disaster*. ScienceDirect Topics, Elsevier. Disponível em: <https://www.sciencedirect.com/topics/computer-science/technological-disaster>. Acesso em: 13 maio 2025.

UNITED NATIONS OFFICE FOR DISASTER RISK REDUCTION (UNDRR). *Sendai Framework for Disaster Risk Reduction 2015–2030*. Geneva: UNDRR, 2015. Disponível em: <https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030>. Acesso em: 23 abr. 2025.

VALENCIO, N. Da morte da quimera à procura de pégaso: a importância da interpretação sociológica na análise do fenômeno denominado desastre. In: VALENCIO, N.; SIENA, M.; MARCHEZINI, V.; COSTA, J. (orgs.). *Sociologia dos desastres: construção, interfaces e perspectivas no Brasil*. São Carlos: RiMa Editor, 2009.

VASCONCELOS, Y. Os impactos do mundo digital no ambiente. *Revista Pesquisa FAPESP*, São Paulo, n. 349, ano 26, p. 12-21, mar. 2025.

VENTRE, D. Ciberguerra. In: Academia General Militar. *Seguridad Global y Potencias Emergentes en un Mundo Multipolar*. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza.

YOUNG, H. R. et al. Strata: Mapping climate, environmental and security vulnerability hotspots. *Political Geography*, v. 100, 2023, 102791, ISSN 0962-6298. DOI: <https://doi.org/10.1016/j.polgeo.2022.102791>.

ZANIRATO, S. H.; RAMIRES, J. Z. S.; AMICCI, A. G. N.; ZULIMAR, M. R.; RIBEIRO, W. C. Sentidos do risco: interpretações teóricas. Biblio 3W, *Revista Bibliográfica de Geografía y Ciencias Sociales*, Universidad de Barcelona, Vol. XIII, nº 785, 25 de mayo de 2008. Disponível em: <http://www.ub.es/geocrit/b3w-785.htm>. Acesso em 18 abr. 2025.