XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

A VULNERABILIDADE DA SOCIEDADE EM FACE DO IMPÉRIO DA TECNOLOGIA.

THE VULNERABILITY OF SOCIETY FACING THE EMPIRE OF TECHNOLOGY.

Stephanie Cordeiro de Lima Silva [1]
Thaysla Caroline Lebron da Cunha [2]
Antônio Carlos Diniz Murta [3]

Resumo

Este artigo investiga os riscos profundos da hiperconectividade e da digitalização para a sociedade moderna. Parte da premissa de que lembranças, dados financeiros, comunicações e registros públicos estão armazenados em ambientes tecnológicos frágeis e expostos a falhas que podem desencadear um colapso institucional. A seção histórica revisita a evolução da internet da ARPANET à sociedade em rede destacando episódios como o ataque cibernético à Estônia (2007) e incidentes recentes como falhas da AWS, ataques por ransomware a sistemas de saúde, e um apagão digital global em 19 de julho de 2024. A análise destaca que nossa dependência tecnológica é invisível e estrutural, afetando desde operações financeiras cotidianas até o funcionamento do Estado, o que compromete a soberania informacional e direitos fundamentais. No âmbito jurídico brasileiro, reconhece-se que dispositivos como a Lei Geral de Proteção de Dados Pessoais não contemplam a continuidade informacional ou a preservação da memória institucional em casos de falhas graves.

Palavras-chave: Vulnerabilidade social, Tecnologia, Colapso digital, Riscos, Preservação

Abstract/Resumen/Résumé

This article investigates the profound risks posed by hyperconnectivity and digitalization to modern society. It starts from the premise that memories, financial data, communications, and public records are stored in fragile technological environments vulnerable to failures capable of triggering institutional collapse. The historical section revisits the evolution of the Internet from ARPANET to the networked society highlighting episodes such as the 2007 cyberattack on Estonia and recent incidents like AWS failures, ransomware attacks on healthcare systems, and a global digital blackout on July 19, 2024. The analysis underscores that our technological dependence is both invisible and structural, impacting everything from daily financial operations to state functions, thereby compromising informational sovereignty

[1] Advogada; Especialista em Direito Digital e Proteção de Dados pelo Ebradi; bolsista do programa PROSUP.

[2] Mestranda em Direito pela Universidade FUMEC. Especialista em Direito Público pela PUC Minas. Especialista em Direito Constitucional e Governança Pública pela PUC Minas. Assessora Parlamentar na ALMG.

[3] Professor titular da Universidade FUMEC; Procurador do Estado de Minas Gerais.

and fundamental rights. Within the Brazilian legal framework, it is acknowledged that instruments such as the General Data Protection Law do not address informational continuity or the preservation of institutional memory in the event of severe failures.

Keywords/Palabras-claves/Mots-clés: Social vulnerability, Technological, Digital collapse, Risks, Preservation

1 INTRODUÇÃO

Vivemos em uma era digital onde tudo, memórias, dados bancários, comunicações, conhecimentos, registros públicos e privados estão armazenados em servidores e sistemas conectados à internet. Mas o que aconteceria se, de repente, tudo isso desaparecesse? A simples hipótese de um colapso tecnológico, seja por um apagão elétrico em larga escala, um ataque cibernético global ou falhas sistêmicas em infraestrutura crítica, pode revelar o quanto somos vulneráveis.

Vivemos cercados por telas, senhas, servidores, dados em nuvem. Tudo está conectado e tudo depende da tecnologia. Mas e se, de repente, tudo se apagasse? Se o mundo digital simplesmente deixasse de responder? Nenhuma rede. Nenhum dado. Nenhuma memória.

O que antes parecia cenário de ficção científica hoje se torna uma possibilidade cada vez mais real. Apagões digitais, ciberataques, falhas energéticas em larga escala e até fenômenos naturais extremos podem colocar abaixo a infraestrutura que sustenta governos, economias, identidades e histórias. A pergunta inquietante que este artigo propõe é: o que acontece com a sociedade quando a tecnologia falha?

Mais do que uma análise técnica, esta é uma reflexão filosófica sobre a nossa vulnerabilidade coletiva. A era digital prometeu eternidade de memória, agilidade de informação e segurança de dados. Mas talvez tenhamos construído um castelo de areia: sofisticado, rápido, bonito, porém frágil.

Este artigo percorre os riscos de uma civilização hiperconectada, os possíveis colapsos, os "planos B" de alguns países, e, por fim, propõe um olhar filosófico inspirado em pensadores como Foucault, Arendt e Agamben sobre o que resta da humanidade quando o mundo digital falha.

2 A VISÃO HISTÓRICA DA INTERNET: DAS ORIGENS MILITARES AO USO COTIDIANO

A internet, hoje percebida como espaço natural de sociabilidade, informação e economia, nasceu em um contexto bastante distinto. Sua gênese remonta à Guerra Fria, quando os Estados Unidos criaram, em 1969, a ARPANET, projeto da Advanced Research Projects Agency (ARPA), voltado para assegurar a comunicação militar mesmo em caso de ataque nuclear. A lógica distribuída da rede buscava garantir que a informação sobrevivesse a

eventuais destruições locais, inaugurando um paradigma de resiliência técnica que se tornaria a marca das redes digitais (CASTELLS, 2003).

Na década de 1980, com o fim do monopólio militar, universidades e centros de pesquisa passaram a utilizar a internet como ferramenta de troca científica. O desenvolvimento dos protocolos TCP/IP e a criação da World Wide Web por Tim Berners-Lee, em 1989, transformaram a rede em um espaço acessível e globalizado, abrindo caminho para a apropriação civil e, posteriormente, para a popularização doméstica nos anos 1990. Desde então, a internet deixou de ser mera infraestrutura de defesa para se tornar um ambiente estruturante da vida social, reorganizando práticas comunicacionais, econômicas e políticas em escala planetária (LÉVY, 1999).

O avanço do século XXI marcou a consolidação da chamada sociedade em rede, caracterizada pela centralidade da informação digital em todas as esferas da vida cotidiana. Serviços bancários, registros jurídicos, sistemas de saúde e até a sociabilidade interpessoal migraram para o ambiente online. Essa ubiquidade, contudo, ampliou as vulnerabilidades sociais e jurídicas diante da falha tecnológica, transformando a internet em elemento estratégico para a própria continuidade institucional (MOROZOV, 2020).

Um exemplo paradigmático desse processo é a Estônia, considerada um dos países mais digitalizados do mundo. Após sua independência, em 1991, o país investiu em um modelo de governo eletrônico que integrou educação, saúde, votação online e serviços públicos em plataformas digitais unificadas. Esse pioneirismo trouxe ganhos de eficiência e transparência, mas também revelou fragilidades: em 2007, a Estônia sofreu um dos primeiros ataques cibernéticos em larga escala da história, que paralisou bancos, ministérios e meios de comunicação. O episódio levou o país a reforçar seus protocolos de cibersegurança e a sediar o Centro de Excelência em Defesa Cibernética da OTAN, demonstrando que até sociedades altamente digitalizadas permanecem expostas a riscos estruturais (KASPERSKY, 2025; BBC, 2025).

Assim, compreender a trajetória histórica da internet de um projeto militar restrito a uma infraestrutura civil ubíqua é fundamental para situar a vulnerabilidade contemporânea diante da dependência digital. A promessa inicial de resiliência técnica, que buscava proteger a informação em tempos de guerra, transformou-se, paradoxalmente, em novo ponto de fragilidade: a sociedade global tornou-se refém de sua própria interconexão.

3 A HIPERDIGITALIZAÇÃO DA SOCIEDADE

Nas últimas três décadas, a sociedade global passou por um processo intenso e irreversível de digitalização. Arquivos físicos cederam lugar a bancos de dados digitais; a informação, outrora armazenada em papel, agora flutua em servidores, nuvens computacionais e redes descentralizadas. Esse movimento, inicialmente celebrado como sinal inequívoco de progresso, carrega em seu bojo uma dependência invisível e perigosa.

A transformação digital trouxe facilidades inegáveis: certidões e documentos legais tornaram-se acessíveis em segundos; prontuários médicos podem ser compartilhados entre instituições em tempo real; obras de arte, fotografias e memórias familiares encontram-se armazenadas em plataformas digitais; e o dinheiro, cada vez mais imaterial, circula em forma de criptomoedas ou saldos eletrônicos.

Essa nova configuração sociotécnica é resultado do que Pierre Lévy denominou como "cibercultura", um ecossistema no qual o conhecimento é descentralizado, fluido e constantemente reconfigurado pela interação digital dos sujeitos. A promessa da era digital foi democratizar o saber, desmaterializar a burocracia e eternizar a memória coletiva. No entanto, a ausência de materialidade não implica ausência de risco. Pelo contrário: quanto mais etérea a informação, mais frágil pode se tornar sua preservação (LÉVY, 1999).

O sociólogo espanhol Manuel Castells já alertava, ainda nos anos 1990, que a "sociedade em rede" se estruturaria em torno de fluxos informacionais, cuja interrupção colocaria em xeque não apenas as comunicações, mas as próprias estruturas de poder, economia e identidade (CASTELLS, 2003).

A dependência da infraestrutura digital é tão profunda que eventos como falhas elétricas em larga escala, ciberataques devastadores ou simples corrupções de banco de dados podem, literalmente, apagar capítulos inteiros da história contemporânea. Ao delegarmos à nuvem a guarda dos nossos bens jurídicos, afetivos e culturais, nos tornamos vulneráveis a um novo tipo de colapso: o colapso da memória digital.

Essa transição pode ser visualmente representada na tabela a seguir, que explicita a passagem do mundo material para o digital:

Categoria	Modelo Analógico (Passado)	Modelo Digital (Atualidade)
Certidões e Documentos	Registros físicos em papel, armazenados em cartórios	Arquivos digitais, em sistemas notariais e cartoriais online
Prontuários Médicos	Pastas físicas arquivadas em hospitais e consultórios	Sistemas eletrônicos interligados, suscetíveis a falhas e ciberataques

Memória Pessoal e Cultural	Fotografias, cartas, diários, álbuns físicos	Armazenamento em nuvem (Google Photos, iCloud), sem cópias físicas
Conhecimento Científico	Livros, periódicos impressos, bibliotecas físicas	Bases de dados digitais, periódicos online, bibliotecas digitais
Dinheiro e Investimentos	Dinheiro em espécie, aplicações bancárias com registro físico	Moedas digitais, banking online, criptomoedas

Fonte: elaboração própria, a partir da observação dos processos de digitalização social e documental.

Como se observa na tabela acima, a sociedade contemporânea migrou de uma estrutura baseada em objetos físicos palpáveis, arquiváveis, visualmente recuperáveis para uma lógica de fluxos digitais intangíveis. Embora o ganho em agilidade e volume de armazenamento seja inegável, o novo modelo é marcado por uma vulnerabilidade radical: tudo depende da permanência e integridade da infraestrutura tecnológica.

Como assinala Byung-Chul Han, a fluidez dos dados não garante sua segurança, em que a ausência do suporte físico é, paradoxalmente, o ponto frágil de uma civilização que aposta na eternidade da memória digital. O digital, ao prometer perenidade, ignora sua própria efemeridade técnica: *"*o excesso de positividade da informação não gera clareza, mas confusão e vulnerabilidade" (HAN, 2017).

Nesse cenário, surge uma questão jurídica e filosófica inadiável: quem responde quando a tecnologia falha? E mais quem somos nós sem os nossos dados?

4 A DEPENDÊNCIA DIGITAL: INVISÍVEL E ESTRUTURAL

Se há algo ainda mais perigoso do que a vulnerabilidade digital, é o fato de que ela é amplamente invisível. A sociedade contemporânea internalizou a tecnologia de tal forma que já não percebe a extensão da sua dependência. O uso de sistemas digitais deixou de ser percebido como mediação e passou a ser vivido como condição natural da existência. Essa invisibilidade torna o risco ainda mais grave: não se prepara para aquilo que se ignora. Neste sentido, adverte Shoshana Zuboff, "a tecnologia não é apenas uma ferramenta, mas um ambiente. E ambientes não são notados, são respirados" (ZUBOFF, 2020).

Esse hábito incorporado de mediação digital faz com que grande parte da população não perceba que depende integralmente de uma complexa infraestrutura tecnológica até

mesmo para as atividades mais banais do cotidiano. A ausência de conexão à internet, por exemplo, inviabiliza operações financeiras corriqueiras como PIX, TED, pagamentos por QR Code ou o simples acesso a aplicativos bancários. A estrutura econômica diária está profundamente enraizada em sistemas digitais que operam em tempo real, de modo que qualquer interrupção imediata da rede se converte em ineficiência econômica, insegurança e exclusão financeira. Situação semelhante se verifica no campo da mobilidade: sem o suporte de sistemas de GPS, milhões de indivíduos já não conseguem se localizar, planejar rotas ou acessar endereços. A geolocalização, outrora habilidade pessoal, foi progressivamente automatizada e incorporada ao modo como os sujeitos se deslocam, trabalham e, em muitos casos, até sobrevivem.

No âmbito empresarial, a dependência também se revela crítica. A inexistência de serviços de nuvem compromete a produtividade, a gestão de dados, os registros contratuais e a comunicação organizacional. Sistemas de administração, inclusive aqueles voltados à gestão jurídica, podem entrar em colapso em questão de minutos se privados de acesso às plataformas digitais das quais dependem. De igual modo, quando os servidores públicos perdem estabilidade, o próprio Estado se vê impossibilitado de manter o controle sobre informações essenciais à vida em sociedade, como cadastros populacionais, registros civis, processos judiciais, receitas médicas e concessão de benefícios sociais. A operacionalização de políticas públicas, portanto, está hoje condicionada à manutenção contínua de sistemas informacionais.

Essa dependência manifesta-se também de maneira psicológica e social. O simples fato de que, durante apresentações acadêmicas e congressos, muitos ouvintes permanecem conectados a seus celulares ilustra a hiperconectividade como condição quase compulsória. Estar offline já não é compreendido como opção legítima, mas como sinal de exclusão ou improdutividade. Essa compulsoriedade da conexão configura uma nova forma de alienação, na qual a ausência de rede equivale à perda de pertencimento social.

Do ponto de vista jurídico, essa realidade evidencia que direitos fundamentais como o acesso à informação, à comunicação e às transações econômicas tornaram-se condicionados à estabilidade de sistemas tecnológicos controlados, em grande parte, por entes privados. A soberania estatal, por sua vez, encontra-se submetida a um novo eixo de vulnerabilidade: a soberania informacional. Trata-se da capacidade de um Estado garantir a preservação, a integridade e a continuidade de seus fluxos de dados essenciais à vida social, mesmo diante de falhas ou ataques digitais. Sem essa soberania, direitos e instituições podem ser suspensos de forma abrupta por fatores externos ao controle nacional.

Nesse sentido, a dependência digital não pode ser interpretada apenas como um efeito colateral da modernidade técnica, mas como um desafio político e jurídico. Assim como a Constituição Federal de 1988 protege a soberania territorial e a autonomia econômica, impõe-se ao Direito a tarefa de reconhecer a soberania informacional como dimensão fundamental da continuidade democrática. Sem garantias mínimas de preservação digital, a sociedade corre o risco de colapsar não apenas nos fluxos de dados, mas também em seus fundamentos institucionais e simbólicos.

5 RISCOS E REALIDADES DO COLAPSO DIGITAL: O CENÁRIO DE UM POSSÍVEL APAGÃO

A digitalização profunda da existência humana vai além de um fenômeno técnico trata-se de uma transformação civilizacional. Essa dependência tecnológica crescente acarreta um risco sistêmico: o "apagão digital", definido como uma interrupção grave e prolongada das infraestruturas tecnológicas essenciais, já não pode ser encarado como mera ficção científica. Em vez disso, tornou-se uma ameaça concreta, documentada e em expansão. Eventos como o incidente global de julho de 2024, causado por uma atualização defeituosa do software da CrowdStrike, que paralisou voos, sistemas bancários e hospitalares, fazem parte de um padrão preocupante de vulnerabilidade digital

5.1 A FALIBILIDADE DA INFRAESTRUTURA DIGITAL

Serviços essenciais como energia elétrica, saúde, comunicação, transporte, segurança pública e inclusive os próprios sistemas judiciais tornaram-se dependentes de infraestruturas digitais. Qualquer evento que comprometa, corrompa ou paralise tais estruturas pode desencadear efeitos em cadeia de difícil controle. Como destaca Evgeny Morozov (MOROZOV, 2020): *"*as utopias digitais ignoram a materialidade da infraestrutura e sua vulnerabilidade às lógicas políticas, militares e econômicas".

A resiliência tecnológica, frequentemente tratada como questão de engenharia, é também uma questão jurídica e institucional. Afinal, como responder normativamente a situações de pane generalizada? Como garantir direitos fundamentais: como identidade, acesso à justiça, memória, propriedade e liberdade quando os sistemas de proteção e registro desses direitos se tornam inacessíveis ou inexistentes?

5.2 CASOS EMBLEMÁTICOS DE COLAPSOS DIGITAIS

O que parecia, até há pouco tempo, um cenário reservado à ficção científica, hoje se concretiza em eventos documentados e recorrentes. A hiperconectividade da sociedade moderna apresentada como símbolo de progresso e eficiência tem revelado sua faceta mais sombria: a falibilidade estrutural dos sistemas digitais que sustentam a vida pública e privada. A ausência de mecanismos robustos de contingência, combinada à crescente complexidade das infraestruturas tecnológicas, tem produzido episódios de colapso que afetam, direta e indiretamente, milhões de pessoas.

Ao observar episódios históricos recentes, é possível destacar quatro casos emblemáticos ocorridos entre 2007 e 2024 que ilustram a gravidade e a multiplicidade dos riscos enfrentados: desde ataques cibernéticos motivados por tensões geopolíticas, passando por falhas técnicas em *datacenters* privados, até um colapso global causado por uma simples atualização mal sucedida de software. Cada um desses episódios evidencia não apenas a vulnerabilidade técnica dos sistemas digitais, mas também a fragilidade jurídica e institucional das respostas disponíveis. Mais do que eventos isolados, esses casos funcionam como sinais de alerta de que a dependência digital, quando não acompanhada de planejamento jurídico e ético, pode colocar em risco direitos fundamentais, serviços essenciais e a própria continuidade institucional.

Entre os episódios mais emblemáticos que evidenciam a fragilidade das infraestruturas digitais, destaca-se, em primeiro lugar, o ataque cibernético à Estônia em 2007. Reconhecida como uma das sociedades mais digitalizadas do mundo, a Estônia foi alvo, entre abril e maio daquele ano, de uma ofensiva em larga escala atribuída a grupos russos. Durante semanas, sites governamentais, bancos, universidades e veículos de imprensa sofreram ataques de negação de serviço (DDoS), paralisando comunicações oficiais e desestabilizando a infraestrutura estatal. O evento motivou a criação do Centro de Excelência em Defesa Cibernética da OTAN, em Tallinn, e marcou a inauguração da era dos conflitos digitais geopolíticos, demonstrando que até um Estado tecnologicamente avançado pode ser sitiado sem o disparo de armas físicas.

Anos depois, em novembro de 2020 e dezembro de 2021, os blackouts da Amazon Web Services (AWS) reforçaram os riscos da concentração de infraestrutura crítica em mãos privadas. As interrupções nos datacenters da empresa, provedora de serviços em nuvem para governos, instituições públicas e corporações, provocaram colapsos temporários em milhares de plataformas digitais. Hospitais, sistemas educacionais, bancos, plataformas de

comunicação corporativa e até serviços judiciais ficaram inacessíveis por horas, evidenciando a ausência de regulação que imponha planos de contingência estruturados.

Em 2021, a vulnerabilidade também atingiu diretamente o direito à saúde, quando o sistema público de saúde da Irlanda (HSE) foi paralisado por um ataque ransomware. O sequestro de dados criptografou arquivos e comprometeu o funcionamento de hospitais, laboratórios e consultórios. Centenas de cirurgias foram canceladas e profissionais precisaram recorrer ao uso de papel, revelando a fragilidade de estruturas digitais em contextos emergenciais. O episódio foi considerado um crime contra os direitos humanos, uma vez que comprometeu diretamente o acesso a cuidados médicos e colocou em risco pacientes em estado crítico.

Em 19 de julho de 2024, ocorreu um incidente de alcance global que ficou conhecido como o "apagão cibernético global". Uma atualização defeituosa do software de segurança Falcon Sensor, da empresa CrowdStrike, afetou computadores com sistema Windows em todo o mundo. O colapso derrubou, entre outros serviços, o sistema de check-in e comunicação de companhias aéreas como Delta, United e American Airlines, ocasionando o cancelamento de mais de 4.900 voos. Hospitais perderam acesso a sistemas clínicos, bancos sofreram atrasos em transações e departamentos governamentais ficaram inoperantes. O episódio demonstrou de forma contundente a vulnerabilidade da arquitetura digital planetária diante de um erro técnico isolado, reforçando a urgência de protocolos internacionais de resposta a crises digitais.

Outros setores também foram atingidos, como hospitais que perderam acesso a sistemas clínicos, serviços bancários sofreram atrasos, e departamentos governamentais ficaram inoperantes. O incidente demonstrou a vulnerabilidade da arquitetura digital planetária diante de um erro técnico isolado, reforçando a urgência de protocolos internacionais de resposta a crises digitais.

6 AS RESPOSTAS JURÍDICAS: PRESERVAÇÃO E CONTINUIDADE INFORMACIONAL

Se o risco de colapso digital é concreto e documentado, impõe-se ao Direito delinear obrigações de preservação e continuidade informacional que sejam proporcionais à ameaça. No Brasil, esse debate se apoia em três pilares: (i) a proteção e gestão de acervos públicos como dever estatal previsto na Lei de Arquivos (Lei nº 8.159/1991), que institucionaliza o CONARQ e orienta políticas de guarda e acesso; (ii) a proteção de dados pessoais sob a

LGPD e o Regulamento de Comunicação de Incidente de Segurança da ANPD (Resolução CD/ANPD nº 15/2024), que estruturam deveres de resposta e reporte de incidentes com potencial dano relevante; e (iii) a governança nacional de cibersegurança, atualmente coordenada pela Política Nacional de Cibersegurança (PNCiber) (Decreto nº 11.856/2023), que estabelece princípios de resiliência e cooperação para serviços essenciais.

6.1 O DIREITO DIANTE DA FALHA SISTÊMICA: LACUNAS E POTENCIALIDADES

O ordenamento jurídico brasileiro ainda não trata com profundidade o problema da resiliência digital como um direito fundamental correlato à proteção de dados, à cidadania e à soberania informacional. Embora a Constituição Federal de 1988 assegure, em seu artigo 5º, os direitos à informação (XIV), à privacidade (X), à inviolabilidade de dados (XII) e à ampla defesa (LV), esses preceitos tornam-se inócuos se as estruturas técnicas que os viabilizam se tornam inacessíveis ou desaparecem. [1]

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) representa um avanço importante, mas sua ênfase recai sobre o tratamento legítimo e seguro dos dados, e não sobre a preservação estrutural da informação no longo prazo, tampouco sobre protocolos em caso de perda massiva e irreversível de registros digitais. O que ocorre com o titular de dados se o banco de dados for destruído por completo? Que garantias lhe restam?

Essa lacuna demanda a construção de uma teoria jurídica da continuidade informacional, com enfoque em dois princípios fundamentais: o princípio da soberania digital (garantia de que dados sensíveis e estratégicos de uma nação estejam armazenados sob controle estatal ou supervisionado) e o princípio da redundância jurídica da informação (garantia de existência de versões alternativas, acessíveis e verificáveis dos dados essenciais à vida em sociedade).

6.2 PRESERVAÇÃO DA MEMÓRIA COMO CONDIÇÃO DE AUTORIDADE

1 Constituição da República Federativa do Brasil de 1988, Art. 5º: *"Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."*

A filosofia político-cultural evidencia que a memória coletiva é pilar da autoridade e da estabilidade do mundo comum. Hannah Arendt afirma que "a autoridade, apoiada no passado como base inabalável, conferia ao mundo a permanência e durabilidade que os mortais precisam", ressaltando que essa memória compartilhada é vital para a coesão política e institucional.

Aplicada ao contexto digital, essa reflexão sugere que delegar toda nossa memória ao etéreo sem redundância ou preservação material constitui um risco civilizacional. Arquivar documentos em suportes físicos, manter cópias offline, preservar versões impressas de acervos jurídicos, descentralizar centros de dados e promover interoperabilidade entre sistemas não são práticas obsoletas, mas mecanismos essenciais para garantir continuidade histórica, legal e social.

Giorgio Agamben oferece um contraponto conceitual relevante. Embora não utilize a expressão “o homem é o animal que arquiva”, em The Open: Man and Animal ele problematiza a distensão entre o humano e o arquivo, sugerindo que o ser humano se sustenta justamente na capacidade de representar e preservar uma operação que equilibra memória e identidade. Essa abordagem filosófica reforça que o armazenamento consciente da memória pública e institucional é condição para a preservação do mundo compartilhado.

6.3 PROPOSTAS NORMATIVAS INSTITUCIONAIS

Diante desse cenário, algumas diretrizes podem ser esboçadas como contribuições para a formulação de políticas públicas e normativas.

Em primeiro lugar, propõe-se a criação de uma Lei Nacional de Preservação da Memória Digital, que estabeleça a obrigatoriedade de cópias físicas ou backups offline para registros públicos e dados sensíveis. Tal medida busca reduzir a dependência exclusiva de sistemas digitais e garantir um nível mínimo de continuidade em caso de pane tecnológica.

Em segundo lugar, sugere-se a institucionalização de Arquivos Jurídicos Redundantes, tanto físicos quanto digitais, supervisionados por órgãos independentes. Esses arquivos funcionariam como uma espécie de “Arquivo Nacional de Emergência”, destinado a resguardar informações jurídicas e administrativas de caráter essencial.

A terceira diretriz refere-se à integração de protocolos de continuidade digital no âmbito do Sistema de Justiça, com a previsão de planos de atuação judicial off-grid. Essa medida possibilitaria que magistrados, servidores e advogados mantivessem acesso a processos e garantias fundamentais mesmo diante de um colapso informacional.

Por fim, recomenda-se o fomento a centros universitários e comunitários de guarda descentralizada de dados históricos e jurídicos, promovendo democratização do acesso e maior resiliência social. A descentralização amplia a pluralidade de suportes e reduz a vulnerabilidade diante de falhas concentradas em grandes provedores de serviços.

Contudo, é preciso reconhecer que nenhuma dessas estratégias é absolutamente imune ao risco. Mesmo backups físicos, armazenados em fitas magnéticas, servidores desconectados ou documentos impressos, estão sujeitos a incêndios, inundações, deterioração material ou negligência institucional. A história recente oferece exemplos trágicos dessa fragilidade: o incêndio no Museu Nacional do Rio de Janeiro, em 2 de setembro de 2018, destruiu cerca de 90% do acervo, composto por aproximadamente 20 milhões de itens, muitos sem qualquer cópia digital. Esse episódio ilustra de forma contundente a vulnerabilidade estrutural da preservação da memória, tanto no suporte físico quanto no digital.

Esse cenário nos conduz a uma reflexão mais profunda: o que resta quando todas as cópias desaparecem? A perda total da memória física e digital coloca em crise não apenas os sistemas de informação, mas a própria condição jurídica da sociedade. Sem arquivo, não há identidade, nem prova, nem história.

Assim, o princípio da redundância deve ser acompanhado do princípio da pluralidade de suportes e da descentralização institucional. A segurança não está apenas na cópia, mas na diversidade de cópias, armazenadas em locais distintos, sob gestões diversas e em formatos múltiplos. A responsabilidade de preservação não pode ser monopólio estatal ou privado, mas deve ser compartilhada com universidades, arquivos comunitários, bibliotecas públicas e mesmo iniciativas cidadãs.

Em última análise, como observa Paul Ricoeur, a memória não nos pertence por direito natural, ela exige cuidado contínuo, proteção institucional e compromisso ético, sob pena de desaparecer não apenas dos arquivos, mas da própria consciência histórica (RICOEUR, 2007).

7 A RUPTURA DA CONTINUIDADE INSTITUCIONAL: QUANDO A TECNOLOGIA FALHA, O ESTADO SE FRAGILIZA

A função mais elementar do Estado moderno é garantir a estabilidade da vida em sociedade: preservar identidades, assegurar direitos, manter registros, organizar instituições e responder com previsibilidade aos cidadãos. Essa estabilidade está baseada, entre outros

fundamentos, na continuidade institucional a capacidade de o Estado existir e operar independentemente de governos, conjunturas políticas ou crises momentâneas.

No entanto, em uma era hiperconectada e digitalizada, a continuidade institucional passou a depender de estruturas técnicas invisíveis, e nem sempre confiáveis. A promessa de eficiência e celeridade que motivou a digitalização dos serviços públicos não foi acompanhada por sistemas equivalentes de resiliência, redundância ou recuperação. Quando a tecnologia falha, o Estado negligencia e com ele, o próprio Direito.

Registros civis, cadastros previdenciários, bases de dados fiscais, sistemas judiciais, boletins de ocorrência, prontuários médicos, registros escolares, sistemas eleitorais: tudo, ou quase tudo, está armazenado em servidores, muitas vezes geridos por empresas terceirizadas, conectados à nuvem e altamente interdependentes.

Essa configuração faz com que a soberania estatal esteja hoje atrelada ao funcionamento ininterrupto dessas infraestruturas técnicas. Um ataque cibernético ou falha sistêmica não compromete apenas a prestação de um serviço compromete a legitimidade do Estado perante seus cidadãos, que se veem impedidos de exercer direitos básicos, como o de acessar benefícios, obter certidões ou peticionar judicialmente.

O colapso dos sistemas digitais públicos pode provocar consequências jurídicas gravíssimas. O Brasil já testemunhou, nos últimos anos, episódios concretos que colocaram em xeque a continuidade institucional do próprio Poder Judiciário. Em novembro de 2020, o Superior Tribunal de Justiça (STJ) foi alvo de um dos ataques cibernéticos mais graves já registrados contra uma instituição de Estado no país. Um ransomware invadiu os servidores da Corte, criptografando completamente o acervo processual. Todos os sistemas foram derrubados, os prazos foram suspensos e o tribunal passou a funcionar em regime de plantão emergencial por vários dias. O ataque revelou que mesmo as instituições mais altas do sistema de Justiça não estão imunes à vulnerabilidade digital.

Poucos meses depois, em abril de 2021, o Tribunal de Justiça do Rio Grande do Sul (TJRS) sofreu outro ataque cibernético que tornou seus sistemas inacessíveis, obrigando à suspensão dos prazos processuais e administrativos por tempo indeterminado.

Esses episódios suscitam questões que o Direito ainda não responde com clareza, como a preservação do direito à ampla defesa sem acesso ao processo, a forma adequada de garantir a contagem ou suspensão de prazos em sistemas comprometidos e o destino jurídico dos atos processuais realizados durante o colapso.

A resposta não pode ser apenas operacional: é preciso elaborar juridicamente o que significa o colapso da infraestrutura que sustenta a justiça. A descontinuidade digital atinge o

cerne da segurança jurídica e revela a urgência de incorporar a resiliência tecnológica como dimensão constitucional da efetividade do Direito.

8 CONCLUSÃO

Ao longo deste trabalho, ficou evidente que a tecnologia, tão celebrada como motor da modernidade, esconde uma fragilidade silenciosa, a vulnerabilidade. Essa dependência digital não se manifesta apenas em falhas técnicas, mas em crises reais: hospitais que voltam aos prontuários em papel, tribunais que perdem prazos processuais e aeroportos que cancelam voos por um simples update. O colapso digital não está no horizonte ele já acontece. E quando ocorre, revela o quanto estamos vulneráveis, frágeis, expostos.

É nesse momento crítico que o Direito encontra seu papel mais urgente: não apenas proteger dados, mas garantir que a sociedade persista mesmo quando a conexão falha. Nós já discutimos como os marcos jurídicos brasileiros, do Marco Civil da Internet à Resolução da ANPD sobre incidentes são avanços importantes. Mas não bastam. É preciso transformar deveres formais em estruturas efetivas de resiliência: planos de continuidade real, preservação segura fora da nuvem, arquivamento plural e governança comprometida com a memória institucional.

A crise digital é, antes de tudo, um desafio civilizatório. O Direito precisa se preparar para quando a infraestrutura falha, para que direitos fundamentais, processos e memórias não desapareçam junto com os bits. É hora de colocar a preservação informacional como prioridade normativa e institucional. Só assim, mesmo na escuridão tecnológica, a sociedade continuará lembrando, julgando e existindo e o Estado de Direito resistirá, imperfeito, mas presente.

No fim, a pergunta que permanece não é apenas “e se houver um colapso?”, mas o que ou quem ainda estará de pé para reconstruir?. Se a tecnologia um dia colapsar e a história sugere que isso é mais provável do que impossível, é imprescindível que o Direito esteja entre as poucas estruturas que ainda sabem lembrar, registrar e reconstruir. Preservar a memória digital é preservar a política, a Justiça, a civilização; sem ela, só restará o silêncio das máquinas.

REFERÊNCIAS

AGAMBEN, Giorgio. **Meios sem fim: notas sobre a política.** Belo Horizonte: Autêntica, 2012.

AGAMBEN, Giorgio. **O que é o contemporâneo?** Chapecó: Argos, 2009.

ARENDT, Hannah. **Entre o passado e o futuro**. São Paulo: Perspectiva, 2009.

ASSOCIAÇÃO DOS ADVOGADOS DE SÃO PAULO (AASP). **TJRS suspende prazos processuais em razão de ataque cibernético.** Disponível em: https://www.aasp.org.br/noticias/tjrs-suspende-prazos-processuais-em-razao-de-ataque-cibernetico/ Acesso em: 19 agosto 2025.

BBC NEWS BRASIL. **Falha da CrowdStrike derruba sistemas no mundo todo e cancela voos**.Disponível em: https://www.bbc.com/portuguese/articles/c51lp8vxd2no](https://www.bbc.com/portuguese/articles/c51lp8vxd2no. Acesso em: 19 agosto 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Senado Federal, 2023.
Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 agosto 2025.
BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018.

CASTELLS, Manuel. **A sociedade em rede.** 6. ed. São Paulo: Paz e Terra, 2003.

DERRIDA, Jacques. **Mal de arquivo: uma impressão freudiana.** Rio de Janeiro: Relume Dumará, 2001.

DONEDA, Danilo. **Dados pessoais, democracia e a proteção do indivíduo.** In: PEREIRA, Patrícia; SOUSA, Rafael de (orgs.). Direito Digital Contemporâneo. Brasília: IDP, 2018.

HAN, Byung-Chul. **Sociedade da transparência.** Petrópolis: Vozes, 2017.

KASPERSKY.**Ataques Cibernéticos à Estônia**. Disponível em: https://cybermap.kaspersky.com/pt. Acesso em: 19 agosto 2025.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

MOROZOV, Evgeny. **Atores sem rosto: a ascensão da tecnocracia digital**. São Paulo: Ubu, 2020.

RICOEUR, Paul. **A memória, a história, o esquecimento.** Campinas: Editora da Unicamp, 2007.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Em razão de ataque cibernético, STJ funcionará em regime de plantão até o dia 9**. Nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-

ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx . Acesso em: 19 agosto 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** Rio de Janeiro: Intrínseca, 2020.

BRASIL. Lei n.º 8.159, de 8 de janeiro de 1991. **Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.** Diário Oficial da União, Brasília, 8 jan. 1991. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 7 set. 2025.

ARENDT, Hannah. **What Is Authority? In: Between Past and Future.** New York: The Viking Press,1961.Disponívelem:https://www.pevpat-ugent.be/wp-content/uploads/2016/09/H-Arendt-what-is-authority.pdf. Acesso em: 7 set. 2025.