XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

YURI NATHAN DA COSTA LANNES

MARCELO ANTONIO THEODORO

ANA CLAUDIA SILVA SCALQUETTE

D597

Direito, governança e novas tecnologias III[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Yuri Nathan da Costa Lannes, Marcelo Antonio Theodoro, Ana Claudia Silva Scalquette – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-306-0
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. Direito. 3. Governança e novas tecnologias. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, teve como sede a cidade de São Paulo, sendo acolhido com excelência pela Universidade Presbiteriana Mackenzie. O evento reafirmou a centralidade da pesquisa jurídica no enfrentamento dos desafios contemporâneos impostos pela transformação digital, pelas inovações tecnológicas e pelas novas formas de governança e controle institucional.

O GT10 – Direito, Governança e Novas Tecnologias III, realizado no dia 26 de novembro, reuniu pesquisadoras e pesquisadores de diversas regiões do Brasil para discutir os múltiplos impactos das tecnologias emergentes sobre os direitos fundamentais, a administração pública, a proteção de dados, a sustentabilidade e a ordem democrática.

Os artigos apresentados passaram por dupla avaliação cega por pares, garantindo rigor acadêmico e excelência científica. A partir da análise dos trabalhos, foram identificados seis eixos temáticos principais, que organizam os anais de forma a evidenciar os distintos focos de abordagem e permitir ao leitor um percurso estruturado pelo conteúdo:

Proteção de Dados Pessoais, Privacidade e Identidade Digital - Este eixo reúne estudos que exploram a proteção de dados pessoais sob a ótica da privacidade, da publicidade institucional, da sustentabilidade e da construção de novas categorias jurídicas, como a identidade digital.

1 - Big Data e direitos fundamentais: uma análise interdisciplinar dos impactos na privacidade e proteção de dados pessoais no ordenamento jurídico brasileiro

2 - Dados pessoais e desenvolvimento sustentável: fundamentos e desafios do direito à privacidade no século XXI

3 - A proteção de dados pessoais dos servidores públicos do Tribunal de Justiça do Distrito Federal e dos Territórios: conflito entre publicidade e privacidade?

4 - A proteção de dados pessoais como direito difuso e a sustentabilidade no uso de dados pessoais

5 - A proteção constitucional da identidade digital: um novo paradigma dos direitos da personalidade na era da informação

6 - A norma ABNT NBR ISO/IEC 27701 como instrumento de suporte à Lei Geral de Proteção de Dados

7 - A Lei Geral de Proteção de Dados Pessoais: os serviços extrajudiciais – governança e boas práticas

Inteligência Artificial, Sistema de Justiça e Direitos Fundamentais - Debate as aplicações da inteligência artificial no Judiciário e os dilemas éticos, institucionais e regulatórios que envolvem a sua adoção em contextos democráticos e de proteção aos direitos.

8 - A inteligência artificial e o Poder Judiciário: reflexões sobre a prestação jurisdicional e a concretização da cidadania

9 - Entre algoritmos e direitos: a reconstrução do direito frente ao capitalismo de vigilância

10 - Entre o algoritmo e a consciência: impactos das decisões automatizadas no Judiciário e a urgência da educação em direitos humanos

11 - A governança da inteligência artificial e os arranjos institucionais: entre inovação tecnológica e a proteção de garantias fundamentais

12 - Regular ou não a inteligência artificial, essa é a questão principal?

13 - O uso do sistema MIDAS pelo Tribunal de Justiça do Estado do Ceará: inovação tecnológica para a concretização do princípio da duração razoável do processo

14 - Entre a liberdade de expressão e os direitos da personalidade: desafios da inteligência artificial na propaganda eleitoral à luz da condição de pessoas expostas politicamente

15 - Inteligência artificial e proteção das comunidades indígenas em contextos globais

Governança Digital e Sustentabilidade – Reúne trabalhos que tratam da relação entre governança institucional e sustentabilidade, especialmente em temas como compliance ambiental, cidades inteligentes e estratégias de desenvolvimento sustentável.

16 - Governança digital sustentável e proteção de dados em cidades inteligentes: desafios jurídicos no Antropoceno

17 - Governança corporativa e compliance ambiental: estratégias para uma gestão sustentável e eficaz

18 - A inteligência artificial como instrumento de fortalecimento do compliance ambiental

19 - A democratização da energia no Brasil: uma análise sobre o acesso e as possibilidades originadas pela energia solar

Inclusão, Acessibilidade e Justiça Digital - Trabalhos que discutem as lacunas e desigualdades digitais, especialmente em relação à acessibilidade e à implementação de tecnologias digitais no poder público.

20 - Acessibilidade negligenciada: capacitismo digital nas redes sociais do governo federal

21 - Jurimetria e o Direito brasileiro – estatística e conceitos preliminares – aplicabilidade

Infância, Direitos Digitais e Exposição Prematura - Este eixo foca nos desafios da regulação da exposição digital de crianças e adolescentes e nos caminhos jurídicos para proteção da infância no ambiente virtual.

22 - Adultização infantil no meio ambiente digital: entre lacunas regulatórias e a construção de caminhos de proteção jurídica

Plataformas Digitais, Regulação e Impactos Psicossociais - Reflete sobre os impactos sociais e econômicos das plataformas digitais, abordando questões regulatórias, manipulação de resultados e proteção do consumidor.

23 - A ascensão das plataformas de apostas digitais no Brasil: uma análise dos impactos psicossociais, da manipulação de resultados e dos desafios regulatórios

Os trabalhos reunidos neste volume demonstram o vigor da produção acadêmica brasileira em torno dos desafios impostos pelas tecnologias emergentes e reafirmam o papel do Direito como campo estratégico para a mediação entre inovação e proteção de garantias fundamentais. A todos os(as) pesquisadores(as), coordenadores(as) e avaliadores(as), registramos nossos agradecimentos por suas valiosas contribuições.

Desejamos uma leitura instigante e transformadora!

Ana Claudia Silva Scalquette - Universidade Presbiteriana Mackenzie

Marcelo Antonio Theodoro- Universidade Federal de Mato Grosso

Yuri Nathan da Costa Lannes – Faculdade de Direito de Franca

BIG DATA E DIREITOS FUNDAMENTAIS: UMA ANÁLISE INTERDISCIPLINAR DOS IMPACTOS NA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

BIG DATA AND FUNDAMENTAL RIGHTS: AN INTERDISCIPLINARY EXAMINATION OF IMPACTS ON PRIVACY AND PERSONAL DATA PROTECTION WITHIN THE BRAZILIAN LEGAL FRAMEWORK

Diego Belchior Ferreira Santana [1]

Resumo

Este estudo apresenta uma análise interdisciplinar do fenômeno Big Data e suas implicações jurídicas no contexto da privacidade e proteção de dados pessoais. Através de metodologia qualitativa, o trabalho examina as origens do termo Big Data, emergido na década de 1990, caracterizado pelos cinco elementos fundamentais: volume, variedade, velocidade, veracidade e valor. A pesquisa demonstra que, apesar das inúmeras aplicações benéficas em setores como aviação, agricultura, saúde e administração pública, o Big Data introduz riscos substanciais à segurança cibernética e à privacidade individual. O estudo passa pela evolução do conceito jurídico de privacidade, que transcendeu a definição clássica de "direito a ser deixado só" para incorporar o controle sobre informações pessoais no ambiente digital. A análise destaca a Lei Geral de Proteção de Dados (LGPD) como marco regulatório fundamental no ordenamento jurídico brasileiro. Conclui-se que a compatibilização entre avanços tecnológicos do Big Data e a proteção de direitos fundamentais demanda interpretação progressiva da legislação em busca de equilibrar desenvolvimento econômico com dignidade humana.

Palavras-chave: Big data, Segurança, Privacidade, Hiperconectividade, Proteção de dados

Abstract/Resumen/Résumé

This study presents an interdisciplinary analysis of the Big Data phenomenon and its legal implications in the context of privacy and personal data protection. Through a qualitative methodology, the research examines the origins of the term Big Data, which emerged in the 1990s, characterized by five fundamental elements: volume, variety, velocity, veracity, and value. The study demonstrates that, despite the numerous beneficial applications in sectors such as aviation, agriculture, healthcare, and public administration, Big Data introduces substantial risks to cybersecurity and individual privacy. The research traces the evolution of the legal concept of privacy, which has transcended the classical definition of "the right to be left alone" to incorporate control over personal information in the digital environment. The analysis highlights the General Data Protection Law as a fundamental regulatory milestone in the Brazilian legal framework. It concludes that reconciling the technological advances of

[1] Mestrando em Direito na UNIVEM - Centro Universitário Eurípedes de Marília

Big Data with the protection of fundamental rights requires a progressive interpretation of legislation to balance economic development with human dignity.

Keywords/Palabras-claves/Mots-clés: Big data, Security, Privacy, Hyperconnectivity, Data protection

1. Introdução

Quase todos os dados atualmente disponíveis foram criados na última década e, atualmente, são gerados quintilhões de bytes por dia (GOMES, p. 7). Esses quintilhões de dados decorrem do cenário de hiperconectividade, impulsionado pela massiva quantidade de dispositivos móveis e popularização de computadores. Para que seja possível compreender a magnitude disso, devemos deixar claro que um quintilhão de bytes (um exabyte-EB) corresponde a um bilhão de gigabytes (GB).

É nesse pano de fundo se desenvolve o fenômeno do Big Data. Segundo o dicionário Michaelis, fenômeno "é fato ou evento que pode ser objeto da ciência, que pode ser descrito e explicado do ponto de vista científico"[1]. Portanto, o Big Data pode ser apreendido de modo científico e devidamente explicado.

Apesar da hiperconectividade ser observável e dialogada pelo senso comum mais recentemente, o termo Big Data já era empregado na década de 1990, quando não conhecíamos os smartphones. E desde lá, o Biga Data vem crescendo exponencialmente, de modo que suas manifestações não são restritas à ciência da computação.

Os negócios, a indústria, a agricultura, a saúde, as administrações privadas e públicas foram e são impactadas pelo Big Data. Está claro a todas as luzes a massiva captura e geração de dados a partir de múltiplas fontes de informações atualmente disponíveis. Fossem apenas esses os campos de exploração do Big Data, a importância da compreensão do termo e de suas implicações já seria por demais relevante. Acontece que em todos os campos de estudos e ciências, há lugar para aplicação do Big Data.

Como o desenvolvimento do Big Data veio no mesmo passo da maior disponibilidade de informações, houve a ressignificação da privacidade. Se antes o termo nos remetia ao ambiente de trabalho ou residencial, hoje, a privacidade também se refere aos dados obtidos através de informações em ambiente virtual. É por isso que há movimentos organizados da sociedade em defesa da privacidade de dados, haja vista que a hiperconectividade potencializou a expansão do fenômeno em estudo.

No presente estudo, através de uma metodologia qualitativa e interdisciplinar, buscou-se trazer as origens do termo Big Data, seus elementos, impactos na privacidade, na segurança e nos direitos à privacidade e à proteção de dados pessoais. Serão abordados alguns exemplos de aplicação do Big Data bem como analisados os aspectos críticos do fenômeno, explicitando a reação e o desenvolvimento da legislação no que se refere à privacidade de dados.

2. Big Data:

2.1 Origens do Termo:

Segundo Francis X. Diebold[2], a criação do termo Big Data não pode ser reputada à ciência da computação. Diebold afirma que sua origem seria nebulosa, envolvendo a indústria e a academia, especificamente nas áreas da computação e da estatística.

Em meados de 1990, o termo em análise foi utilizado pelo então cientista chefe da Silicon Graphics (SGI), empresa americana fabricante de estações de trabalho de alto desempenho, supercomputadores e softwares gráficos avançados, com sede em Mountain View, Califórnia[3].

---

[1] https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=fen%C3%B4meno

[2] Professor de Economia, Finanças, Estatística e Data Science da Universidade da Pensilvânia.

[3] O primeiro protótipo da estação de trabalho do computador da SGI foi doado em 1984 para George Lucas , o criador da série de filmes *Star Wars* . A partir deste pequeno passo, a SGI emergiu como o fornecedor de

Em março de 1996, novembro de 1997 e fevereiro de 1998, a Silicon Graphics utilizou o termo Big Data em seus anúncios publicados em revistas, como a Black Enterprise[4] (DIEBOLD, 2012).

No âmbito acadêmico, em 2003 foi publicado na Cambridge University Press o artigo '*Big Data' Dynamic Factor Models for Macroeconomic Measurement and Forecasting*, de Francis X. Diebold, cuja submissão ocorreu no ano de 2000. O próprio autor indica que criou o termo para conjurar uma "imagem mais nítida" da explosão de dados e abertamente contrastar com os métodos anteriores (DIEBOLD, 2012).

Há também autores que atribuem a origem do termo a Laney, que publicou em 2001 uma nota de pesquisa no qual destacou no conceito de Big Data a importância do Volume, Variedade e Velocidade (os três "Vs"), indo além do foco de Dielbold no Volume (PERWEJ, 2017). Dielbold, por sua vez, defende que utilizou o termo antes de Laney (DIEBOLD, 2012).

2.2 Conceitos fundamentais:

Antes de imergir no conceito propriamente dito, é relevante afirmar que Big Data merece tanto destaque pela capacidade descritiva. Sim, é da essência do Big Data a capacidade de descrever dados que excedem a capacidade de processamento dos sistemas de banco de dados convencionais (ALMEIDA, SANTOS, p. 199).

Isso porque o volume de informações, a variedade delas e a velocidade com que são produzidos simplesmente inviabilizam que se possa retirar alguma conclusão deles sem método de captura, pré-processamento e uso de ferramentas auxiliares (ALMEIDA, SANTOS, 2014). Sem o Big Data, é como se estivessem ocultos.

A definição clássica sustenta que o Big Data envolve três características fundamentais sem as quais não se pode considerar existir Big Data. São elas o volume, a variedade e a velocidade. Posteriormente, acrescentaram-se mais dois elementos: a veracidade e o valor (GOMES, p. 21-22).

A depender do contexto, outros dados são acrescentados, como valência, validade, variabilidade e volatilidade (PERWEJ, 2017), mas não interessam ao propósito do presente artigo

Tendo em vista a natureza elementar, não é possível compreender o todo sem explicar o que cada elemento significa.

A começar pelo Volume, é ser essencial apar o Biga Data haver imensas quantidades de dados gerados para se falar. Considere que a cada segundo são criados diversos posts em redes sociais, acompanhado de fotos, áudios e vídeos, e incontáveis mensagens são trocadas por e-mails e aplicativos. Por outro lado, são gerados outros tantos dados de

computadores favorito de Hollywood. HALL, Mark. " SGI ." Encyclopedia Britannica , 05 de setembro de 2025, https://www.britannica.com/money/SGI. Acessado em 05 de setembro de 2025.

[4] Empresa multimídia americana, cujo site pode ser acessado em https://www.blackenterprise.com, focada em publicações para empreendedores negros, empresas de propriedade de negros e conteúdo sobre carreira, tecnologia e finanças para pessoas negras, existente desde a década de 1970.

sensores de máquinas industriais. Ao serem contabilizados, não teremos terabytes, mas zetabytes ou, futuramente, brontobytes[5] (PERWEJ, 2017).

No contexto do Big Data, a Velocidade se refere tanto à rapidez com que são gerados os dados como à capacidade de reuni-los em curto lapso temporal. A Variedade, por sua vez, se relaciona com os diversos tipos de formatos e de dados que precisam ser suportados por soluções de Big Data. São planilhas, vídeos, dispositivos de monitoramento, PDFs, e-mails, fotos, áudios (PERWEJ, 2017).

O elemento veracidade tem relação com a atividade de classificá-los como válidos ou inválidos e de eliminar ruídos. Ruído deve ser entendido, de forma simplificada, como dados confusos que não geram informações relevantes cujo armazenamento deve ser evitado (CHANGQING, WENMING, 2012).

A relevância do Big Data tem estreita relação com a capacidade de gerar conclusões que tenham valor. E para ter valor, depende-se da veracidade. Uma vez que o dado é fidedigno, ele possui mais valor. Mas não para por aí. O valor depende da velocidade de duração do processamento dos dados. Ao perder contemporaneidade, perde-se o valor. Por outro lado, o resultado analítico tem prazo de validade, ante as rápidas mudanças das circunstâncias (CHANGQING, WENMING, 2012).

Em síntese, Big Data pode ser assim definido:

> Big Data is a collection of data whose content cannot be captured, stored, processed, and analyzed with conventional software tools within a certain time frame. The core of big data processing is the storage and processing of massive data, and the greater the amount of data, the faster the processing speed[6]. (HUANG et al, p. 1115, 2025)

2.3 Exemplos de aplicação do Big Data

A literatura especializada enumera diversas aplicações dos sistemas de processamento de Big Data. Relacionado ao campo da aviação, por exemplo, foi projetado um sistema para melhorar a eficiência com base em satélites científicos (HUANG et al, p. 1116, 2025). O mesmo autor cita a ampla utilização do Big Data na pesquisa científica, previsão do tempo, e-commerce e vários campos industriais (HUANG et al, p. 1116, 2025).

Acrescente-se a aplicação na gestão otimizada de infraestruturas com foco na mobilidade urbana, gerenciamento e planejamento na evacuação em emergências, de modo a direcionar fluxos de multidões para as zonas mais convenientes e seguras (MARTINO et al., 2025, p. 42).

Na agricultura, o Big Data possibilita práticas de precisão (GOMES, p. 10), racionalizando a utilização de insumos e reduzindo impactos ambientais, em busca de sustentabilidade.

---

[5] Um terabyte (TB) é uma unidade de medida de armazenamento digital que equivale a cerca de 1.000 gigabytes (GB). Um zettabyte (ZB) é uma unidade de medida de informação digital que representa 1 trilhão de gigabytes. Um brontobyte é uma unidade astronômica de armazenamento digital, superando terabytes e petabytes. Representa 1 quatrilhão de gigabytes. Embora não seja viável na prática com a tecnologia atual, o conceito de brontobyte destaca a crescente demanda por soluções de armazenamento robustas em nosso mundo impulsionado por dados (https://www.lenovo.com/us/en/glossary/brontobyte/?orgRef=https%253A%252F%252Fwww.google.com%252F&srsltid=AfmBOoqVb7AP-xw6pf_TAg1z5KwkJFCNKMiAUMuovmJ3ypbW17vdCdAQ).

[6] Tradução livre: Big Data é uma coleção de dados cujo conteúdo não pode ser capturado, armazenado, processado e analisado com ferramentas de software convencionais dentro de um tempo razoável. O núcleo do processamento de big data é o armazenamento e processamento de dados massivos, e quanto maior a quantidade de dados, mais rápida a velocidade de processamento.

MUNHOZ, PERIN, RIBEIRO (p. 30, 2024) enumeram diversos estudos que envolvem a aplicação do Big Data nos mais variados campos, como sistemas de justiça, práticas educacionais, modelos de saúde, programas de assistência social, segurança pública, administração pública, infraestrutura e governança ambiental.

Entretanto, é preciso ter em mente que, em virtude do quantitativo de dados em massa obtidos e agregados de diferentes fontes, sequer é possível determinar a gama completa de usos reais e potenciais do Big Data (LYON, p. 12, 2014).

2.4 Os riscos do Big Data

A expansão do Big Data vem acompanhada de riscos inerentes. À medida que crescem o volume e variedade de dados, inúmeras são as preocupações quanto à segurança e à privacidade dos dados. Os múltiplos formatos, fluxos, fontes e infraestruturas de dados representam vulnerabilidades de segurança próprias do Big Data (PERWEJ, 2017).

O volume de dados digitais e a capacidade de analisá-los, apesar de criarem oportunidades, já citadas, fazem emergir ameaças, exigindo atenção e atuação responsiva dos setores privado e público (LIMA et al, 2023).

Por essa razão, medidas de segurança e privacidade são essenciais e não podem ser ignoradas. Isso porque as falhas de segurança tem o potencial de reduzir o próprio valor das análises e resultar em responsabilização pelo eventual vazamento de informações confidenciais.

Examinemos primeiramente o conceito de privacidade no contexto do Big Data para depois expor sobre segurança. Segundo PERWEJ, 2017, p. 19, "a privacidade da informação é o privilégio de ter o controle sobre como as informações específicas são coletadas e usadas"[7]. Garantir a privacidade significa impedir que informações se tornem familiares a terceiros quando assim não for desejado.

Existem métodos convencionais para preservação da privacidade em Big Data. A Desidentificação, por exemplo, é:

> "uma técnica convencional para mineração de dados com preservação da privacidade, onde, para proteger a privacidade pessoal, os dados devem ser primeiro descontaminados por meio de generalização e supressão antes de serem disponibilizados para mineração de dados. A desidentificação é uma ferramenta vital na proteção da privacidade e pode ser um caminho para a análise de big data com preservação da privacidade" (PERWEJ, 2017, p. 19)[8].

Há ainda o K-Anonimado, que consiste em inviabilizar que, durante a liberação de dados, as informações de cada pessoa contidas nos dados não possam ser percebidas por pelo menos k-1 indivíduos (PERWEJ, 2017).

A L-Diversidade é uma forma de anonimização baseada em grupo, que busca garantir a privacidade através da redução na representação dos dados em quantitativo suficiente para resultar em alguma perda de viabilidade de algoritmos de gerenciamento ou mineração de dados (PERWEJ, 2017). Há outros métodos de anonimização, mas fogem do escopo proposto no presente artigo.

---

[7] No original: The information privacy is the privilege to have some rein over how the particular information is collected and used.

[8] Tradução livre do seguinte trecho: De-identification is a conventional technique for privacy-preserving data mining, where in order to intercede personal privacy, [26] data should be first decontaminate with generalization and suppression before the deliverance for data mining. De-identification is a vital tool in privacy protection, and can be wayfaring to privacy preserving big data analytics.

Passemos agora a conceituar Segurança no contexto do Big Data. A partir da publicação dos dez desafios de segurança da organização Cloud Security Alliance (CSA) em 2014, é possível afirmar que segurança consiste nos exercícios de defesa de informações e ativos de informação por meio do uso de tecnologia, processos e treinamento contra acesso não autorizado, interrupção, modificação, inspeção, divulgação, gravação e destruição.

Como facilmente se conclui, a Privacidade dos dados caminha na esteira da Segurança, sendo decorrente da eficácia desta. Para que se possa assegurar o valor dos dados e gerir os riscos da coleta, armazenamento, uso e compartilhamento de dados, há a necessidade de uma Política de Governança bem definida, de maneira a exercer a autoridade e o controle sobre a gestão dos dados (FILGUEIRAS et al, 2025):

> Governança de dados é um tópico central frente às inovações digitais contemporâneas, mas deve estar apoiada em valores que justificam as arquiteturas institucionais. Nesse caso, o valor público da privacidade dos cidadãos é fundamental para justificar a governança de dados. Privacidade é um conceito normativamente dependente, significando o direito à reserva de informações pessoais como um direito fundamental de liberdade. (FILGUEIRAS et al, p. 10, 2025)

A Governança de Dados não se confunde com a Proteção de Dados. A Proteção se refere:

> a um conjunto extensivo de procedimentos e estratégias para garantir que dados pessoais sejam acessados e utilizados de maneira adequada para atingir os objetivos incutidos em regras de privacidade e proteção, ao mesmo tempo que possibilite o desenvolvimento econômico e tecnológico. (FILGUEIRAS et al, p. 10, 2025)

Nesse contexto, é importante destacar que a Lei Geral de Proteção de Dados (LGPD) é instrumental tanto relação à Proteção de Dados, como se pode inferir pela designação que recebe, mas também o é em relação à Governança. Isso porque, a LGPD estabeleceu uma arquitetura institucional com as figuras do controlador e do encarregado de dados, bem como da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (FILGUEIRAS et al, 2025).

As preocupações com a Governança merecem destaque sobretudo porque o Big Data intensificou a Vigilância. No presente contexto, Vigilância deve ser compreendida como a obtenção sistemática, periódica e detalhada de dados com finalidade específica (LYON, 2014).

O Big Data reorientou a Vigilância para alguns focos. Novos softwares permitiram a automação da vigilância, viabilizou as análises preditivas, com a promessa de abordagem preventiva e adaptou métodos do marketing para a segurança nacional no que se refere à busca por padrões de comportamentos (LYON, 2014).

Convém relembrar que em 2013 Snowden revelou que a Agência de Segurança Nacional (NSA) dos EUA coletou e armazenou incontáveis dados interceptados indistintamente, a pretexto de combate ao terrorismo após os ataques de 11 de setembro de 2001(FAVERA, SILVA, 2016). O fato é tido como o maior caso de vigilância cibernética da história do governo americano:

> Um dos vários programas implementados pela *NSA*, denominado PRISM, permitia à Agência coletar dados diretamente dos serviços das empresas e provedores de *Internet AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo!* e *YouTube*. Outros programas, como BLARNEY, FAIRVIEW, OAKSTAR e STORMBREW, possibilitavam que a *NSA* interceptasse cabos de fibra óptica de sistemas de

> telecomunicações e computadores, a fim de coletar informações e dados daqueles que se utilizassem desses recursos (FAVERA, SILVA, 2016, p. 111)

O caso Snowden expôs programas de vigilância que alcançaram bilhões de comunicações, demonstrando a vulnerabilidade da intimidade no ambiente digital. O escândalo apontou que, sob o pretexto de combate ao terrorismo, a agência americana de espionagem coletou dados massivos, que ficaram à disposição de diversos colaboradores que sequer tinham posição de comando na instituição, o que possibilitou o vazamento de parte dos dados como forma de demonstrar o risco inerente à atividade (SZINVELSKI, ARCENO e FRANCISCO, p. 136).

A grande discussão que surgiu com as revelações de Edward Snowden provocou a academia a debater as interseções entre a Vigilância social estatal e o Big Data, indicando-o como catalizador da exponencial apreensão não consentida de dados:

> "Agora, os dados em massa são obtidos e agregados de diferentes fontes antes de determinar a gama completa de seus usos reais e potenciais e mobilizar algoritmos e análises não apenas para entender uma sequência passada de eventos, mas também para prever e intervir antes que comportamentos, eventos e processos sejam desencadeados." (LYON, 2017, p. 4)

Sobre o panorama científico relativo ao tema das violações de dados governamentais, Hamid e Huda (2025), a partir da análise de 107 artigos publicados entre 2006 e 2023, realizaram um mapeamento na base de dados Scopus. No período, foi constatado que houve o crescimento anual de 10,84% e, a partir de 2016, as publicações sobre o tema avançaram significativamente, coincidindo com o aumento de 300% de ciberataques entre os anos de 2015 e 2016 (HAMID; HUDA, 2025).

Destacaram também que entre 2020 e 2023, o foco da pesquisa científica apontou para a política governamental e sua responsabilidade na segurança de dados (HAMID; HUDA, 2025). Além disso, incluiu a computação em nuvem como um desafio da cibersegurança.

As quatro principais categorias de violações destacadas por Hamid e Huda (2025) são:

HACK:	"hackeado por terceiros ou infectado por malware" (HAMID; HUDA, 2025, p.2).
ELET:	"dispositivo portátil perdido, jogado fora ou roubado ou computador estacionário perdido" (HAMID; HUDA, 2025, p.2).
DISC:	"divulgação não intencional, por exemplo, informações sensíveis postadas publicamente ou mal manuseadas ou enviadas à parte errada" (HAMID; HUDA, 2025, p.2).
INSD:	"má conduta interna por funcionários, contratados ou clientes". (HAMID; HUDA, 2025, p.2)[9]

Considerando que crescente quantidade de ataques de Ransomware, tem-se que ele é um dos principais desafios em relação aos riscos de segurança aqui contextualizados. Trata-

[9] Tabela elaborada a partir da tradução da seguinte passagem do artigo citado: “Data breaches involve the unauthorised use of personal information for fraudulent activities, including accessing government benefits and other services (Burnes et al., 2020). They are categorised into four types: HACK (hacked by a third party or infected by malware), ELET (lost, thrown away, or stolen portable device or lost stationary computer), DISC (unintended disclosure, for example, sensitive information posted on public or mishandled or sent to the wrong party), and INSD (insider misconduct by employees, contractors, or customers)”.

se de malware (ou software malicioso) capaz de criptografar arquivos em um dispositivo, tornando esses arquivos e os sistemas que os utilizam inúteis. Após isso acontecer, exigem-se valores como resgate para que seja restaurado o acesso aos dados (CEN et al., 2024).

3. Do direito à Privacidade e à Proteção de dados pessoais:

Como foi observado até agora, a expansão do Big Data veio acompanhado do risco à Privacidade e de exigências de Segurança. No contexto do Big Data "a privacidade da informação é o privilégio de ter o controle sobre como as informações específicas são coletadas e usadas" (PERWEJ, 2017, p. 19). Esse conceito é diferente do conceito jurídico porque ele está voltado para o controle das informações dentro das soluções de Big Data e não ao direito à privacidade individualmente considerado.

Questão tormentosa é definir o direito à privacidade. Apesar da maior facilidade de observar fenômenos que configurem violação desse direito fundamental, a tentativa de conceituá-lo encontra dificuldades nos limites da linguagem. Parece que algum elemento sempre escapa das tentativas de enquadramento.

Ao tratar da concepção tradicional do direito à privacidade MIRANDA, 2013, p. 222 enumera que as doutrinas alemã, italiana e americana o tratam sobre diferentes ângulos. A doutrina alemã observa o direito à privacidade por três esferas. A esfera do segredo, que envolve a proteção contra a publicidade de fatos ou notícias que devem ser ignorados. A da intimidade, relativa à vida pessoal e familiar. A esfera da individualidade, que se refere à honra, imagem, nome.

Ainda segundo o mesmo autor, a doutrina italiana concebe a privacidade sob quatro fases da modalidade de isolamento. A *soledad* corresponde ao isolamento físico. A *intimidad* se relaciona com o isolamento em pequeno grupo de pessoas com relações especiais (família). *Anonimato* se refere à possibilidade de, apesar do contato com diversas pessoas, manter a liberdade de identifica-se ou não. E a quarta fase, denominada *reserva,* diz com a barreira psicológica contra intromissões não consentidas.

Pela perspectiva da violação do direito à privacidade, a doutrina americana trata de quatro tipos de ilícitos: (i) intromissão em assuntos privados, (ii) divulgação de fatos embaraçosos privados, (iii) revelação à opinião pública de fatos que expressem falsa imagem e (iv) a apropriação indevida, em proveito próprio, de nome ou imagem de outrem.

Para MIRANDA, 213, p. 240, o direito à privacidade "pode ser entendido como a faculdade/garantia do indivíduo encontrar na solidão aquela paz e aquele equilíbrio demasiadamente comprometidos pelo ritmo da vida moderna".

Entretanto, essas perspectivas não dialogam com a massiva coleta de dados proporcionada pelo Big Data. Elas não tangenciam a apropriação de informações no âmbito digital e a repercussão na intimidade. A insuficiência do conceito jurídico tradicional de privacidade é destacada por VIEGA, 2024, p. 5, que, citando Stefano Rodotà, refere:

> "parece cada vez mais frágil a definição de 'privacidade' como 'o direito a ser deixado só', que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito."

Com o atual estágio de circulação de informações e dados no meio virtual, o direito à privacidade tem de levar em conta as relações que se desenvolvem no ambiente digital (VIEGA, 2024). Nesse sentido, "identifica-se, assim, essa nova função da privacidade e a tendência de ampliação de suas funções" (VIEGA, 2024, p. 6).

Portanto, o direito à privacidade deve considerar a exposição virtual e, além do direito de ser deixado só, compreende o direito de controlar as informações que produz durante a navegação solitária nas redes sociais virtuais e no acesso de serviços eletrônicos.

A função jurídica do direito à privacidade de possibilitar o controle das próprias informações que nos dizem respeito é realmente desafiador. Com efeito, se para as grandes corporações empresariais há enormes riscos de violações quando operacionalizam as soluções de Big Data, o que se pode esperar em termos de riscos em relação à população sem letramento digital. A propósito, pode-se definir que o Letramento Digital se refere "não só a competências imediatas e mensuráveis do que se sabe fazer nos ambientes digitais (dimensão técnica), mas também do localizar, questionar e criar (dimensão cognitiva e crítica)" (LIMA NETO; CARVALHO, p. 9, 2022).

Agora que ficou limitada a acepção de direito à privacidade, parte-se para o conceito do direito da proteção de dados pessoais. Antes, é preciso preliminarmente compreender o que são dados pessoais.

Segundo TAMER, 2025, dados não se confundem totalmente com informações. Os dados são os elementos a partir dos quais se deduz uma informação. A partir da interpretação dos dados se alcança a informação.

Já o dado *pessoal* é a aquele com o potencial de se obter uma informação sobre uma pessoa. Para que o dado seja *pessoal*, ele precisa permitir obter uma informação *pessoal*. Sem isso ele é apenas um dado e foge do escopo do direito fundamental à proteção de dados pessoais. Em suma, dado pessoal é:

> "algo que se faz conhecer uma pessoa por identificá-la, como o nome da pessoa física, o número do seu RG ou outro documento. Ou algo que possa levar à identificação de uma pessoa (identificável – capaz de identificar uma pessoa), por exemplo, a data de nascimento, o endereço, a geolocalização; ou mesmo a soma de informações (TEIXEIRA, 2024, p. 108)".

Os dados pessoais podem ser classificados em dados pessoais diretos e indiretos (TEIXEIRA, 2024). Os primeiros permitem a identificação imediata da pessoa natural. Os indiretos tornam a pessoa identificável, havendo a possibilidade de dedução da identificação da pessoa.

Necessário se faz enfatizar que pessoa jurídica não é titular do direito à proteção de dados em virtude da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) ter expressamente as afastado de sua tutela (art. 5º).

Portanto, não se pode tratar dado pessoal como sinônimo de informação. Todavia, é necessário destacar que as publicações na área da computação não enfatizam essa distinção, tratando os dois termos como sinônimos.

Pontuado isso, parte-se para a definição do direito à proteção de dados pessoais, direito fundamental cristalizado na Constituição no art. 5º, inciso LXXIX, TAMER, 2025, p. 11, esclarece que:

> "(...) proteger os dados que identificam o indivíduo ou possam implicar a identificação de informações a seu respeito é direito em si mesmo, mas também parte necessária da proteção de algo maior, que é justamente a privacidade e o livre desenvolvimento de sua personalidade".

A Emenda Constitucional n. 115/2022 foi o marco formal para a proteção de dados ao incluir o inciso LXXIX no artigo 5º, da CF/88 e estabelecer ser assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

O direito à proteção de dados pessoais, dessa forma, passou ser formalmente fundamental em 2022, embora o STF já tenha sinalizado isso em 2020.

Em abril de 2020, a Min. Rosa Weber deferiu a Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387 contra a Medida Provisória nº 954/2020, a qual determinava que os serviços de telecomunicações compartilhassem dados pessoais dos usuários com o IBGE sob a justificativa de possibilizar a realização de pesquisas remotamente durante a pandemia do COVID. Na decisão a Ministra sustentou a necessidade de "assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações." [10].

Logo, a Emenda Constitucional n. 115/2022 apenas explicitou a proteção de dados enquanto direito fundamental, sepultando a discussão de que ele seria mera expressão do direito à privacidade. Assim, embora a proteção de dados já compunha o bloco de constitucionalidade, foi relevante a aprovação da Emenda Constitucional como forma de endossar a importância do tema na sociedade da informação.

Ademais, a constitucionalização da proteção de dados endossa a necessidade da implementação do Letramento Digital enquanto política pública a ser desenvolvida para garantir a cidadania, prevenir ilícitos civis e criminais, bem como desnudar os riscos digitais à convivência comunitária, à exposição infantil, aos direitos humanos e à própria democracia.

Considerando que em âmbito internacional se busca a uniformização legislativa para o combate ao crime cibernético (SIEBER, 1998), não seria salutar que cada ente federativo legislasse arbitrariamente sobre a proteção de dados.

Bem por isso, o inciso XXX, do art. 22, da Constituição Federal, dispõe que compete privativamente à União legislar sobre proteção e tratamento de dados pessoais.

A importância dessa disposição, também incluída pela Emenda Constitucional n. 115/2022, tem reflexo prático imediato:

> Em curto espaço de tempo de vigência da Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), já houve iniciativas legislativas locais. É o caso, por exemplo, da Lei Estadual de São Paulo n. 17.301/2020, que proibiu as farmácias paulistas de exigir, no ato da compra, o número do CPF dos consumidores sem informações claras sobre o tratamento desse dado pessoal. (TEIXEIRA, 2024, p. 76).

Portanto, a Emenda Constitucional, em bom momento, apascentou os legislativos regionais e locais, fincando a União como responsável por traçar os marcos normativos no que se refere à proteção de dados.

O direito da proteção de dados pessoais, portanto, tem suas balizas estabelecidas pelo processo legislativo federal, o que reafirma ser imprescindível regramento uniforme em todo território nacional. Afinal, tanto as ameaças como a coleta de dados podem ser remotas. Logo, a diversidade de disposições de Estados e de Municípios poderia representar um conjunto de disposições caóticas e, no limite, conflitantes.

Na Ação Declaratória de Constitucionalidade (ADC) n. 51, o STF enfrentou o tema da constitucionalidade do Decreto nº 3.810/2001 (Acordo de Assistência Judiciária em

---

[10] A decisão liminar da ADI em referência também é reconhecida como marco por SARLET, Ingo W.; SARLET, Gabrielle B S.; BITTAR, Eduardo C B. Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital, p. 11. Rio de Janeiro: Saraiva Jur, 2022. E-book. p.11. ISBN 9786555599527. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555599527/. Acesso em: 08 mai. 2025.

Matéria Penal - MLAT entre Brasil e EUA), do art. 237, II do Código de Processo Civil, e dos arts. 780 e 783 do Código de Processo Penal, que tratam de cooperação jurídica internacional (cartas rogatórias) para obtenção de dados e comunicações eletrônicas controladas por empresas de tecnologia sediadas no exterior. Buscava-se que apenas esses mecanismos fossem utilizados para tal fim.

Contudo, o STF validou a possibilidade de solicitação de dados feitas também de forma direta, com fundamento nas hipóteses do art. 11 da Lei nº 12.965/2014 (Marco Civil da Internet)[11] e do art. 18 da Convenção de Budapeste[12], considerando a necessidade de agilidade na persecução de ilícitos digitais.

Neste mesmo julgamento o STF determinou a comunicação da decisão aos Poderes Legislativo e Executivo para que adotem providências para o aperfeiçoamento do quadro legislativo, a discussão e aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal).

Este caso ilustra como a velocidade de produção das informações que alimentam o Big Data impõe que o Estado também busque meios ágeis para obter as evidências necessárias para coibir ilícitos. Por outro lado, expõe que o referencial normativo da Lei Geral de Proteção de Dados necessita de aprimoramentos para a temática penal, de maneira a tutelar eficientemente o direito fundamental subjacente.

Em outro julgamento, na Ação Direta de Inconstitucionalidade nº 5.545, o Pleno do STF consignou que direito à privacidade, na dimensão de uma prestação positiva por parte do Estado, impõe a necessidade de medidas proteção de dados da esfera privada dos indivíduos para evitar acessos não autorizados a essas informações. Tal assertiva exemplifica o entrelaçamento entre os direitos fundamentais à privacidade e à proteção de dados pessoais. E, para além desse aspecto, também enfatiza a necessidade de atividades

---

[11] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

[12] Artigo 18 - Ordem de exibição

1. Cada Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a autoridades competentes para ordenar:

a. a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador;

b. a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor.

2. Os poderes e procedimentos referidos neste artigo estão sujeitos aos Artigos 14 e 15.

3. Paras os fins deste Artigo, o termo "informações cadastrais do assinante" indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:

a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço;

b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço.

c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.

administrativas prestacionais do estado que possam efetivamente tutelar a privacidade por meio da proteção dos dados pessoais.

Os riscos inerentes do Big Data à Segurança e à Privacidade são expressão do que Ulrich Beck alertou: as ciências e a tecnologia *"já não são vistas como um manancial de soluções para os problemas, mas ao mesmo tempo também como manancial de causas de problemas"* (BECK, p. 236).

Como um desses problemas, os crimes cibernéticos são uma realidade cristalizada. Segundo estudo contratado pelo Conselho da Europa e realizado pela Universidade de Wusburg, em 1998, os crimes informáticos datam de pelo menos 1960. No início eram restritos às sabotagens, espionagem e fraudes. Atualmente, os ataques aos sistemas de informações são sofisticados, planejados e eficazes (SIEBER, 1998). E quando grandes empresas e instituições públicas são alvo de subtração de dados, o prejuízo é compartilhado entre toda a sociedade.

O referido estudo auxiliou a União Europeia a promulgar, em 2001, a Convenção de Budapeste, que trata sobre crimes cibernéticos e procurou reforçar o uso legítimo das tecnologias da informação ao criar compromissos internacionais de combate aos mencionados crimes. A necessidade subjacente é a proteção da confidencialidade, da integridade e da disponibilidade de sistemas informáticos, redes e dados de computador.

Como se percebe, as palavras-chave sobre a política de cibersegurança são confidencialidade, integridade e disponibilidade dos sistemas informáticos (CID), de maneira que se algum desses pilares forem violados a segurança falhou (STINGHEN, 2025).

Nesse contexto, a cibersegurança, como subconjunto da segurança da informação (ADMASS, MUNAYE e DIRO, 2024), merece cuidado redobrado dos agentes que operacionalizam soluções de Big Data.

A dimensão da problemática da cibersegurança é tamanha que no ano de 2017 o prejuízo dos crimes informáticos no Brasil foi de 22,5 bilhões de dólares. Com tal cifra, o Brasil só teve menos prejuízos econômicos com a prática dos ilícitos cibernéticos que a China (MESSIAS et al, 2023).

É preciso atentar que a invasão de privacidade no mundo digital vai além da mera coleta de dados, estendendo-se a práticas como o *spamming*, na qual aplicativos coletam informações específicas do sistema e do usuário e as enviam de forma independente, através de uma rede, sem o conhecimento do usuário (SIEBER, 1998).

Dada a extensão internacional do tema, além da Convenção de Budapeste (primeiro tratado internacional sobre crimes informáticos) entrará em vigor a, provavelmente em 2026, a Convenção da ONU sobre Cibercrime.

Ela foi aprovada na Assembleia Geral da ONU dezembro de 2024, mas seu texto ainda não está formalmente publicado e ainda não foi assinada oficialmente por nenhum país. A cerimônia formal de abertura para assinaturas está prevista para ocorrer em 25 de outubro de 2025, em Hanói, no Vietnã. Após, os países poderão assinar e ratificar o Tratado, cuja obrigatoriedade ocorrerá 90 dias após a ratificação pelo 40º país signatário, por isso se afirma que provavelmente a sua vigência ocorrerá apenas em 2026 (UNODC, 2024).

Sobre Política de Segurança da Informação (PSI), não pode deixar de ser mencionado a norma padrão ABNT NBR ISO/IEC 27001, a qual "é composta por 114 controles recomendados de segurança", com a finalidade de "prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da

informação (STINGHEN, 2025, p. 247). Observar essa norma padrão, portanto, é uma solução estratégica para mitigar os riscos das soluções de Big Data.

A propósito, os operadores das referidas soluções, por lidarem com bancos de dados, devem obediência à Lei Geral de Proteção de Dados, que é imperativa aos que realizam o tratamento de dados pessoais nos meios digitais (art. 1º da Lei nº 13.709/2018 - LGPD).

Também é importante destacar o conceito jurídico de banco de dados, que é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (art. 5°, inciso IV, da LGPD).

Por sua vez, tratamento de dados pessoais é conceituado pela Lei Geral de Proteção de Dados (art. 5°, X) como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Portanto, a compatibilização entre o avanço do Big Data e direitos fundamentais à privacidade e à proteção de dados pessoais depende não apenas da efetivação da LGPD, mas da sua interpretação progressiva e abertura para futuras reformas legislativas, sob as lentes dos instrumentos internacionais, dada a ausência de fronteiras no ciberespaço (SZINVELSKI, ARCENO e FRANCISCO, p. 137).

O STF enfatizou a necessidade do Poder Legislativo se debruçar sobre LGPD na área Penal e o Letramento Digital é estratégia de proteção de dados que vai além do papel regulamentador do Estado. É o que se vislumbra para assegurar que a proteção de dados acompanhe a velocidade da inovação tecnológica sem comprometer a dignidade da pessoa humana quando injustamente exposta.

4. Conclusão

Foi possível identificar que o Big Data representa uma oportunidade seguida de grandiosos desafios, talvez na mesma proporção dos volumes de dados que suas soluções são capazes de processar.

De um lado, a fonte de inovação, riqueza e avanços sociais cria soluções para o setor público e privado, gerando comodidades e análises precisas que antes não se cogitava. Porém, expõe a pessoa a riscos de vigilância e perda da privacidade através da violação de dados pessoais.

O Direito não pode ignorar a centralidade dessa tecnologia. Cabe-lhe atuar estabelecendo barreiras contra abusos sem sufocar a inovação, buscando o justo equilíbrio.

No contexto brasileiro, a Emenda Constitucional nº 115, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) buscam acompanhar as transformações tecnológicas, cabendo aos operadores jurídicos buscar rápidas adaptações frente às constantes novidades e à velocidade como se criam e destroem dados.

Por outro aspecto, no âmbito internacional a Convenção de Budapeste (que já é vigente em 81 países) e a Convenção da ONU sobre Crimes Cibernéticos (que alcançará número significativamente maior de partes assim que entrar em vigor nos próximos meses) representam a teia de proteção dos dados no ciberespaço.

Assim, ao ser realizado o enquadramento jurídico das soluções do Big Data, observa-se que elas operam banco de dados e realizam tratamento de dados, atraindo a incidência da LGPD. O grande desafio é compatibilizar o desenvolvimento econômico e tecnológico dessas soluções com a tutela dos direitos à privacidade e à proteção dos dados pessoas

pessoa, garantindo que os benefícios dessa tecnologia não se convertam em violações dos direitos fundamentais. Nessa tarefa, os empreendimentos legislativos devem ser acompanhados de medidas de Letramento Digital da sociedade na era da informação.

Referências

ALMEIDA, Fernando; SANTOS, Mário. 2014. "A Conceptual Framework for Big Data Analysis. In Organizational, Legal, and Technological Dimensions of Information System Administration", ed. Irene Maria Portela, Fernando Almeida, 199-223. ISBN: 9781466645264. USA: IGI Global.

BECK, Ulrich. A sociedade do risco: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

C. Ji, Y. Li, W. Qiu, U. Awada and K. Li, "Big Data Processing in Cloud Computing Environments," 2012 12th International Symposium on Pervasive Systems, Algorithms and Networks, San Marcos, TX, USA, 2012, pp. 17-23, doi: 10.1109/I-SPAN.2012.9. Disponível em: https://ieeexplore.ieee.org/document/6428800. Acesso em: 06 de setembro de 2025.

CEN, Mingcan et al. Ransomware early detection: A survey. Computer Networks, v. 239, p. 110138, 2024. Disponível em: ScienceDirect. Acesso em 03 de setembro de 2025.

CLOUD SECURITY ALLIANCE (CSA). Expanded Top Ten Big Data Security and Privacy Challenges, 2013. Disponível em: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf. Acesso em 06 de setembro de 2025.

DIEBOLD, Francis X. On the Origin(s) and Development of the Term "Big Data". Philadelphia: Penn Institute for Economic Research, Department of Economics, University of Pennsylvania, 2012. Disponível em: http://ssrn.com/abstract=2152421. Acesso em: 15 mai. 2024.

DIEBOLD, Francis X. "Big Data" Dynamic Factor Models for Macroeconomic Measurement and Forecasting: A Discussion of the Papers by Lucrezia Reichlin and by Mark W. Watson. In: DEWATRIPONT, Mathias et al. (eds.). Advances in Economics and Econometrics: Volume 3: Theory and Applications, Eighth World Congress. Cambridge: Cambridge University Press, 2003, p. 115-122.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 19 abril. 2024.

FAVERA, Rafaela Bolson Dalla; SILVA, Rosane Leal da. CIBERSEGURANÇA NA UNIÃO EUROPEIA E NO MERCOSUL: BIG DATA E SURVEILLANCE VERSUS PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET. Revista de Direito, Governança e Novas Tecnologias, Curitiba, v. 2, n. 2, p. 112-134, jul./dez. 2016. e-ISSN: 2526-0049.

FILGUEIRAS, Fernando; LUI, Lizandro; VELOSO, Maria Tereza Trindade. A Gramática Institucional da Proteção de Dados e da Privacidade no Brasil. Dados, Rio de Janeiro, v. 68, n. 1, p. 346, 2025. DOI: https://doi.org/10.1590/dados.2025.68.1.346.

GOMES, Rodrigo Dias de Pinho. Big data: desafios à tutela da pessoa humana na sociedade da informação. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2017.
HALL, Mark. " SGI ." Encyclopedia Britannica , 5 de setembro de 2025, https://www.britannica.com/money/SGI. Acessado em 5 de setembro de 2025.
HAMID, Supardi; HUDA, Mohammad Nurul. Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. Social Sciences & Humanities Open, v. 11, p. 101234, 2025. Disponível em: https://doi.org/10.1016/j.ssaho.2024.101234. Acesso em: 15 mai. 2024.
HUANG, Siqi et al. Design and implementation of big data processing system based on Hadoop. Procedia Computer Science, [s.l.], v. 259, p. 1115-1122, 2025. DOI: 10.1016/j.procs.2025.04.065. Disponível em: https://www.sciencedirect.com. Acesso em: 03 de agosto de 2025.
LIMA, José Vinícus V., ALENCAR, Fernanda, RODRIGUES, Cleyton e SANTOS, Wylliams. 2023. "Transformação digital no setor público: resultados preliminares de um estudo terciário," In Anais estendidos do XIX simpósio brasileiro de sistemas de informação. Porto Alegre: Sociedade Brasileira de Computação. https://doi.org/10.5753/sbsi_estendido.2023.229395.
LIMA NETO, N. V.; CARVALHO, A. B. DE .. Letramento digital: breve revisão bibliográfica do limiar entre conceitos e concepções de professoras e de professores. Texto Livre, v. 15, p. e40207, 2022.
LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, London, v. 1, n. 2, p. 1-13, jul./dez. 2014. DOI: 10.1177/2053951714541861. Disponível em: https://bds.sagepub.com. Acesso em: 03 de setembro de 2025.
MARTINO, G. et al. Risk Management in Transportation Systems: How Big Data Can Help Predict Behaviors and Events. In: INTERNATIONAL CONFERENCE ON AMBIENT SYSTEMS, NETWORKS AND TECHNOLOGIES (ANT), 16., 2025, Patras, Greece. Procedia Computer Science. [S. l.]: Elsevier B.V., 2025. v. 257, p. 39-46.
MESSIAS, Gabriel Soares; PEQUENO JUNIOR, José Eronides de Sousa. Análise jurimétrica comparada da legislação acerca de cibercrime do Brasil e Estados Unidos. Revista Vertentes do Direito, v. 10, n. 2, p. 70-92, 2023. DOI: https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92.
MIRANDA, Jorge. Direitos Fundamentais - 1ª Edição 2013. Rio de Janeiro: Atlas, 2013. E-book. p.222. ISBN 9788522481095. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788522481095/. Acesso em: 07 mai. 2025.
MUNHOZ, Sara R.; PERIN, Vanessa Parreira; RIBEIRO, Magda dos Santos. Big Data: modos de fazer, comparar e governar. MANA, v. 30, n. 2, p. e2024014, 2024. DOI: https://doi.org/10.1590/1678-49442024v30n2e2024014.pt
PERWEJ, Yusuf. An Experiential Study of the Big Data. International Transaction of Electrical and Computer Engineers System. Vol. 4, No. 1, 2017, pp 14-25. https://pubs.sciepub.com/iteces/4/1/3
STINGHEN, João Rodrigo de Morais et al. Cartórios, compliance e transformação digital. 1. ed. Indaiatuba, SP: Foco, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 06 maio 2025.

SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. Perspectivas em Ciência da Informação, v.24, n.4, p.132-144, out./dez. 2019.
TAMER, Maurício. Manual de Direito da Proteção de Dados Pessoais - 1ª Edição 2025. Rio de Janeiro: SRV, 2024. E-book. p.18. ISBN 9786553629905. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553629905/. Acesso em: 20 abr. 2025.
TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico - 8ª Edição 2024. 8. ed. Rio de Janeiro: Saraiva Jur, 2024. E-book. p.XXVIII. ISBN 9788553622344. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788553622344/. Acesso em: 20 abr. 2025.
TEIXEIRA, Tarcisio; STINGHEN, João R.; LIMA, Adrianne Correia de; et al. LGPD Nos Cartórios: Implementação e Questões Práticas - 1ª Edição 2021. Rio de Janeiro: Saraiva Jur, 2021. E-book. p.99. ISBN 9786555597967. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786555597967/. Acesso em: 20 abr. 2025.
UNODC – UNITED NATIONS OFFICE ON DRUGS AND CRIME. United Nations Convention against Cybercrime – Home. [S. l.: s. n.], [s. d.]. Disponível em: https://www-unodc-org.translate.goog/unodc/en/cybercrime/convention/home.html?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc. Acesso em: 26 set. 2025.
VIEGA, João Ricardo Bet. Privacidade e proteção de dados pessoais: autonomia dos direitos e desdobramento no Brasil. Revista de Direito Civil Contemporâneo, vol. 40, ano 11, p. 57-88, jul./set.2024.