RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

Da conformidade formal à proteção efetiva: privacidade desde a concepção, gestão de terceiros e o desacoplamento entre norma e prática na proteção de dados pessoais

From formal compliance to effective protection: privacy by design, third-party management and the decoupling between law and practice in personal data protection

De la conformidad formal a la protección efectiva: privacidad desde el diseño, gestión de terceros y el desacoplamiento entre norma y práctica en la protección de datos personales

Cassiano Rodolfo Jung
Mestrando em Cybersecurity pela American Global Tech University (AGTU). Especialista em Inteligência e Investigação em Fontes Abertas (OSINT) pela WB Educação. Especialista em Computação Forense e Segurança da Informação pelo Instituto de Pós-Graduação e Graduação (IPOG). Especialista em Gestão Estratégica da Tecnologia da Informação pela Universidade Estácio de Sá. Tecnólogo em Segurança da Informação pela Universidade do Vale do Rio dos Sinos (UNISINOS).

RESUMO
A multiplicação de leis de proteção de dados pessoais, como a Lei Geral de Proteção de Dados Pessoais no Brasil e o Regulamento Geral sobre a Proteção de Dados na União Europeia, não foi acompanhada de redução proporcional dos incidentes que expõem informações de clientes, pacientes e consumidores. Este artigo investiga a distância entre a conformidade formal, expressa em políticas, registros e contratos, e a proteção efetiva dos dados no ambiente tecnológico das organizações. A pesquisa, de abordagem qualitativa e caráter exploratório e descritivo, combina revisão narrativa da literatura jurídica, organizacional e de engenharia de privacidade com análise documental de legislação, normas técnicas, relatórios setoriais, depoimentos oficiais e decisões de autoridades de proteção de dados do Brasil, da União Europeia e dos Estados Unidos. A análise indica que a conformidade tende a se desacoplar da prática quando é tratada como produção de documentos, e que as falhas mais recorrentes nos casos examinados envolvem controles técnicos básicos, desconhecimento dos próprios fluxos de dados e supervisão insuficiente de terceiros. As decisões sancionadoras mais recentes passaram a examinar a arquitetura dos sistemas, e não apenas a existência de documentos. Conclui-se que a proteção efetiva depende da tradução das obrigações legais em requisitos de engenharia, inventários atualizados e controles verificáveis ao longo da cadeia de fornecimento.
Palavras-chave: Proteção de dados pessoais. Conformidade regulatória. Privacidade desde a concepção. Gestão de riscos de terceiros. LGPD.

ABSTRACT
The proliferation of personal data protection laws, such as Brazil's General Data Protection Law and the European Union's General Data Protection Regulation, has not been matched by a proportional reduction in incidents that expose the information of customers, patients and consumers. This article examines the gap between formal compliance, expressed in policies, records and contracts, and the effective protection of data within organizations' technological environments. The study follows a qualitative, exploratory and descriptive approach, combining a narrative review of legal, organizational and privacy engineering literature with documentary analysis of legislation, technical standards, industry reports, official testimony and decisions issued by data protection authorities in Brazil, the European Union and the United States. The analysis indicates that compliance tends to decouple from practice when it is treated as the production of documents, and that the most recurrent failures in the cases examined involve basic technical controls, limited knowledge of the organization's own data flows and insufficient oversight of third parties. Recent enforcement decisions have begun to scrutinize system architecture rather than merely the existence of documents. The study concludes that effective protection depends on translating legal obligations into

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

engineering requirements, up-to-date inventories and verifiable controls across the supply chain.
Keywords: Personal data protection. Regulatory compliance. Privacy by design. Third-party risk management. LGPD.

1 INTRODUÇÃO

A última década consolidou um ciclo de expansão normativa em matéria de proteção de dados pessoais. O Regulamento Geral sobre a Proteção de Dados da União Europeia passou a ser aplicado em maio de 2018 e serviu de referência para diversas legislações nacionais, entre elas a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais brasileira (União Europeia, 2016; Brasil, 2018; Doneda, 2019). A lei brasileira passou a exigir, entre outras medidas, a indicação de encarregado pelo tratamento de dados pessoais, a manutenção de registro das operações de tratamento e a adoção de medidas de segurança desde a concepção dos produtos e serviços (Brasil, 2018). Essa expansão de obrigações, contudo, não foi acompanhada de redução proporcional dos incidentes. O relatório da Verizon publicado em 2025 analisou 12.195 violações de dados confirmadas, e o estudo realizado pelo Ponemon Institute para a IBM estimou o custo médio global de uma violação em US$ 4,88 milhões em 2024 (Verizon, 2025; IBM, 2024).

A coexistência entre mais regulação e exposição persistente sugere que a conformidade formal e a proteção efetiva nem sempre caminham juntas. Waldman (2020) sustenta que as leis de privacidade correm o risco de falhar quando símbolos de conformidade, como treinamentos protocolares, auditorias e registros documentais, passam a ser tratados como se fossem a própria proteção prometida pela lei. A literatura organizacional descreve fenômeno semelhante há décadas, ao mostrar que organizações podem adotar estruturas formais para obter legitimidade perante o ambiente institucional, sem que essas estruturas alterem de fato suas atividades centrais (Meyer; Rowan, 1977). A questão que orienta este trabalho é saber de que modo essa distância se manifesta na proteção de dados pessoais e quais fatores contribuem para reduzi-la.

O objetivo deste artigo é analisar os mecanismos pelos quais a conformidade com as leis de proteção de dados pode se dissociar da proteção efetiva das informações e identificar, a partir da literatura, de normas técnicas e de casos documentados, as condições que favorecem a convergência entre ambas. O texto percorre os fundamentos teóricos do desacoplamento entre norma e prática, o princípio da privacidade desde a concepção e sua tradução em engenharia, o papel do inventário de dados, a segurança técnica como requisito legal, a gestão de terceiros e, por fim, o que as decisões de autoridades reguladoras revelam sobre o modo como a conformidade passou a ser avaliada. Atenção especial é dada aos setores de saúde e financeiro, que tratam dados de saúde, classificados pela LGPD como dados pessoais sensíveis, e dados financeiros, ambos objeto de regulação setorial específica

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

(Brasil, 2018).

2 METODOLOGIA

Trata-se de pesquisa de abordagem qualitativa, com objetivos exploratórios e descritivos. Na classificação proposta por Gil (2008), a pesquisa exploratória busca proporcionar visão geral e maior familiaridade com um fenômeno ainda pouco sistematizado, enquanto a descritiva se ocupa da caracterização de fenômenos e do estabelecimento de relações entre variáveis. O tema exige essa combinação, pois a distância entre conformidade e proteção efetiva envolve dimensões jurídicas, organizacionais e técnicas, e não se identificou, na literatura consultada, indicador padronizado que permita sua mensuração direta. A opção metodológica, portanto, privilegia a interpretação articulada de fontes de diferentes naturezas.

O procedimento bibliográfico assumiu a forma de revisão narrativa, modalidade que, segundo Rother (2007), se presta à discussão do estado da arte de um tema sob perspectiva teórica ou contextual, sem a exigência de protocolos sistemáticos de busca e seleção. Foram reunidos três conjuntos de literatura. O primeiro abrange estudos jurídicos e sociojurídicos sobre a aplicação das leis de privacidade nas organizações, como os de Bamberger e Mulligan (2011), Edelman (2016) e Waldman (2020). O segundo reúne contribuições da teoria organizacional sobre conformidade simbólica e auditoria. O terceiro compreende trabalhos de engenharia de privacidade, como os de Spiekermann e Cranor (2009) e Hoepman (2014). As obras foram identificadas por meio do Google Acadêmico, dos portais das editoras e de repositórios institucionais.

A análise documental contemplou a legislação brasileira e europeia de proteção de dados, resoluções da Autoridade Nacional de Proteção de Dados e do Conselho Monetário Nacional, publicações técnicas do National Institute of Standards and Technology, normas da International Organization for Standardization, diretrizes do Comitê Europeu para a Proteção de Dados e da Agência da União Europeia para a Cibersegurança e a proposta de atualização da regra de segurança da legislação norte-americana de saúde. Também foram examinados relatórios setoriais publicados por IBM e Verizon, um alerta conjunto de agências norte-americanas, um relatório do Government Accountability Office, um depoimento prestado ao Senado dos Estados Unidos e decisões sancionadoras da autoridade irlandesa de proteção de dados, do Office of the Comptroller of the Currency e da ANPD, complementados por reportagens jornalísticas utilizadas apenas para dados factuais específicos.

O material foi organizado em seis eixos analíticos, a saber, os fundamentos do desacoplamento entre norma e prática, a privacidade desde a concepção, o inventário e a minimização de dados, a segurança técnica como condição da conformidade, a gestão de terceiros e a fiscalização. Em cada eixo, os

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

requisitos normativos foram confrontados com evidências empíricas e com casos concretos, de modo a identificar convergências e lacunas. A principal limitação do estudo decorre do uso de casos públicos, que tendem a representar incidentes de grande escala e, por isso, não refletem necessariamente a realidade de organizações de menor porte. Os dados de relatórios setoriais, produzidos com amostras e métodos próprios, são tratados como indicativos de tendência.

3 CONFORMIDADE SIMBÓLICA E O DESACOPLAMENTO ENTRE NORMA E PRÁTICA

O ponto de partida teórico para compreender a distância entre conformidade e proteção encontra-se na sociologia das organizações. Meyer e Rowan (1977) argumentaram que as organizações incorporam estruturas formais, como cargos, programas e procedimentos, em grande medida porque essas estruturas são socialmente reconhecidas como racionais e legítimas, e não necessariamente porque aumentam sua eficiência. Quando as exigências formais entram em conflito com a atividade cotidiana, as organizações tendem a manter as estruturas como fachada e a desacoplá-las das práticas efetivas. O conceito de desacoplamento oferece uma chave de leitura útil para a proteção de dados, campo no qual a adoção de políticas e a nomeação de responsáveis podem coexistir com práticas técnicas pouco alteradas.

Edelman (2016), ao estudar a aplicação das leis antidiscriminatórias nos Estados Unidos, desenvolveu o conceito de endogeneidade jurídica para descrever o processo pelo qual as organizações criam estruturas simbólicas de conformidade e, com o tempo, essas estruturas passam a ser aceitas pelos próprios tribunais como prova de cumprimento da lei. O significado da norma, nesse processo, é progressivamente moldado pelas organizações que ela pretendia regular. A contribuição é relevante porque desloca a análise da simples pergunta sobre se a lei é cumprida para a investigação de como as organizações definem, na prática, o que significa cumpri-la, e de quem participa dessa definição.

Waldman (2020) transpôs esse referencial para o campo da privacidade. Com base em entrevistas com engenheiros, profissionais de privacidade e executivos de empresas fornecedoras de soluções de conformidade, além da análise de demonstrações de produtos e de literatura setorial, o autor sustenta que as leis de privacidade correm o risco de falhar porque símbolos de conformidade, como treinamentos sem efeito prático, auditorias e trilhas documentais, passam a ser confundidos com a adesão real à lei. Em obra posterior, Waldman (2021) aprofundou a análise do modo como as rotinas internas das empresas de tecnologia influenciam a interpretação das obrigações de privacidade. O problema apontado pelo autor, portanto, não está na existência de documentos, mas na possibilidade de que eles sejam tomados como substitutos da proteção real.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

A literatura não é unânime quanto ao alcance desse diagnóstico. Bamberger e Mulligan (2011), em estudo baseado em entrevistas com diretores de privacidade apontados por seus pares como referências do setor, identificaram que parte das empresas norte-americanas havia deslocado o foco de uma abordagem centrada em procedimentos, como aviso e consentimento, para uma preocupação substantiva com a prevenção de violações às expectativas de privacidade dos consumidores. Entre os fatores associados a essa mudança, os autores apontam a atuação da Federal Trade Commission, a pressão de mercado e da imprensa, a profissionalização da área e as leis estaduais de notificação de incidentes, que elevaram o custo da má gestão das informações pessoais.

A teoria da auditoria acrescenta outra camada ao problema. Power (1997) descreveu a expansão das práticas de verificação nas sociedades contemporâneas e observou que a auditoria tende a avaliar a existência de sistemas de controle, e não necessariamente o desempenho substantivo das atividades que esses sistemas deveriam controlar. Aplicado à proteção de dados, esse diagnóstico ajuda a explicar por que uma organização pode obter avaliações favoráveis quanto à existência de políticas e registros e, ainda assim, manter falhas técnicas exploráveis. Em conjunto, os autores discutidos nesta seção indicam que a efetividade da conformidade depende menos da quantidade de documentos produzidos e mais da capacidade de esses documentos alterarem decisões técnicas e operacionais.

4 PRIVACIDADE DESDE A CONCEPÇÃO: DO PRINCÍPIO JURÍDICO À ENGENHARIA

A ideia de que a proteção de dados deve ser incorporada aos sistemas desde a sua concepção, e não acrescentada ao final, foi sistematizada por Cavoukian (2009) em sete princípios fundamentais, entre eles a atuação proativa e preventiva, a privacidade como configuração padrão, a incorporação da privacidade ao projeto, a funcionalidade plena, a segurança de ponta a ponta durante todo o ciclo de vida da informação, a visibilidade e transparência e o respeito à privacidade do usuário. A conversão desses princípios em requisitos concretos de sistema, porém, não decorre automaticamente de sua enunciação. O relatório elaborado para a agência europeia de cibersegurança por Danezis *et al.* (2014) propôs justamente a reduzir a distância entre o quadro jurídico e as medidas técnicas disponíveis, o que indica que essa tradução constitui problema próprio, que exige método.

O Regulamento Geral sobre a Proteção de Dados converteu o princípio em obrigação jurídica no artigo 25, que exige do responsável pelo tratamento a adoção de medidas técnicas e organizativas adequadas tanto no momento da definição dos meios de tratamento quanto durante o próprio tratamento, além de garantir que, por padrão, apenas os dados necessários a cada finalidade sejam tratados (União Europeia, 2016). A legislação brasileira seguiu orientação semelhante. O artigo 46 da LGPD impõe aos agentes de tratamento a adoção de medidas de segurança, técnicas e

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

administrativas aptas a proteger os dados pessoais, e seu parágrafo 2º determina que essas medidas sejam observadas desde a fase de concepção do produto ou do serviço até a sua execução (Brasil, 2018).

As diretrizes do Comitê Europeu para a Proteção de Dados sobre o artigo 25 procuraram reduzir a distância entre o texto legal e sua aplicação. O documento esclarece que a obrigação se dirige à efetividade das medidas, e não à sua mera existência, e que o responsável deve ser capaz de demonstrar que as salvaguardas adotadas produzem os efeitos pretendidos em relação a cada princípio de proteção de dados (EDPB, 2020). Essa ênfase na efetividade aproxima a obrigação jurídica das preocupações da engenharia e afasta a leitura segundo a qual a conformidade com o artigo 25 poderia ser alcançada apenas com a elaboração de políticas ou de cláusulas contratuais.

A literatura de engenharia de privacidade oferece instrumentos para essa tradução. Spiekermann e Cranor (2009) distinguiram duas abordagens de projeto, uma baseada em políticas, que depende de aviso, escolha e cumprimento de regras pelo próprio responsável, e outra baseada na arquitetura, que procura reduzir a identificabilidade dos dados e limitar sua coleta, tornando a proteção menos dependente do comportamento das organizações. Hoepman (2014) propôs oito estratégias de projeto que permitem aplicar a privacidade desde as etapas iniciais do desenvolvimento, a saber, minimizar, ocultar, separar, agregar, informar, controlar, impor e demonstrar. As estratégias traduzem objetivos de proteção em escolhas concretas de projeto, como a coleta apenas dos dados necessários ou a separação de bases para dificultar o cruzamento de informações.

O mesmo relatório de Danezis *et al.* (2014) examinou o estado da arte das tecnologias de reforço da privacidade e registrou que, embora essas tecnologias tenham demonstrado seu potencial em pesquisas e projetos piloto, elas ainda não haviam se tornado componente padrão e amplamente utilizado no projeto de sistemas, com exceção da criptografia, e propôs um método para relacionar as obrigações legais às estratégias de projeto. No plano das normas técnicas, a ISO/IEC 27701, cuja edição de 2025 passou a ser publicada como norma independente para sistemas de gestão da informação de privacidade, e o Privacy Framework do NIST oferecem estruturas que permitem converter as obrigações legais em controles organizacionais e técnicos passíveis de verificação (ISO, 2025; NIST, 2020).

5 CONHECER OS DADOS PARA PROTEGÊ-LOS: INVENTÁRIO, MINIMIZAÇÃO E DADOS NÃO GERENCIADOS

Nenhum controle pode ser aplicado a dados cuja existência a organização desconhece. Por essa razão, as leis de proteção de dados atribuem papel central ao registro das operações de tratamento. O artigo

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

37 da LGPD determina que controlador e operador mantenham registro das operações que realizarem, e o artigo 30 do regulamento europeu estabelece obrigação equivalente, com o detalhamento das finalidades, das categorias de titulares e de dados, dos destinatários e, sempre que possível, dos prazos previstos para eliminação e das medidas de segurança adotadas (Brasil, 2018; União Europeia, 2016). O registro, nessa perspectiva, não é apenas uma exigência documental, mas o ponto de partida para a avaliação de riscos e para a definição de controles.

O Privacy Framework do NIST confere a esse inventário uma dimensão operacional. A função identificar do modelo inclui o inventário e o mapeamento dos sistemas, produtos e serviços que tratam dados, dos proprietários ou operadores desses sistemas, das categorias de indivíduos cujos dados são tratados e das ações de tratamento realizadas em cada etapa do ciclo de vida da informação (NIST, 2020). Esse mapeamento orienta as demais funções do modelo, como governar, controlar, comunicar e proteger, e explicita a dependência entre conhecer os fluxos de dados e ser capaz de gerenciar os riscos que eles produzem. Um inventário desatualizado, portanto, compromete todas as decisões que dele dependem.

Os dados empíricos mostram que essa dependência tem consequências concretas. O estudo da IBM de 2024 registrou que 35% das violações analisadas envolveram dados não gerenciados, também chamados de dados de sombra, isto é, informações armazenadas fora dos ambientes controlados e inventariados pela organização (IBM, 2024). Segundo o mesmo relatório, as violações que envolveram esse tipo de dado tiveram custo médio 16% superior e exigiram mais tempo para serem identificadas e contidas, e cerca de 40% das violações envolveram dados distribuídos por múltiplos ambientes, como nuvens públicas, nuvens privadas e infraestrutura local. A fragmentação dos ambientes tende a ampliar a probabilidade de que cópias de dados escapem ao inventário formal.

A minimização é a contrapartida do inventário. O artigo 6º da LGPD estabelece o princípio da necessidade, que limita o tratamento ao mínimo indispensável para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos (Brasil, 2018). Do ponto de vista da segurança, a minimização reduz a superfície de exposição, pois dados que não foram coletados ou que já foram eliminados não podem ser subtraídos em um incidente. A estratégia de minimizar, a primeira entre as propostas por Hoepman (2014), parte exatamente desse raciocínio. O regulamento europeu explicita o alcance dessa obrigação ao determinar, no número 2 do artigo 25, que a proteção por padrão se aplica à quantidade de dados recolhidos, à extensão do tratamento, ao prazo de conservação e à acessibilidade dos dados (União Europeia, 2016).

Na doutrina brasileira, Bioni (2019) examina a função e os limites do consentimento como instrumento de proteção, considerando a assimetria entre titulares e organizações, e discute a necessidade de mecanismos que não dependam exclusivamente da escolha individual do titular.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

Doneda (2019), ao reconstituir a formação da LGPD, defende o reconhecimento da proteção de dados pessoais como direito fundamental e examina a centralidade dos princípios no modelo de regulação adotado pela lei. Lidas em conjunto com a literatura técnica, essas contribuições reforçam que o inventário e a minimização são deveres materiais dos agentes de tratamento, e não formalidades acessórias.

6 A SEGURANÇA TÉCNICA COMO CONDIÇÃO DA CONFORMIDADE

A LGPD não trata a segurança da informação como tema separado da proteção de dados. Além do dever geral previsto no artigo 46, o artigo 44 considera irregular o tratamento que deixar de fornecer a segurança que o titular dele pode esperar, consideradas circunstâncias como o modo pelo qual é realizado, o resultado e os riscos razoavelmente esperados e as técnicas disponíveis à época, e o parágrafo único do mesmo artigo atribui responsabilidade pelos danos decorrentes da violação da segurança dos dados ao controlador ou ao operador que, ao deixar de adotar as medidas previstas no artigo 46, der causa ao dano (Brasil, 2018). A conformidade, nesse desenho legal, inclui necessariamente a qualidade dos controles técnicos efetivamente implementados.

O caso da Equifax, empresa norte-americana de informações de crédito, ilustra como falhas em controles de segurança podem produzir exposição em larga escala. Segundo o relatório do Government Accountability Office sobre o incidente de 2017, os invasores tiveram acesso, pela internet, a um portal de contestações de consumidores e alcançaram dados pessoais de pelo menos 145,5 milhões de pessoas (United States, 2018). A investigação conduzida pela própria empresa, relatada no documento, atribuiu o incidente a falhas em quatro áreas, a identificação de vulnerabilidades, a detecção da intrusão, a segmentação do acesso às bases de dados e a governança de dados. Trata-se de áreas cobertas por controles de segurança amplamente descritos na literatura técnica, o que situa o problema mais na aplicação desses controles do que na indisponibilidade de soluções.

No setor de saúde, o ataque à Change Healthcare, empresa de processamento de transações de saúde controlada pelo UnitedHealth Group, oferece outro exemplo dessa dinâmica. Em depoimento ao Comitê de Finanças do Senado norte-americano, em 1º de maio de 2024, o presidente-executivo do grupo afirmou que os criminosos acessaram um portal da empresa que não estava protegido por autenticação multifator, extraíram dados e implantaram *ransomware* em 21 de fevereiro daquele ano, e confirmou o pagamento de resgate de US$ 22 milhões (Witty, 2024). Em janeiro de 2025, a empresa estimou em cerca de 190 milhões o número de pessoas afetadas (Fierce Healthcare, 2025).

A regra de segurança da Health Insurance Portability and Accountability Act distingue especificações

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

de implementação obrigatórias e especificações classificadas como endereçáveis. Segundo o próprio Departamento de Saúde e Serviços Humanos, nenhuma delas era opcional, mas a designação permitia que cada entidade avaliasse se a medida era razoável e apropriada em seu ambiente, com o objetivo de conferir maior flexibilidade (United States, 2025). Em janeiro de 2025, o departamento publicou proposta de atualização dessa regra, motivada, segundo seu preâmbulo, entre outros fatores, pelo forte crescimento das violações de dados de saúde comunicadas entre 2018 e 2023. A proposta elimina essa distinção, torna exigíveis a criptografia dos dados de saúde em repouso e em trânsito e a autenticação multifator, e passa a exigir inventário escrito dos ativos tecnológicos e mapa da rede (United States, 2025).

A mesma proposta prevê a obrigação de restaurar sistemas e dados críticos em até 72 horas após uma perda, de realizar auditoria de conformidade ao menos a cada doze meses e de obter, com a mesma periodicidade, verificação escrita de que os parceiros de negócios implementaram as salvaguardas técnicas exigidas (United States, 2025). No caso da criptografia, o próprio texto da proposta explica que a mudança dispensaria as entidades de avaliar se a medida é razoável e apropriada, o que exprime a substituição de avaliações caso a caso por requisitos verificáveis. O exemplo é relevante para o debate brasileiro, pois indica que, mesmo em um sistema regulatório consolidado, o regulador passou a considerar necessário especificar expressamente controles básicos, em vez de confiar apenas em obrigações gerais de segurança sujeitas à avaliação de cada entidade.

7 TERCEIROS E CADEIA DE FORNECIMENTO COMO VETOR DE EXPOSIÇÃO

A crescente dependência de fornecedores de tecnologia desloca parte relevante do risco para fora das fronteiras da organização. O relatório da Verizon de 2025 registrou que a participação de terceiros nas violações analisadas dobrou em relação ao ano anterior, chegando a 30% dos casos (Verizon, 2025). Esse dado indica que a proteção efetiva dos dados de uma organização depende, em medida considerável, das práticas de seus prestadores de serviço, e que abordagens limitadas aos controles internos tendem a deixar parte relevante do risco sem tratamento. Por essa razão, tanto a LGPD quanto o regulamento europeu disciplinam expressamente a relação entre quem decide sobre o tratamento e quem o executa.

A LGPD estabelece que o operador deve realizar o tratamento segundo as instruções fornecidas pelo controlador, cabendo a este verificar a observância das próprias instruções e das normas sobre a matéria, conforme o artigo 39 (Brasil, 2018). O artigo 42, por sua vez, prevê que o operador responde solidariamente pelos danos causados quando descumprir as obrigações da legislação ou não seguir as instruções lícitas do controlador. No regulamento europeu, o artigo 28 exige que o responsável recorra

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas e detalha o conteúdo mínimo do contrato que rege essa relação (União Europeia, 2016).

O caso do MOVEit Transfer mostrou a escala que um único fornecedor pode alcançar. Segundo alerta conjunto do Federal Bureau of Investigation e da Cybersecurity and Infrastructure Security Agency, a partir de 27 de maio de 2023 o grupo criminoso conhecido como CL0P passou a explorar uma vulnerabilidade de injeção de SQL até então desconhecida, catalogada como CVE-2023-34362, nesse software de transferência gerenciada de arquivos, instalando um *web shell* denominado LEMURLOOT nas aplicações expostas à internet e extraindo dados de suas bases (FBI; CISA, 2023). Por viabilizar a transferência de arquivos entre organizações, clientes e parceiros, a ferramenta permitiu que a exploração de uma única vulnerabilidade expusesse simultaneamente dados de múltiplas organizações.

As publicações técnicas recomendam que a gestão de terceiros seja tratada como processo contínuo, e não como verificação pontual realizada no momento da contratação. O guia do NIST sobre gestão de riscos de cibersegurança na cadeia de fornecimento, elaborado por Boyens *et al.* (2022), orienta as organizações a integrar esses riscos à gestão de riscos corporativos, a definir requisitos de segurança nos contratos, a avaliar a criticidade de cada fornecedor e a monitorar seu desempenho ao longo de toda a relação. A proposta de atualização da regra de segurança da legislação norte-americana de saúde, ao exigir verificação escrita anual das salvaguardas dos parceiros de negócios, aplica essa mesma lógica de supervisão periódica (United States, 2025).

No sistema financeiro brasileiro, a Resolução CMN nº 4.893/2021 estabeleceu requisitos para a política de segurança cibernética das instituições autorizadas a funcionar pelo Banco Central e para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem (Conselho Monetário Nacional, 2021). A norma foi alterada pela Resolução CMN nº 5.274/2025, que passou a exigir, entre outros pontos, a verificação dos controles de sistemas adquiridos ou desenvolvidos por prestadores de serviço, autenticação multifator para acesso à rede corporativa a partir de ambientes externos e testes de intrusão com periodicidade mínima anual (Conselho Monetário Nacional, 2025). O detalhamento progressivo dos controles exigidos aproxima a regulação setorial da lógica de requisitos verificáveis.

8 FISCALIZAÇÃO E SANÇÕES: O QUE AS DECISÕES REVELAM SOBRE A DISTÂNCIA ENTRE NORMA E PRÁTICA

As decisões de autoridades reguladoras constituem fonte privilegiada para observar como a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

conformidade é avaliada na prática. No Brasil, a primeira sanção pecuniária aplicada pela ANPD, publicada em julho de 2023, atingiu uma microempresa, a Telekall Infoservice, com advertência e multa total de R$ 14,4 mil, por infração ao artigo 7º da LGPD, relativo às hipóteses legais de tratamento, e ao artigo 5º do Regulamento de Fiscalização, que estabelece deveres dos agentes regulados perante a autoridade (Mobile Time, 2023). O processo havia sido instaurado em 2022, e a lista de apuração divulgada pela autoridade mencionava também a ausência de registro das operações e de encarregado, o que mostra que, nesse primeiro caso, deficiências básicas de base legal e de documentação ocuparam posição central.

O Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4/2023, classifica as infrações em leves, médias e graves e prevê circunstâncias atenuantes e agravantes para o cálculo das multas (ANPD, 2023). Entre as atenuantes estão a implementação de política de boas práticas e governança, ou a adoção reiterada e comprovada de mecanismos internos capazes de minimizar os danos aos titulares, e a adoção de medidas que revertam ou mitiguem os efeitos da infração. A segunda hipótese exige que os mecanismos internos sejam adotados de forma reiterada e comprovada, o que indica atenção à sua efetiva aplicação, e não apenas à sua previsão formal.

Na União Europeia, decisões recentes da autoridade irlandesa de proteção de dados examinaram diretamente a arquitetura dos sistemas. Em novembro de 2022, a autoridade aplicou à Meta Platforms Ireland multas que somaram 265 milhões de euros por infração aos números 1 e 2 do artigo 25 do regulamento, em razão do tratamento realizado por meio de ferramentas de busca e de importação de contatos do Facebook e do Instagram, exploradas para a raspagem de dados (Data Protection Commission, 2022). Em dezembro de 2024, nova decisão impôs 251 milhões de euros relacionados a uma violação de 2018, dos quais 240 milhões corresponderam a infrações ao artigo 25 e os 11 milhões restantes, a falhas na notificação e na documentação da violação (Data Protection Commission, 2024).

A decisão de 2024 descreve que a combinação de funcionalidades da plataforma permitia a geração de uma credencial de acesso, denominada *token*, com acesso pleno ao perfil de outro usuário, falha explorada entre 14 e 28 de setembro de 2018 e que afetou cerca de 29 milhões de contas no mundo, das quais aproximadamente 3 milhões na União Europeia e no Espaço Econômico Europeu (Data Protection Commission, 2024). Nos Estados Unidos, o Office of the Comptroller of the Currency aplicou em 2020 multa de US$ 80 milhões à Capital One por não ter estabelecido processos eficazes de avaliação de riscos antes de migrar operações relevantes de tecnologia para a nuvem pública e por não ter corrigido tempestivamente as deficiências identificadas (Office of the Comptroller of the Currency, 2020). A Tabela 1 reúne esses casos.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

Tabela 1 – Casos selecionados de sanção relacionados à proteção de dados e à segurança da informação

Organização	Autoridade e ano	Sanção	Fundamento principal
Telekall Infoservice (Brasil)	ANPD, 2023	Advertência e multa de R$ 14,4 mil	Art. 7º da LGPD e art. 5º do Regulamento de Fiscalização
Capital One (Estados Unidos)	OCC, 2020	US$ 80 milhões	Ausência de avaliação de riscos eficaz antes da migração para nuvem pública
Meta Platforms Ireland (raspagem de dados)	DPC, 2022	€ 265 milhões	Art. 25(1) e 25(2) do RGPD, proteção desde a concepção e por padrão
Meta Platforms Ireland (violação de 2018)	DPC, 2024	€ 251 milhões	Art. 25(1) e 25(2) do RGPD (€ 240 milhões) e art. 33(3) e 33(5) (€ 11 milhões)

Fonte: elaborado pelo autor com base em Mobile Time (2023), Office of the Comptroller of the Currency (2020) e Data Protection Commission (2022; 2024).

Os casos reunidos na Tabela 1 diferem quanto às jurisdições, aos portes empresariais e aos fundamentos legais, o que impede comparações quantitativas diretas entre as sanções. Sua contribuição analítica reside, portanto, não na magnitude das multas, mas nos critérios utilizados pelas autoridades para avaliar a conformidade. Nas decisões europeias e norte-americana, a fundamentação concentra-se na ausência de proteção incorporada ao projeto dos sistemas ou na insuficiência da avaliação de riscos anterior às decisões tecnológicas. Na decisão de 2024, as infrações relativas à notificação e à documentação representaram parcela minoritária da multa, reforçando, nesse caso, a centralidade das falhas materiais de proteção. Esses elementos sugerem uma orientação fiscalizatória voltada à verificação de como as obrigações legais se concretizam em escolhas de arquitetura e práticas de gestão. Sob essa perspectiva, políticas, registros e procedimentos não perdem sua relevância, mas precisam demonstrar vínculo com os controles efetivamente implementados. A distinção é central para o debate sobre conformidade simbólica: a existência de estruturas formais não equivale, por si só, à proteção dos titulares. Contudo, a heterogeneidade e o número limitado dos casos não permitem afirmar uma trajetória uniforme de amadurecimento regulatório; permitem identificar, nas decisões examinadas, sinais de uma avaliação mais substantiva da relação entre norma e prática.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

9 CONCLUSÃO

Este artigo examinou a distância entre a conformidade formal com as leis de proteção de dados e a proteção efetiva das informações pessoais. A literatura organizacional e sociojurídica discutida permite compreender essa distância não apenas como desvio individual de organizações negligentes, mas também como tendência estrutural, associada à adoção de estruturas formais em busca de legitimidade e à possibilidade de que essas estruturas se desacoplem das práticas técnicas. O conceito de endogeneidade jurídica e sua aplicação ao campo da privacidade oferecem instrumentos para identificar quando os documentos de conformidade deixam de orientar decisões e passam a substituí-las.

A literatura também mostra que esse desfecho não é inevitável. O estudo de Bamberger e Mulligan, baseado em entrevistas com diretores de privacidade, identificou organizações que deslocaram o foco dos procedimentos formais para a prevenção substantiva de danos, impulsionadas pela atuação de reguladores, pela pressão de mercado e pela profissionalização da área. Isso indica que o ambiente regulatório e institucional influencia a direção que a conformidade assume dentro das organizações, e que mecanismos de fiscalização orientados a resultados podem favorecer a convergência entre norma e prática.

A privacidade desde a concepção, prevista no artigo 25 do regulamento europeu e no parágrafo 2º do artigo 46 da LGPD, constitui instrumento jurídico central para essa convergência, desde que interpretada como obrigação de efetividade. As diretrizes européias sobre o tema e a literatura de engenharia de privacidade convergem ao indicar que a proteção precisa ser convertida em requisitos de sistema, como a minimização da coleta, a separação de bases e configurações protetivas por padrão, e que princípios genéricos, por si só, não alteram a arquitetura das aplicações.

O inventário de dados revelou-se condição prévia de qualquer controle. A proporção de violações que envolveram dados não gerenciados, registrada no estudo da IBM de 2024, mostra que o registro das operações de tratamento exigido pela LGPD só cumpre sua função quando reflete o ambiente real, inclusive as cópias e os repositórios criados fora dos processos formais. A minimização, ao reduzir o volume de informações mantidas, complementa o inventário e diminui a exposição em caso de incidente, o que a torna também uma medida de segurança.

Os casos da Equifax e da Change Healthcare evidenciam que falhas em controles técnicos amplamente conhecidos, como a identificação de vulnerabilidades, a segmentação do acesso a bases de dados e a autenticação multifator, podem produzir exposição de dezenas ou centenas de milhões de pessoas em organizações de grande porte, sujeitas a extensa regulação setorial. A proposta de atualização da regra de segurança do setor de saúde norte-americano, ao tornar exigíveis controles

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

antes sujeitos à avaliação discricionária das entidades, indica que o regulador norte-americano da saúde passou a preferir requisitos expressos a obrigações genéricas de segurança sujeitas à avaliação de cada entidade.

A gestão de terceiros despontou como dimensão decisiva. A elevação da participação de fornecedores nas violações e a exploração em massa de um único software de transferência de arquivos sugerem que a conformidade contratual, limitada a cláusulas e questionários aplicados na contratação, tende a não acompanhar a dinâmica dos riscos. As orientações técnicas e as normas setoriais mais recentes, inclusive no sistema financeiro brasileiro, apontam para a supervisão contínua e para a verificação dos controles efetivamente implementados pelos prestadores.

Os casos sancionadores examinados sugerem que a fiscalização tende a evoluir da verificação documental para o exame da arquitetura dos sistemas e da qualidade das avaliações de risco. No Brasil, a atuação da ANPD ainda se encontra em fase de consolidação, mas o regulamento de dosimetria já prevê, entre as atenuantes, a adoção reiterada e comprovada de mecanismos internos de minimização de danos. Essa orientação, se mantida, pode contribuir para reduzir o incentivo à conformidade apenas simbólica e estimular investimentos em controles verificáveis.

Como limitação, registra-se que os casos analisados são majoritariamente de grande porte e de jurisdições estrangeiras, o que restringe a generalização das conclusões para organizações brasileiras de menor porte. Recomenda-se, para estudos futuros, a realização de pesquisas empíricas com organizações nacionais que comparem a maturidade documental de seus programas de privacidade com indicadores técnicos de proteção, bem como a análise sistemática das decisões da ANPD à medida que sua jurisprudência administrativa se consolide. Tais estudos permitiriam verificar em que medida o desacoplamento entre norma e prática se manifesta no contexto brasileiro.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy on the books and on the ground. **Stanford Law Review**, Stanford, v. 63, n. 2, p. 247, 2011.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOYENS, Jon; SMITH, Angela; BARTOL, Nadya; WINKLER, Kris; HOLBROOK, Alexander; FALLON, Matthew. **Cybersecurity supply chain risk management practices for systems and organizations**. Gaithersburg: National Institute of Standards and Technology, 2022. (NIST Special Publication 800-161, rev. 1). DOI: 10.6028/NIST.SP.800-161r1.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

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.

CAVOUKIAN, Ann. **Privacy by design**: the 7 foundational principles. Toronto: Information and Privacy Commissioner of Ontario, 2009.

CONSELHO MONETÁRIO NACIONAL (Brasil). **Resolução CMN nº 4.893, de 26 de fevereiro de 2021**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Brasília, DF: Banco Central do Brasil, 2021.

CONSELHO MONETÁRIO NACIONAL (Brasil). **Resolução CMN nº 5.274, de 18 de dezembro de 2025**. Altera a Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Brasília, DF: Banco Central do Brasil, 2025.

DANEZIS, George; DOMINGO-FERRER, Josep; HANSEN, Marit; HOEPMAN, Jaap-Henk; LE MÉTAYER, Daniel; TIRTEA, Rodica; SCHIFFNER, Stefan. **Privacy and data protection by design**: from policy to engineering. Heraklion: European Union Agency for Network and Information Security (ENISA), 2014.

DATA PROTECTION COMMISSION (Irlanda). **Data Protection Commission announces decision in Facebook "Data Scraping" inquiry**. Dublin: DPC, 28 nov. 2022.

DATA PROTECTION COMMISSION (Irlanda). **Irish Data Protection Commission fines Meta €251 million**. Dublin: DPC, 17 dez. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EDELMAN, Lauren B. **Working law**: courts, corporations, and symbolic civil rights. Chicago: University of Chicago Press, 2016.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 4/2019 on Article 25**: data protection by design and by default. Version 2.0. Brussels: EDPB, 2020.

FEDERAL BUREAU OF INVESTIGATION (FBI); CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). **#StopRansomware**: CL0P ransomware gang exploits CVE-2023-34362 MOVEit vulnerability. Washington, DC: CISA, 2023. (Cybersecurity Advisory AA23-158A).

FIERCE HEALTHCARE. UnitedHealth estimates 190M people impacted by Change Healthcare cyberattack. **Fierce Healthcare**, [S. l.], 24 jan. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

HOEPMAN, Jaap-Henk. Privacy design strategies. In: IFIP INTERNATIONAL INFORMATION SECURITY CONFERENCE, 29., 2014, Marrakech. **ICT Systems Security and Privacy Protection**. Berlin: Springer, 2014. p. 446-459. DOI: 10.1007/978-3-642-55415-5_38.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

IBM. **Cost of a data breach report 2024**. Armonk: IBM Corporation, 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27701**: information security, cybersecurity and privacy protection, privacy information management systems, requirements and guidance. Geneva: ISO, 2025.

MEYER, John W.; ROWAN, Brian. Institutionalized organizations: formal structure as myth and ceremony. **American Journal of Sociology**, Chicago, v. 83, n. 2, p. 340-363, 1977.

MOBILE TIME. ANPD aplica sua primeira sanção com multa à Telekall. **Mobile Time**, São Paulo, 6 jul. 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **NIST Privacy Framework**: a tool for improving privacy through enterprise risk management. Version 1.0. Gaithersburg: NIST, 2020.

OFFICE OF THE COMPTROLLER OF THE CURRENCY (Estados Unidos). **OCC assesses $80 million civil money penalty against Capital One**. Washington, DC: OCC, 6 ago. 2020. (News Release 2020-101).

POWER, Michael. **The audit society**: rituals of verification. Oxford: Oxford University Press, 1997.

ROTHER, Edna Terezinha. Revisão sistemática X revisão narrativa. **Acta Paulista de Enfermagem**, São Paulo, v. 20, n. 2, p. v-vi, 2007.

SPIEKERMANN, Sarah; CRANOR, Lorrie Faith. Engineering privacy. **IEEE Transactions on Software Engineering**, [New York], v. 35, n. 1, p. 67-82, 2009.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial da União Europeia**, Luxemburgo, L 119, p. 1-88, 4 maio 2016.

UNITED STATES. Government Accountability Office. **Data protection**: actions taken by Equifax and federal agencies in response to the 2017 breach. Washington, DC: GAO, 2018. (GAO-18-559).

UNITED STATES. Department of Health and Human Services. HIPAA Security Rule to strengthen the cybersecurity of electronic protected health information: proposed rule. **Federal Register**, Washington, DC, v. 90, n. 3, p. 898-1022, 6 jan. 2025.

VERIZON. **2025 data breach investigations report**. Basking Ridge: Verizon Business, 2025.

WALDMAN, Ari Ezra. Privacy law's false promise. **Washington University Law Review**, St. Louis, v. 97, n. 3, p. 773, 2020.

WALDMAN, Ari Ezra. **Industry unbound**: the inside story of privacy, data, and corporate power. Cambridge: Cambridge University Press, 2021.

WITTY, Andrew. **Testimony before the United States Senate Committee on Finance**: hacking America's health care, assessing the Change Healthcare cyberattack and what's next. Washington,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/11/2026 | aceito: 11/11/2026 | publicação: 16/11/2026

DC: U.S. Senate, 1 maio 2024.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.