O Estado como controlador de dados: Brasil, EUA, Canadá e Europa

Adilson Braga

A disciplina da proteção de dados pessoais nasceu, no Atlântico Norte, como resposta ao Estado. A primeira lei do gênero, a do Land alemão de Hesse, de 1970, destinava-se à administração pública (Mayer-Schönberger, 1997); o *Privacy Act* norte-americano, de 1974, alcança apenas agências federais; e o *Privacy Act* canadense, em vigor desde 1983, rege exclusivamente instituições federais. O Tribunal Constitucional Federal alemão formulou a autodeterminação informativa em 1983 justamente ao julgar o recenseamento promovido pelo governo (Alemanha, 1983). No Brasil, a Lei nº 13.709/2018 (LGPD) chegou como lei geral, aplicável a particulares e ao Poder Público, e dedicou ao setor público um capítulo próprio (arts. 23 a 32), opção que distingue o modelo brasileiro (Braga; Ferreira, 2026, p. 107-108).

Essa diferença de origem ajuda a explicar diferenças de cultura institucional, mas não resolve a pergunta que interessa ao gestor e ao controle: como os Estados que regulam o tema há décadas fiscalizam a si mesmos, e o que seus relatórios oficiais revelam sobre as dificuldades que enfrentam? Adoto aqui o método funcional do direito comparado, que parte de problemas comuns e examina as soluções que cada ordenamento dá a eles (Zweigert; Kötz, 1998). Os problemas escolhidos são cinco: quem supervisiona o ente público, com que poderes, que responsável interno a lei exige, que instrumentos preventivos são obrigatórios e como se tratam os incidentes. O foco recai sobre Estados Unidos, Canadá, União Europeia e Reino Unido, com base em relatórios de auditoria, de autoridades de proteção de dados e de parlamentos.

1. Culturas de privacidade e desenho institucional

Whitman (2004) sintetizou a divergência transatlântica em duas matrizes: a europeia, centrada na dignidade e na proteção contra a exposição pública, e a norte-americana, centrada na liberdade diante do Estado. O paradoxo é que, justamente por desconfiar do governo, os Estados Unidos regularam cedo o tratamento federal de dados, mas o fizeram por meio de controles internos ao Executivo, sem criar autoridade independente com poder sobre as agências (Regan, 1995). Flaherty (1989), no estudo comparado clássico sobre as agências de proteção de dados da Alemanha, da Suécia, da França, do Canadá e dos Estados Unidos, já mostrava que a eficácia da proteção diante do Estado depende menos do texto legal e mais da existência de um órgão de

supervisão com independência, recursos e disposição para confrontar a administração.

Mayer-Schönberger (1997) descreveu a evolução europeia em gerações, das leis voltadas aos grandes bancos de dados estatais à tutela de direitos individuais e, depois, à proteção setorial e participativa. O RGPD consolidou esse percurso com autoridades independentes dotadas de poderes corretivos também sobre entes públicos. No Brasil, a proteção de dados foi construída a partir de outra trajetória, que Doneda (2019) e Mendes (2014) reconstituem como deslocamento da tutela da intimidade para a disciplina dos fluxos informacionais, com forte influência do direito do consumidor. O resultado é um regime mais recente, ainda em formação institucional, que se aplica a todos os entes federativos, inclusive aos 5.570 municípios, universo que as leis federais norte-americana e canadense não alcançam e que, na Europa, o RGPD alcança.

2. Estados Unidos: controle hierárquico sem autoridade independente

O regime federal norte-americano é um mosaico. O *Privacy Act* de 1974 disciplina os sistemas de registros das agências; a seção 208 do *E-Government Act* de 2002 exige avaliações de impacto à privacidade antes do desenvolvimento ou da aquisição de sistemas que coletem informações identificáveis; e a *Federal Information Security Modernization Act* de 2014 (FISMA) estrutura a segurança da informação. Em 2016, a Ordem Executiva 13.719 criou o Federal Privacy Council, e o Memorando M-16-24 do Office of Management and Budget (OMB) detalhou o papel do *Senior Agency Official for Privacy* (SAOP) que cada agência deve designar. A supervisão cabe ao OMB, aos inspetores-gerais e ao Government Accountability Office (GAO). Estados e municípios ficam fora do *Privacy Act* e dependem de leis estaduais próprias.

Os números oficiais mostram a escala do problema. No último relatório anual FISMA disponível, relativo ao exercício de 2023, as agências federais reportaram 32.211 incidentes de segurança, 9,9% a mais que os 29.319 do exercício anterior, dos quais 11 foram classificados como incidentes maiores. As agências abrangidas pelo *CFO Act* registraram internamente 18.909 violações de informações pessoais identificáveis e reportaram 8.420 à Cybersecurity and Infrastructure Security Agency (CISA). No mesmo relatório, 100% das agências declararam ter designado seu SAOP (Estados Unidos, 2024). A designação formal, porém, não garante função efetiva. O GAO examinou 24 agências e concluiu que os responsáveis designados acumulavam outras atribuições principais e dificilmente dedicavam à privacidade a maior parte do tempo; 21 agências apontaram insuficiência de recursos, e o órgão sugeriu ao Congresso exigir por lei um responsável sênior dedicado (Estados Unidos, 2022). Em 2023, o GAO incluiu a proteção da

privacidade entre as ações prioritárias da área de alto risco em cibersegurança federal (Estados Unidos, 2023).

O caso que moldou a percepção pública foi o do Office of Personnel Management (OPM): em 2015, dados de investigações de antecedentes de 21,5 milhões de pessoas, com números de seguridade social e registros de impressões digitais, foram subtraídos (Christensen, 2015). A reparação individual, por sua vez, é estreita. O *Privacy Act* prevê indenização mínima de US$ 1.000 por violação intencional, mas a Suprema Corte, em *FAA v. Cooper*, limitou os danos reais a prejuízos patrimoniais, excluindo o sofrimento mental ou emocional (Estados Unidos, 2012). Quanto aos incidentes, as diretrizes federais exigem comunicação à CISA em até uma hora após a identificação (Estados Unidos, 2017), prazo que revela a lógica de segurança nacional do sistema.

O ponto mais sensível é a independência. O Privacy and Civil Liberties Oversight Board, órgão colegiado independente cujo mandato se restringe às atividades de contraterrorismo do Executivo, teve três de seus cinco membros removidos pelo Presidente em janeiro de 2025; a disputa judicial que se seguiu foi sobrestada em segunda instância à espera do julgamento de *Trump v. Slaughter* (Brennan Center for Justice, 2025). Em 29 de junho de 2026, no caso *Trump v. Slaughter*, a Corte declarou contrária à separação de poderes a proteção contra remoção imotivada dos membros da Federal Trade Commission, superando o precedente *Humphrey's Executor* (Estados Unidos, 2026). Para um sistema que já não dispunha de autoridade independente sobre as agências, a decisão reduz ainda mais a margem de supervisão externa ao Executivo.

3. Canadá: o modelo de ombudsman e seus limites

O *Privacy Act* canadense alcança mais de 250 instituições federais e, segundo o próprio governo, não foi substancialmente atualizado desde 1983 (Canadá, 2026c). O Office of the Privacy Commissioner (OPC) atua como ombudsman: investiga e recomenda, mas, na maior parte das violações, não pode emitir ordens vinculantes, ao contrário do Comissário de Informação, que já dispõe desse poder no regime de acesso (Canadá, 2026b). Duas obrigações centrais não estão na lei. A avaliação de impacto à privacidade e a notificação de violações relevantes ao OPC e ao Treasury Board of Canada Secretariat (TBS) decorrem de políticas do TBS, e não de comando legal (Canadá, 2026b).

Os relatórios do OPC ao Parlamento mostram o perfil das falhas. No exercício de 2024-2025, instituições federais notificaram 615 violações, contra 561 no ano anterior, e o número de pessoas afetadas mais que dobrou, de 138.434

para 309.865; a manipulação inadequada de informações, como erros de digitação, correspondência enviada ao destinatário errado e falhas de etiquetagem, respondeu por 508 casos (Canadá, 2025b). Em 2025-2026, foram 451 notificações, que afetaram 48.159 pessoas: 368 por manipulação inadequada, 39 por incidentes cibernéticos e 22 por acesso indevido de servidores, e 94% foram avaliadas como aptas a causar risco real de dano significativo (Canadá, 2026a). O dado qualitativo relevante é que a falha dominante no setor público canadense é procedimental e humana. Há também indício de subnotificação: em documento preparado para comissão parlamentar, ao tratar das diferentes obrigações de notificação dos setores público e privado, o OPC registrou que, em 2024-2025, recebeu 429 notificações do setor privado e apenas 55 de instituições federais relativas a incidentes cibernéticos (Canadá, 2025a).

O OPC encaminhou ao Parlamento sete recomendações prioritárias de reforma: exigência expressa de necessidade e proporcionalidade na coleta, avaliação de impacto obrigatória em situações de alto risco, poder de emitir ordens vinculantes, discricionariedade para recusar reclamações, dever legal expresso de salvaguarda, obrigação legal de notificar violações e maior liberdade para relatórios públicos (Canadá, 2025a). Em 2 de abril de 2026, o governo abriu revisão formal da lei, com propostas de converter em obrigação legal a gestão e a notificação de violações, tornar obrigatória a avaliação de impacto quando programas usarem dados pessoais para decisões, com publicação de sumários em registro central, e conferir ao Comissário poder de ordem sobre planos de ação corretiva (Canadá, 2026b; 2026c). No plano da auditoria, o Comitê de Contas Públicas da Câmara dos Comuns, ao examinar o relatório do Auditor-Geral sobre dados pessoais em nuvem, registrou fragilidades nos controles de prevenção, detecção e resposta, papéis e responsabilidades pouco claros e ausência de modelo de custeio e de financiamento para os serviços de nuvem (Canadá, 2024).

4. União Europeia e Reino Unido: supervisão independente com poder sobre o Estado

4.1 União Europeia

O RGPD aplica-se integralmente às autoridades públicas, torna obrigatória a designação de encarregado para elas (art. 37, n. 1, a), exige avaliação de impacto nos tratamentos de alto risco (art. 35), fixa 72 horas para a notificação de violações à autoridade (art. 33) e submete os entes públicos aos poderes corretivos das autoridades de controle (art. 58, n. 2). Apenas as multas ficam a critério de cada Estado-membro (art. 83, n. 7). As instituições da própria União

respondem ao Regulamento (UE) 2018/1725, sob supervisão da Autoridade Europeia para a Proteção de Dados (EDPS).

A distinção entre o modelo europeu e o norte-americano aparece com nitidez em dois casos. Em 8 de março de 2024, a EDPS concluiu que a Comissão Europeia, ao utilizar o Microsoft 365, violara regras de limitação da finalidade, de transferências internacionais e de divulgações não autorizadas, e ordenou a suspensão, a partir de 9 de dezembro de 2024, dos fluxos de dados para a Microsoft e suas subcontratadas em países sem decisão de adequação, além da adequação contratual e do mapeamento das transferências (European Data Protection Supervisor, 2024). Em julho de 2025, a EDPS reconheceu que as infrações haviam sido sanadas e encerrou o procedimento (European Data Protection Supervisor, 2025). Um órgão de supervisão impôs à principal instituição executiva da União a correção de seu contrato de nuvem, e a correção ocorreu.

O segundo caso é o neerlandês. A Autoridade de Proteção de Dados multou a administração tributária (Belastingdienst) em 2,75 milhões de euros, em dezembro de 2021, pelo tratamento discriminatório e ilícito da dupla nacionalidade de requerentes de auxílio para creche, no contexto do escândalo dos auxílios para creche (Boete, 2021). Em abril de 2022, aplicou nova multa, de 3,7 milhões de euros, pela lista de sinalização de fraudes (FSV), que reunia cerca de 270 mil pessoas sem base legal e cuja criação não contou, a tempo, com a participação do responsável interno pela supervisão de privacidade (Recordboete..., 2022). O episódio mostra que a multa ao ente público, admitida pela lei neerlandesa, pode ser instrumento de reconhecimento institucional de uma violação sistêmica.

O Tribunal de Justiça da União Europeia, por sua vez, tem traçado os limites da transparência administrativa. Considerou incompatível com o RGPD a divulgação pública irrestrita de pontos de penalidade de condutores (C-439/19, 2021) e a publicação em linha, com dados que permitiam inferir aspectos sensíveis, de declarações de interesses de agentes públicos (C-184/20, 2022) (União Europeia, 2021; 2022). A tensão entre publicidade e privacidade, que no Brasil se expressa na convivência entre a Lei de Acesso à Informação e a LGPD, é resolvida ali por um teste de necessidade e proporcionalidade aplicado caso a caso.

As ações coordenadas do European Data Protection Board (EDPB) oferecem um retrato empírico do setor público europeu. Em 2022, 22 autoridades examinaram cerca de 100 órgãos públicos de saúde, finanças, tributação e educação e constataram dificuldade na contratação de serviços de nuvem conformes ao RGPD (European Data Protection Board, 2023). Em 2023, com 25 autoridades e 17.490 respondentes, o EDPB listou como problemas a falta de designação do encarregado mesmo quando obrigatória, recursos e

formação insuficientes, conflito de interesses e ausência de reporte à alta direção, e verificou que os encarregados do setor público tinham menos acesso a substituto (36,4% contra 56,3%) e a orçamento (26,6% contra 56,8%), e que os recursos eram considerados suficientes em 66% dos casos no setor público, contra 91% no privado (European Data Protection Board, 2024, p. 16). A Agência dos Direitos Fundamentais registrou que as autoridades nacionais têm dificuldade de supervisionar e orientar autoridades públicas controladoras, e que a insuficiência de recursos compromete sua independência (European Union Agency for Fundamental Rights, 2024). O Tribunal de Contas Europeu, por sua vez, concluiu que o nível de preparação das instituições da União em cibersegurança não era, no geral, compatível com as ameaças (European Court of Auditors, 2022).

4.2 Reino Unido

O Reino Unido manteve, após a saída da União, o RGPD incorporado ao direito interno (UK GDPR) e a Data Protection Act 2018, com o Information Commissioner's Office (ICO) como supervisor. A particularidade britânica é a política de preferência por reprimendas públicas ao setor público, adotada em 2022 e mantida em dezembro de 2024 após avaliação: cerca de 60 reprimendas foram dirigidas a órgãos públicos no período de teste, e as multas somaram 1,2 milhão de libras, quando poderiam ter alcançado 23,2 milhões (Information Commissioner's Office, 2024b).

Os casos que motivaram as multas remanescentes são reveladores. O Police Service of Northern Ireland publicou, em agosto de 2023, em resposta a um pedido de acesso à informação, planilha com aba oculta contendo sobrenomes, iniciais, cargos, lotação e outros dados de todos os 9.483 policiais e servidores; a multa foi de 750 mil libras e, sem a política para o setor público, teria sido de 5,6 milhões (Information Commissioner's Office, 2024a). No Ministério da Defesa, em 22 de fevereiro de 2022, um servidor enviou por e-mail, fora dos sistemas oficiais, planilha com dados de 18.700 afegãos candidatos a reassentamento; o programa de resposta tem custo estimado pelo ministério em cerca de 850 milhões de libras (National Audit Office, 2025b). O ICO reconheceu a gravidade do dano, mas decidiu não adotar nova medida, considerando, entre outros fatores, a multa de 350 mil libras já aplicada ao ministério em 2023 por falha correlata (Information Commissioner's Office, 2025). Na dimensão de segurança, o National Audit Office constatou lacunas significativas de resiliência nos 58 sistemas críticos avaliados em 2024, ao menos 228 sistemas legados com vulnerabilidades desconhecidas e um terço das funções de cibersegurança vagas ou ocupadas por temporários (National Audit Office, 2025a).

5. O Brasil no espelho

Tabela 1. Regime aplicável a entes públicos, por jurisdição

Aspecto	EUA (federal)	Canadá (federal)	União Europeia	Reino Unido	Brasil
Norma para o setor público	Privacy Act (1974), E-Government Act (2002) e FISMA (2014)	Privacy Act (1983)	RGPD e Reg. 2018/1725	UK GDPR e DPA 2018	LGPD, cap. IV
Supervisor	OMB, inspetores-gerais e GAO; sem autoridade independente geral	OPC (ombudsman)	Autoridades nacionais e EDPS	ICO	ANPD e, na gestão, Tribunais de Contas
Ordem vinculante contra o ente	Não	Não, na maior parte dos casos	Sim (art. 58)	Sim	Sim, exceto multa
Multa ao ente público	Não se aplica	Não	Conforme o Estado-membro (art. 83, n. 7)	Sim, com política de redução	Vedada (art. 52, § 3º)
Responsável interno	SAOP (política do OMB)	Delegação pelo chefe da instituição	Encarregado obrigatório (art. 37)	Encarregado obrigatório	Encarregado obrigatório (art. 23, III)

Aspecto	EUA (federal)	Canadá (federal)	União Europeia	Reino Unido	Brasil
Avaliação de impacto	Obrigatória em lei (E-Gov Act, seção 208)	Por política do TBS	Obrigatória no alto risco (art. 35)	Obrigatória no alto risco	RIPD; publicação pode ser exigida (art. 32)
Comunicação de incidente	Uma hora à CISA	Por política, ao OPC e ao TBS	72 horas	72 horas	Três dias úteis (Res. CD/ANPD nº 15/2024)

Fontes: legislação citada; Estados Unidos (2017; 2024); Canadá (2026b); European Data Protection Board (2025); Information Commissioner's Office (2024b); elaboração do autor.

Colocado ao lado desses modelos, o regime brasileiro apresenta uma combinação singular. No plano normativo, está mais próximo do europeu do que o norte-americano ou o canadense: encarregado obrigatório, dever de transparência ativa sobre as hipóteses de tratamento (art. 23, I), prazo curto para comunicação de incidentes e uma autoridade que, desde a Lei nº 15.352/2026, é a Agência Nacional de Proteção de Dados, autarquia de natureza especial. O EDPB reconheceu, no mesmo parecer, a natureza especial da autarquia, a autonomia orçamentária e o acréscimo de mais de 200 cargos à sua estrutura (European Data Protection Board, 2025, § 47-50). A diferença decisiva está na sanção: o art. 52, § 3º, afasta multas contra entes públicos, e o EDPB, ao opinar sobre a adequação do Brasil, registrou essa exceção e convidou a Comissão Europeia a acompanhar a aplicação consistente das sanções (European Data Protection Board, 2025, § 55). A decisão de adequação foi adotada pela Comissão em 27 de janeiro de 2026 (Brazil..., 2026), o que torna o desempenho do setor público brasileiro objeto de monitoramento externo periódico.

No plano empírico, os achados brasileiros convergem com os estrangeiros. A auditoria do Tribunal de Contas da União (TCU) concluída em 2025 encontrou 58,4% das 387 organizações federais nos graus inexpressivo ou inicial de adequação, 69,77% sem registro das operações de tratamento, 72,35% sem qualquer relatório de impacto e 12,4% sem encarregado (Brasil, 2025a; 2025b). O descompasso entre designação formal e capacidade real, identificado pelo

GAO e pelo EDPB, reaparece aqui. O que o Brasil tem de próprio é o protagonismo dos Tribunais de Contas. O Auditor-Geral canadense, o National Audit Office e o Tribunal de Contas Europeu tratam do tema sobretudo pela via da segurança da informação, e o GAO examina programas de privacidade das agências federais em trabalhos específicos. O TCU e os tribunais estaduais, por sua vez, passaram a auditar em ciclos sucessivos, com questionário comum de nove dimensões, a conformidade à lei geral de proteção de dados de quase dois mil entes, somados apenas os ciclos do TCU, do TCE-RJ, do TCE-PE e do TCE-MG, e o TCU fixou em 2025 determinações com prazo para nomeação de encarregado, Política de Segurança da Informação e comunicação de incidentes (Brasil, 2025a).

6. Lições da comparação

A primeira lição é que a designação formal do responsável interno é um indicador fraco. Nos Estados Unidos, 100% das agências têm SAOP, e ainda assim o GAO sugeriu lei que exija um responsável sênior dedicado; na Europa, o encarregado é obrigatório, e o setor público é o que menos lhe dá orçamento e substituto. Auditorias brasileiras que se limitem a verificar o ato de nomeação medirão pouco. Posição hierárquica, tempo, orçamento e ausência de conflito de interesses precisam entrar na matriz de fiscalização.

A segunda é que as violações no setor público são, em sua maioria, procedimentais. No Canadá, a manipulação inadequada de informações responde pela grande maioria das notificações; no Reino Unido, dois dos casos de maior repercussão envolveram planilhas enviadas ou publicadas sem controle, um deles em resposta a pedido de acesso à informação. Para o Brasil, onde a Lei de Acesso à Informação produz diariamente respostas com anexos, o caso da polícia norte-irlandesa é um alerta direto sobre a necessidade de revisão de metadados e de abas ocultas antes de qualquer publicação.

A terceira diz respeito à natureza jurídica dos instrumentos preventivos. O Canadá discute, após mais de quatro décadas, converter em lei a avaliação de impacto e a notificação de violações que hoje dependem de política administrativa. No Brasil, a LGPD permite à ANPD solicitar a publicação de relatórios de impacto de agentes públicos (art. 32), mas não os torna obrigatórios de modo geral. Um regulamento que exija RIPD para tratamentos de alto risco no setor público, com registro público de sumários, na linha da proposta canadense, aproximaria o país do padrão europeu.

A quarta refere-se à sanção. Os modelos variam da exclusão alemã de multas a entes públicos (§ 43, Abs. 3, do BDSG), passando pelo limite de um milhão

de euros previsto na seção 141 da Data Protection Act 2018 irlandesa e pela política britânica de reprimendas, até a multa efetiva aplicada pela autoridade neerlandesa. O caso britânico sugere que a reprimenda publicada tem efeito reputacional relevante, e o neerlandês, que a multa pode marcar a gravidade institucional de uma violação. No Brasil, sem multa, a publicização da infração (art. 52, IV) e a responsabilização pessoal do gestor pelos Tribunais de Contas assumem a função dissuasória que a lei não confiou à sanção pecuniária.

A quinta é a nuvem. A decisão da EDPS contra a Comissão Europeia e a ação coordenada do EDPB sobre serviços em nuvem mostram que a contratação de soluções de produtividade e hospedagem é o ponto em que o setor público mais facilmente perde o controle das transferências internacionais. Com a adequação recíproca entre Brasil e União Europeia, o fluxo com o bloco europeu ficou simplificado, mas contratos com provedores sujeitos a legislações de terceiros países continuam a exigir mapeamento, avaliação e cláusulas específicas.

A sexta, por fim, é a independência. A trajetória norte-americana, com a remoção de membros do PCLOB e a superação de *Humphrey's Executor*, mostra que a supervisão da privacidade no interior do Estado é frágil quando depende da vontade do chefe do Executivo. A transformação da ANPD em agência reguladora caminha no sentido oposto, e o próprio EDPB pediu esclarecimentos sobre a relação entre a agência e o Conselho Nacional de Proteção de Dados (European Data Protection Board, 2025, § 52). A independência formal, contudo, vale pouco sem estrutura: a agência europeia de direitos fundamentais registrou que a falta de recursos compromete a capacidade das autoridades de supervisionar a administração pública (European Union Agency for Fundamental Rights, 2024).

Considerações finais

A comparação desfaz duas impressões. A primeira é a de que os países de tradição mais antiga resolveram o problema do Estado como controlador de dados: os relatórios do GAO, do OPC, do EDPB, do ICO e do National Audit Office descrevem falta de recursos, responsáveis internos sem dedicação exclusiva, violações por erro humano e dificuldade de supervisionar a própria administração. A segunda é a de que o Brasil estaria normativamente atrasado. Em vários pontos, a LGPD é mais exigente com o Poder Público do que as leis federais norte-americana e canadense, e foi considerada adequada pela União Europeia.

O que separa o Brasil dos modelos mais consistentes não é o texto, e sim a execução: capacidade dos entes subnacionais, instrumentos preventivos ainda facultativos e ausência de sanção pecuniária contra o Estado. Nos Estados Unidos e no Canadá, a supervisão é fraca por desenho; na Europa, é forte, mas sobrecarregada. O Brasil tem uma autoridade recém-fortalecida e, como

traço original, uma rede de Tribunais de Contas que já audita a conformidade à LGPD. Articular essas duas instâncias, com critérios comuns e troca de informações, é a vantagem comparativa que os demais sistemas não têm.

REFERÊNCIAS

ALEMANHA. Bundesverfassungsgericht. BVerfGE 65, 1 (Volkszählungsurteil). Karlsruhe, 15 dez. 1983.

ALEMANHA. Bundesdatenschutzgesetz (BDSG), de 30 de junho de 2017. Bundesgesetzblatt, Teil I, p. 2097, 2017.

BOETE voor Belastingdienst van 2,7 miljoen voor discriminatie toeslagenouders. NOS, Hilversum, 7 dec. 2021. Disponível em: https://nos.nl/artikel/2408587-boete-voor-belastingdienst-van-2-7-miljoen-voor-discriminatie-toeslagenouders. Acesso em: 11 set. 2026.

BRAGA JUNIOR, Adilson Fernandes; FERREIRA, Ricardo Padovini Pleti. Transformação digital e proteção de dados na Administração Pública. Uberlândia: Marco Teórico, 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.

BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a Agência Nacional de Proteção de Dados (ANPD), e dá outras providências. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15352.htm. Acesso em: 11 set. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024.

BRASIL. Tribunal de Contas da União (Plenário). Acórdão 1.372/2025. Relatório de Auditoria. Processo TC 009.980/2024-5. Relator: Min. Walton Alencar Rodrigues, 25 jun. 2025a. Disponível em: https://portal.tcu.gov.br/tecnologia-da-informacao/auditoria-sobre-lgpd. Acesso em: 11 set. 2026.

BRASIL. Tribunal de Contas da União. Voto do Relator no Processo TC 009.980/2024-5. Relator: Min. Walton Alencar Rodrigues. Brasília, DF: TCU, 2025b. Disponível em: https://portal.tcu.gov.br/data/files/3A/83/B3/7D/64BF791070549D79F18818A8/P

eca%20967%20-%20TC-009-980-2024-5_Peca%20967%20-%20VOTO-MIN-WAR-2025-3-20.pdf. Acesso em: 11 set. 2026.

BRAZIL, EU finalize adequacy agreement. IAPP News, Portsmouth, NH, 27 Jan. 2026. Disponível em: https://iapp.org/news/a/brazil-eu-finalize-adequacy-agreement. Acesso em: 11 set. 2026.

BRENNAN CENTER FOR JUSTICE. LeBlanc v. U.S. Privacy and Civil Liberties Oversight Board. New York: Brennan Center, 2025. Disponível em: https://www.brennancenter.org/our-work/research-reports/leblanc-v-us-privacy-and-civil-liberties-oversight-board. Acesso em: 11 set. 2026.

CANADÁ. House of Commons. Standing Committee on Public Accounts. Cybersecurity of personal information in the cloud. Report 44. Ottawa: House of Commons, Oct. 2024. Disponível em: https://www.ourcommons.ca/documentviewer/en/44-1/PACP/report-44/. Acesso em: 11 set. 2026.

CANADÁ. Office of the Privacy Commissioner of Canada. Consolidated issue sheets for a general information session (ETHI). Gatineau: OPC, 6 Oct. 2025a. Disponível em: https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_20251006/is_20251006/. Acesso em: 11 set. 2026.

CANADÁ. Office of the Privacy Commissioner of Canada. Highlights from the Commissioner's 2024-2025 annual report. Gatineau: OPC, 5 June 2025b. Disponível em: https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20250605/. Acesso em: 11 set. 2026.

CANADÁ. Office of the Privacy Commissioner of Canada. Highlights from the Privacy Commissioner of Canada's 2025-2026 annual report. Gatineau: OPC, 4 June 2026a. Disponível em: https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20260604/. Acesso em: 11 set. 2026.

CANADÁ. Treasury Board of Canada Secretariat. 2026 Review of the Privacy Act: policy approaches. Ottawa: TBS, 2026b. Disponível em: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches/2026-review-privacy-act-policy-approaches.html. Acesso em: 11 set. 2026.

CANADÁ. Treasury Board of Canada Secretariat. Government of Canada launches review of the Privacy Act. Ottawa: TBS, 2 Apr. 2026c. Disponível em: https://www.canada.ca/en/treasury-board-secretariat/news/2026/04/government-of-canada-launches-review-of-the-privacy-act.html. Acesso em: 11 set. 2026.

CHRISTENSEN, Michelle D. OPM data breach: personnel security background investigation data. IN10327. Washington, DC: Congressional Research Service, 24 July 2015.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

ESTADOS UNIDOS. Cybersecurity and Infrastructure Security Agency. Federal incident notification guidelines. Washington, DC: CISA, 2017. Disponível em: https://www.cisa.gov/federal-incident-notification-guidelines. Acesso em: 11 set. 2026.

ESTADOS UNIDOS. Government Accountability Office. Privacy: dedicated leadership can improve programs and address challenges. GAO-22-105065. Washington, DC: GAO, 2022. Disponível em: https://www.gao.gov/products/gao-22-105065. Acesso em: 11 set. 2026.

ESTADOS UNIDOS. Government Accountability Office. Cybersecurity high-risk series: challenges in protecting privacy and sensitive data. GAO-23-106443. Washington, DC: GAO, 2023. Disponível em: https://www.gao.gov/products/gao-23-106443. Acesso em: 11 set. 2026.

ESTADOS UNIDOS. Office of Management and Budget. Federal Information Security Modernization Act of 2014: annual report to Congress, fiscal year 2023. Washington, DC: OMB, 2024. Disponível em: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/FY23-FISMA-Report.pdf. Acesso em: 11 set. 2026.

ESTADOS UNIDOS. Office of Management and Budget. Memorandum M-16-24: role and designation of Senior Agency Officials for Privacy. Washington, DC: OMB, 15 Sept. 2016.

ESTADOS UNIDOS. President. Executive Order 13719: establishment of the Federal Privacy Council. Washington, DC: The White House, 9 Feb. 2016.

ESTADOS UNIDOS. Supreme Court. Federal Aviation Administration v. Cooper, 566 U.S. 284. Washington, DC, 28 Mar. 2012.

ESTADOS UNIDOS. Supreme Court. Trump v. Slaughter, n. 25-332. Washington, DC, 29 June 2026. Disponível em: https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf. Acesso em: 11 set. 2026.

EUROPEAN COURT OF AUDITORS. Special report 05/2022: cybersecurity of EU institutions, bodies and agencies: level of preparedness overall not commensurate with the threats. Luxembourg: ECA, 2022. Disponível em: https://www.eca.europa.eu/en/publications/SR22_05. Acesso em: 11 set. 2026.

EUROPEAN DATA PROTECTION BOARD. 2022 Coordinated Enforcement Action: use of cloud-based services by the public sector. Brussels: EDPB, 2023. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en. Acesso em: 11 set. 2026.

EUROPEAN DATA PROTECTION BOARD. 2023 Coordinated Enforcement Action: designation and position of data protection officers. Brussels: EDPB, 2024. Disponível em: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf. Acesso em: 11 set. 2026.

EUROPEAN DATA PROTECTION BOARD. Opinion 28/2025 regarding the European Commission draft implementing decision on the adequate protection of personal data by Brazil. Brussels: EDPB, 4 Nov. 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-11/edpb_opinion_202528_brazil_adequacy_en_0.pdf. Acesso em: 11 set. 2026.

EUROPEAN DATA PROTECTION SUPERVISOR. Decision on the European Commission's use of Microsoft 365. Brussels: EDPS, 8 Mar. 2024. Disponível em: https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf. Acesso em: 11 set. 2026.

EUROPEAN DATA PROTECTION SUPERVISOR. European Commission brings use of Microsoft 365 into compliance with data protection rules for EU institutions and bodies. Brussels: EDPS, 28 July 2025. Disponível em: https://www.edps.europa.eu/system/files/2025-07/2025-07-28_Press-Release_EDPS_Microsoft_EC_in_compliance_EN.pdf. Acesso em: 11 set. 2026.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. GDPR in practice: experiences of data protection authorities. Luxembourg: Publications Office of the European Union, 2024.

FLAHERTY, David H. Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill: University of North Carolina Press, 1989.

INFORMATION COMMISSIONER'S OFFICE. What price privacy? Poor PSNI procedures culminate in £750k fine. Wilmslow: ICO, 3 Oct. 2024a. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/10/what-price-privacy-poor-psni-procedures-culminate-in-750k-fine/. Acesso em: 11 set. 2026.

INFORMATION COMMISSIONER'S OFFICE. Statement on the public sector approach. Wilmslow: ICO, 9 Dec. 2024b. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-

blogs/2024/12/statement-on-the-public-sector-approach/. Acesso em: 11 set. 2026.

INFORMATION COMMISSIONER'S OFFICE. Explaining our approach to the MoD data breach. Wilmslow: ICO, 17 July 2025. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/07/explaining-our-approach-to-the-mod-data-breach/. Acesso em: 11 set. 2026.

IRLANDA. Data Protection Act 2018 (Number 7 of 2018). Dublin: Houses of the Oireachtas, 2018.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (ed.). Technology and privacy: the new landscape. Cambridge, MA: MIT Press, 1997. p. 219-241.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

NATIONAL AUDIT OFFICE. Government cyber resilience. London: NAO, 29 Jan. 2025a. Disponível em: https://www.nao.org.uk/reports/government-cyber-resilience/. Acesso em: 11 set. 2026.

NATIONAL AUDIT OFFICE. Afghanistan Response Route. London: NAO, 3 Sept. 2025b. Disponível em: https://www.nao.org.uk/wp-content/uploads/2025/09/afghanistan-response-route.pdf. Acesso em: 11 set. 2026.

RECORDBOETE voor Belastingdienst vanwege zwarte lijst. NOS, Hilversum, 12 apr. 2022. Disponível em: https://nos.nl/artikel/2424861-recordboete-voor-belastingdienst-vanwege-zwarte-lijst. Acesso em: 11 set. 2026.

REGAN, Priscilla M. Legislating privacy: technology, social values, and public policy. Chapel Hill: University of North Carolina Press, 1995.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia, Luxemburgo, L 119, p. 1-88, 4 maio 2016.

UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União. Jornal Oficial da União Europeia, Luxemburgo, L 295, 21 nov. 2018.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 22 de junho de 2021, Latvijas Republikas Saeima (Pontos de penalidade), processo C-439/19. Luxemburgo, 2021.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Acórdão de 1 de agosto de 2022, Vyriausioji tarnybines etikos komisija, processo C-184/20. Luxemburgo, 2022.

WHITMAN, James Q. The two western cultures of privacy: dignity versus liberty. Yale Law Journal, New Haven, v. 113, n. 6, p. 1151-1221, 2004.

ZWEIGERT, Konrad; KÖTZ, Hein. An introduction to comparative law. 3. ed. Tradução de Tony Weir. Oxford: Clarendon Press, 1998.