Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT3 – Coordenação Interinstitucional e Eficiência Administrativa da ANPD

Relatório Final

Membros:

Rodrigo Borges Valadão (Coordenador)

Ana Paula Moraes Canto de Lima

Rodrigo Badaró Almeida de Castro

Rony Vainzof

Tiago Lopes de Aguiar

Brasília, 02 de junho de 2026

Sumário

Introdução

A instituição da Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) inaugurou um novo paradigma no ordenamento jurídico brasileiro, caracterizado pela transversalidade da proteção de dados pessoais. Diferentemente de diplomas legais setoriais, que regulam verticais específicas da economia ou da administração pública, a LGPD irradia seus efeitos sobre todas as esferas de atividade que envolvam o tratamento de dados pessoais. Essa característica onipresente, contudo, não ocorre em um vácuo normativo. O Estado brasileiro já dispõe de um complexo ecossistema regulatório, composto por agências, autarquias e órgãos de controle com competências consolidadas, muitas das quais tangenciam, interceptam ou, por vezes, colidem com as atribuições da Agência Nacional de Proteção de Dados (ANPD).

Essa pluralidade normativa e regulatória pré-existente, do qual a proteção de dados e a ANPD agora fazem parte, traz um cenário de atuação complexa, onde regras e autoridades supervisoras podem entrar em choque regularmente. De fato, a natureza transversal da proteção de dados exige que a ANPD atue de forma coordenada com outros entes ou órgãos regulatórios setoriais. A ausência de mecanismos formais, perenes e eficientes de cooperação interinstitucional representa um risco sistêmico significativo, uma lacuna que tem o potencial de gerar (a) sobreposições normativas, onde o ente regulado se vê submetido a diretrizes contraditórias emanadas de reguladores distintos, (b) o fenômeno do *bis in idem* administrativo, onde um mesmo fato gerador enseja múltiplas sanções, e, em última análise, (c) uma insegurança jurídica que compromete o ambiente de negócios e a efetiva proteção dos titulares de dados.

O presente Grupo de Trabalho sobre Coordenação Interinstitucional e Eficiência Administrativa (GT3) foi instituído[1] pelo Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) com uma dupla finalidade. A primeira, fornecer à ANPD um diagnóstico claro da sua atual interface regulatória, por meio de entrevistas com seus diretores[2] e de pesquisa documental abrangente, que inclui os modelos de coordenação regulatória (adotados no direito comparado e no direito brasileiro), a revisão da legislação nacional pertinente, os acordos de cooperação (ACTs) já ou não firmados entre a ANPD e outros entes ou órgãos regulatórios federais, publicações oficiais e a análise de casos práticos de intercessão regulatória. A segunda, trazer sugestões para o aprimoramento da sua atuação interinstitucional, otimizando a aplicação da

[1] Portaria CNPD n° 03, de 5 de novembro de 2025. Disponível aqui: https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2a-formacao/2as-grupos-de-trabalho-da-2a-formacao-do-cnpd/portaria_cnpd_gt03_2025.pdf, Acesso em 07 abril 2026

[2] Faz-se necessário, aqui, registrar o agradecimento à Diretora Miriam Wimmer pela disponibilidade em manter um diálogo permanente com o GT3.

LGPD, reforçando a Política Nacional de Proteção de Dados e promovendo a eficiência administrativa e a segurança jurídica no ecossistema regulatório brasileiro.[3]

1. Coordenação Interinstitucional

A crescente complexidade das economias digitais e a interconexão dos mercados têm levado a um cenário de crescente sobreposição de competências entre diferentes órgãos estatais. No Brasil, a coexistência de agências reguladoras setoriais com órgãos de atuação transversal, como o Conselho Administrativo de Defesa Econômica (CADE) e, mais recentemente, a Agência Nacional de Proteção de Dados (ANPD), cria um ambiente propício a conflitos interinstitucionais, mas também a oportunidades de sinergia. A atuação da ANPD, em particular, assemelha-se à do CADE por seu caráter horizontal, perpassando todos os setores da economia que realizam tratamento de dados pessoais, o que a coloca em interface direta com as atribuições de múltiplos reguladores setoriais.

Este documento apresenta uma revisão de literatura jurídica e especializada sobre o tema dos conflitos e da coordenação interinstitucional entre órgãos regulatórios. O objetivo é analisar o arcabouço teórico, os modelos institucionais e os instrumentos de cooperação em âmbito nacional e internacional, a fim de identificar boas práticas e caminhos para aprimorar a articulação entre a ANPD e as demais agências e órgãos reguladores brasileiros. A análise parte do pressuposto de que a ausência de mecanismos de coordenação formalizados pode levar à insegurança jurídica, a decisões conflitantes e à ineficiência regulatória, enquanto a cooperação estruturada pode potencializar a capacidade do Estado de proteger direitos e garantir o bom funcionamento dos mercados e dos setores regulados.

1.1. A Teoria da Sobreposição de Competências Regulatórias

A sobreposição de competências regulatórias (*regulatory overlap*) é um fenômeno inerente à organização administrativa contemporânea, definido como o "uso conjunto de múltiplas

[3] O presente relatório foi elaborado com o auxílio de ferramentas de inteligência artificial generativa, utilizadas como suporte à pesquisa, à organização das informações e à redação inicial dos textos. Todo o conteúdo produzido foi submetido a revisão crítica, substantiva e editorial pelo relator do GT3, que assume integral responsabilidade pelas análises, conclusões e recomendações aqui apresentadas. O uso de IA não substitui nem compromete o juízo técnico e jurídico dos autores. Ao contrário, funcionou como instrumento de produtividade que permitiu maior profundidade analítica no tratamento do tema.

regras legais para abordar uma falha de mercado comum"[4] ou a situação em que múltiplas agências recebem autoridade concorrente para regular um mesmo campo.[5] A literatura especializada apresenta um balanço entre os custos e benefícios desse modelo, cuja resultante depende crucialmente da existência de mecanismos de coordenação.

Por um lado, a sobreposição pode gerar benefícios significativos. A redundância no controle estatal é vista como um mecanismo de resiliência, onde a falha de uma instituição pode ser compensada pela atuação de outra.[6] Adicionalmente, a interação entre órgãos com diferentes expertises fomenta a aprendizagem recíproca, reduz a assimetria de informação entre reguladores e regulados e, crucialmente, diminui o risco de captura regulatória, uma vez que é mais difícil para um grupo de interesse influenciar múltiplas agências independentes.[7]

Por outro lado, a sobreposição desordenada acarreta ineficiência administrativa, com diversas consequências regulatórias indesejadas. A principal delas é a insegurança jurídica, decorrente da possibilidade de coexistirem entendimentos e decisões conflitantes sobre a mesma matéria, o que ofende o princípio da proteção da confiança legítima.[8] Outra consequência diz respeito ao aumento dos encargos de conformidade para os regulados, que precisam navegar em múltiplos regimes, e a ineficiência gerada pela duplicação de esforços e pelo desperdício de recursos públicos.[9]

A síntese teórica aponta que a sobreposição não é intrinsecamente positiva ou negativa. O desafio do desenho institucional não é eliminá-la, mas sim construir um arcabouço robusto de cooperação que maximize as sinergias e mitigue os conflitos, transformando um potencial problema em uma solução para uma regulação mais eficaz e resiliente.

---

[4] TURK, Matthew C. *Overlapping Legal Rules in Financial Regulation and the Administrative State*. *Georgia Law Review*, v. 54, n° 3, 2020, p. 791.
[5] GERSEN, Jacob E. *Overlapping and Underlapping Jurisdiction in Administrative Law*. The Supreme Court Review, v. 2006, p. 201-247, 2006.
[6] BENDOR, Jonathan B. *Parallel Systems: Redundancy in Government*. 2. ed. Berkley: University of California Press, 1985, p. 209 e ss.
[7] SCHILLEMANS, Thomas; BOVENS, Mark. *The Challenge of Multiple Accountability: Does Redundancy Lead to Overload?* In: DUBNICK, Melvin J.; FREDERICKSON, H. George (Ed.). *Accountable Governance: Problems and Promises*. Armonk, NY: M. E. Sharpe, 2011, p. 18 e s.
[8] ARAUJO, Valter Shuenquener de; DIONÍSIO, Pedro de Hollanda. *A sobreposição de órgãos de controle e seus desafios à coordenação dos acordos substitutivos no Brasil*. Revista Quaestio Iuris, v. 16, n° 2, 2023, p. 530 e s. DOI: 10.12957/rqi.2023.64595.
[9] ADMINISTRATIVE CONFERENCE OF THE UNITED STATES. *Recommendation 2012-4, Improving Coordination of Related Agency Responsibilities*. Disponível em: https://www.acus.gov/document/improving-coordination-related-agency-responsibilities, Acesso em 05 abr. 2026

1.2. Modelos Internacionais de Cooperação Interinstitucional

A experiência internacional oferece um repertório valioso de modelos para a gestão da sobreposição regulatória, especialmente no contexto da economia digital. O modelo mais proeminente é o de fóruns permanentes de cooperação, como o *Digital Regulation Cooperation Forum* (DRCF) do Reino Unido. Criado em 2020, o DRCF reúne os quatro principais reguladores britânicos (concorrência, proteção de dados, comunicações e conduta financeira) para promover uma abordagem coerente e proativa na regulação de mercados digitais, operando com base em um plano de trabalho anual e publicando orientações conjuntas, sem suprimir a autonomia de cada membro.[10] Modelo similar foi adotado na Austrália com o *Digital Platform Regulators Forum* (DP-REG).[11]

Nos Estados Unidos, o papel de coordenação regulatória é realizado pelo *Office of Information and Regulatory Affairs* (OIRA). Seu papel central é coordenar, revisar e supervisionar a atividade regulatória do Poder Executivo federal dos Estados Unidos, funcionando como o principal mecanismo de coerência horizontal do Estado regulador norte-americano. O OIRA exerce controle prévio sobre atos normativos relevantes das agências federais independentes e não independentes,[12] avaliando análises de impacto regulatório, custos e benefícios, riscos de sobreposição, inconsistências interagências e compatibilidade com as prioridades presidenciais. Não atua como regulador setorial nem substitui a competência técnica das agências, mas opera como instância de coordenação e racionalização regulatória (*regulatory oversight*), reduzindo duplicidades, conflitos normativos e cargas administrativas excessivas. Assim, o OIRA desempenha função estruturalmente análoga à de um "orquestrador" do sistema regulatório, assegurando coerência sistêmica, eficiência administrativa e previsibilidade jurídica em um ambiente marcado pela pluralidade de autoridades reguladoras.[13]

Na Alemanha, a eficiência regulatória está a cargo do *Nationaler Normenkontrollrat* (NKR), um órgão consultivo independente do governo federal alemão, criado em 2006, com a função específica de avaliar – *ex ante* e *ex post* – os custos regulatórios e os encargos administrativos decorrentes de projetos e atos normativos, bem como se existem alternativas mais sim-

[10] DIGITAL REGULATION COOPERATION FORUM. *About Us*. Disponível em: https://www.drcf.org.uk/about-us. Acesso em 9 dez. 2025.
[11] DIGITAL PLATFORM REGULATORS FORUM. *Joint Statement on the ACCC Digital Platform Services Inquiry 2020-2025.* Disponível em: https://www.accc.gov.au/about-us/media-and-publications/digital-platform-regulators-forum. Acesso em 9 dez. 2025.
[12] Note-se que desde a *Executive Order* n° 12.291/1981), as agências reguladoras independentes eram expressamente excluídas da revisão centralizada do OIRA, que alcançava apenas as agências do Poder Executivo. Essa exclusão só foi alterada pela *Executive Order* n° 14.215, de 18 de fevereiro de 2025 (*Ensuring Accountability for All Agencies*), cuja extensão é até hoje objeto de controvérsia.
[13] Sobre o tema: SUNSTEIN, Cass R. *The Office of Information and Regulatory Affairs: Myths and Realities*. *Harvard Law Review*, v. 126, 2013. Disponível em: https://papers.ssrn°com/sol3/papers.cfm?abstract_id=2192639. Acesso em 9 dez. 2025.

ples ou eficientes para atingir os mesmos objetivos regulamentares. Seu foco está na mensuração do impacto burocrático da legislação sobre cidadãos, empresas e a própria Administração Pública, atuando como instância técnica de racionalização normativa. O NKR não exerce coordenação interministerial nem possui poder de veto ou revisão material do conteúdo regulatório; sua atuação limita-se à análise de impactos e à emissão de pareceres não vinculantes. Desde 2023, seu mandato foi ampliado para incluir o chamado *Digital-Check*, que verifica se os ministérios consideraram desde a fase de elaboração a possibilidade de implementação digital das normas, favorecendo o uso de soluções eletrônicas e reduzindo procedimentos burocráticos. Trata-se, portanto, de um mecanismo de *better regulation* voltado à eficiência administrativa, e não de um órgão de coordenação regulatória sistêmica nos moldes do OIRA.[14]

1.3. Regime Jurídico Brasileiro

No direito brasileiro, ainda não há um órgão público ou estruturas administrativas que façam a coordenação entre órgãos regulatórios, aos moldes do direito comparado.[15] Na experiência nacional, destaca-se o Programa de Fortalecimento da Capacidade Institucional para Gestão em Regulação (PRO-REG), originalmente instituído pelo Decreto n° 6.062, de 16 de março de 2007 como um programa voltado ao fortalecimento da capacidade institucional do Estado regulador brasileiro. Seu foco principal era a qualificação técnica das agências reguladoras, a difusão de boas práticas regulatórias e a introdução de instrumentos como a Análise de Impacto Regulatório. Tratava-se de um mecanismo de *capacity building*, sem competências decisórias ou de coordenação vinculante. Ao longo da década de 2010, o PRO-REG perdeu centralidade política e operacional, sobretudo com a consolidação de instrumentos regulatórios previstos em legislações específicas. A aprovação da Lei n° 13.848, de 25 de junho de 2019 (Lei Geral das Agências Reguladoras) contribuiu para deslocar parte de suas funções para um marco legal próprio, gerando o esvaziamento do Decreto n° 6.062, de 16 de março de 2007 (PRO-REG) e sua posterior revogação pelo Decreto n° 11.738, de 18 de outubro de 2023.

Em 2023, o PRO-REG foi recriado por meio do Decreto n° 11.738, de 18 de outubro de 2023, com novo desenho institucional.[16] O foco do programa foi deslocado da mera coordenação interinstitucional para o apoio ativo à implementação de boas práticas regulatórias, como

[14] Sobre o tema: NATIONALER NORMENKONTROLLRAT. *Gute Gesetze, digitale Verwaltung und weniger Bürokratie*. Disponível em: https://www.normenkontrollrat.bund.de/Webs/NKR/DE/der-nkr/aufgabe/aufgabe_node.html. Acesso em 9 dez. 2025.

[15] ESPÍRITO SANTO, Paulo André. *A cooperação entre a autoridade antitruste e as agências reguladoras nos mercados setoriais: critérios e formas*. São Paulo: JusPodivm, 2025, p. 115.

[16] Decreto n° 6.062, de 16 de março de 2007 (instituição original do PRO-REG), disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6062.htm e Decreto n° 11.738, de 18 de outubro de 2023 (recriação do programa), disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11738.htm. Acesso em 2 jun. 2026.

a Análise de Impacto Regulatório (AIR). A abrangência foi significativamente expandida, passando a englobar não apenas as agências, mas toda a administração pública federal direta, autárquica e fundacional. A nova arquitetura institucional transferiu a coordenação para o Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC) e extinguiu o Comitê Consultivo, substituindo-o por um Comitê Gestor mais robusto e com representação de órgãos estratégicos de controle e de governo, como a Advocacia-Geral da União (AGU) e a Controladoria-Geral da União (CGU).

A principal diferença entre os dois PRO-REGs reside na natureza e ambição institucional. O PRO-REG de 2007 era voltado prioritariamente às agências reguladoras, enquanto o de 2023 adota uma perspectiva mais sistêmica e processual, abrangendo ministérios e demais órgãos normativos. Do ponto de vista institucional, o PRO-REG – em qualquer das suas versões – apresenta limites claros quando comparado a modelos de supervisão regulatória centralizada, como o *Office of Information and Regulatory Affairs* (OIRA) norte-americano. O programa não exerce revisão prévia obrigatória de atos normativos, não possui poder de veto ou de harmonização vinculante e não atua como instância decisória para resolução de conflitos regulatórios. Seu papel é predominantemente indutivo e pedagógico, refletindo uma opção brasileira por um modelo de coordenação baseado em *soft law*, capacitação e alinhamento metodológico, mais compatível com a estrutura constitucional descentralizada da Administração Pública, mas também menos eficaz para lidar com conflitos interinstitucionais complexos e sobreposições regulatórias persistentes.

Outro mecanismo de coordenação interinstitucional está previsto na Lei n° 13.848, de 25 de junho de 2019 (Lei Geral das Agências Reguladoras), em seu Capítulo IV, que estabelece mecanismos de articulação entre as agências setoriais e o CADE. Os artigos 26 a 29 preveem a solicitação de pareceres técnicos, a comunicação de indícios de infração à ordem econômica e a possibilidade de edição de atos normativos conjuntos.[17] Embora represente um avanço, a lei não prevê um mecanismo formal de resolução de conflitos e não contêm qualquer previsão de atuação coordenada das agências reguladoras setoriais e a Agência Nacional de Proteção de Dados (ANPD).[18]

Além desses instrumentos, existem outras formas de coordenação interinstitucional, embora previstos de forma fragmentada e nem sempre com a devida densidade normativa. Uma dessas iniciativas é a Associação Brasileira de Agências Reguladoras (ABAR), fundada em

[17] Artigos 26 a 29 da Lei n° 13.848, de 25 de junho de 2019, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13848.htm. Acesso em 2 jun. 2026.

[18] A experiência do CADE na gestão de suas interfaces com as agências setoriais, acumulada ao longo de décadas e consolidada na Lei 13.848/2019, oferece um aprendizado valioso para a ANPD. Ambas as autoridades enfrentam o desafio de aplicar uma norma geral (Lei de Defesa da Concorrência ou LGPD) em contextos setoriais específicos, que possuem lógicas e regulações próprias. A necessidade de balancear os objetivos da política transversal (concorrência ou proteção de dados) com os objetivos da política setorial (universalização, modicidade tarifária, segurança institucional etc.) é um desafio comum que reforça a necessidade de diálogo e cooperação.

8 de abril de 1999. Trata-se de uma entidade de direito privado, criada sob a forma de associação civil, sem fins lucrativos e de natureza não partidária. Seu objetivo é promover a mútua colaboração entre as agências associadas e os poderes públicos, na busca do aprimoramento da regulação e da capacidade técnica, contribuindo para o avanço e consolidação da atividade regulatória em todo Brasil. Embora a ANPD tenha sido transformada em Agência Reguladora pela Medida Provisória n° 1.317, de 17 de setembro de 2025[19], ela ainda não consta, até a data de fechamento deste relatório, nos quadros associativos da ABAR.[20]

Outro importante instrumento de cooperação regulatório interinstitucional é o Fórum das Agências Reguladoras, oficialmente denominado Comitê das Agências Reguladoras Federais (COARF).[21] Trata-se de um arranjo interinstitucional entre agências reguladoras federais voltado à troca de experiências, ao alinhamento de práticas e à defesa de pautas comuns relacionadas à autonomia, capacidade institucional e qualidade regulatória. Na sua origem, era uma instância reservada aos dirigentes das agências reguladoras federais,[22] mas por meio da Resolução Normativa Conjunta n° 1, de 16 de junho de 2023,[23] foi transformada em um espaço permanente de diálogo entre diretores e servidores de onze autarquias federais (ANA, ANAC, ANCINE, ANEEL, ANM, ANP, ANS, ANATEL, ANTAQ, ANTT e ANVISA), com ênfase em transparência, participação social e *accountability* e com a finalidade de fortalecer a atuação técnica e institucional junto ao governo, Congresso, TCU e sociedade. Até a data de fechamento deste relatório, não há notícia da integração da ANPD nesse órgão.

Por fim, não se pode esquecer que a LGPD, em seu artigo 55-J – e especialmente seus §§ 3º e 4º, atribui à ANPD o dever de coordenar sua atuação com outros entes e órgãos regulatórios, posicionando-a como o órgão central de coordenação do ecossistema brasileiro de proteção de dados pessoais. Não se trata de uma relação de hierarquia ou subordinação, mas de um mandato para que a ANPD atue como o ponto focal e o motor da articulação interinstitucional. Cabe à ANPD, portanto, a iniciativa de convocar os demais órgãos, propor os instrumentos de cooperação e liderar a construção de uma interpretação uniforme e coerente da LGPD em todos os setores.

---

[19] Medida Provisória n° 1.317, de 17 de setembro de 2025 (publicada no Diário Oficial da União em 18 set. 2025), que inseriu a ANPD no rol das agências reguladoras regidas pela Lei n° 13.848/2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Mpv/mpv1317.htm. Acesso em 2 jun. 2026. Conversão realizada pela Lei nº 15.352, de 24 de fevereiro de 2026.

[20] Vide: https://abar.org.br/quem-somos/, com acesso em 10 dez 2025.

[21] O principal fundamento deste Fórum é o artigo 30 da Lei das Agências Reguladoras. Confira-se a sua redação: "As agências reguladoras poderão constituir comitês para o intercâmbio de experiências e informações entre si ou com os órgãos integrantes do Sistema Brasileiro de Defesa da Concorrência (SBDC), visando a estabelecer orientações e procedimentos comuns para o exercício da regulação nas respectivas áreas e setores e a permitir a consulta recíproca quando da edição de normas que impliquem mudanças nas condições dos setores regulados."

[22] Fórum de Dirigentes das Agências Reguladoras Federais (FDAR)

[23] O referido documento normativo pode ser encontrado aqui: https://www.in°gov.br/en/web/dou/-/resolucao-normativa-conjunta-n-1-de-16-de-junho-de-2023-523226833, Acesso em 07.01.26

Esse papel de coordenação central é indispensável para evitar a fragmentação regulatória. Se cada agência setorial passasse a interpretar e aplicar a LGPD de forma autônoma e isolada, o resultado seria um mosaico de regimes de proteção de dados, com diferentes níveis de exigência e obrigações por vezes contraditórias, anulando o propósito unificador da Lei Geral. A ANPD, como guardiã da LGPD, tem o dever de garantir a consistência e a integridade da política nacional de proteção de dados, e o exercício de seu papel de coordenação é o principal meio para atingir esse fim.

Tabela 1: Principais Competências da ANPD por Eixo Temático

Eixo Temático	Competências Relevantes (Art. 55-J, LGPD)
Regulação e Normatização	**III** - editar regulamentos e procedimentos; **X** - elaborar estudos sobre práticas; **XIII** - editar normas e orientações; **XVIII** - garantir que o tratamento seja feito de forma transparente; **XX** - editar normas sobre Relatório de Impacto à Proteção de Dados Pessoais
Fiscalização e Sanção	**IV** - zelar pela proteção de dados pessoais; **V** - deliberar sobre a interpretação da LGPD; **XVI** - fiscalizar e aplicar sanções; **XXIV** - realizar auditorias
Supervisão do Poder Público	**XI** - requisitar informações de entidades do poder público; **XXII** - preservar o segredo comercial e industrial
Cooperação Internacional	**IX** - comunicar às autoridades competentes as infrações e medidas administrativas aplicadas; **XXI** - dispor sobre padrões de interoperabilidade

Resolução de Conflitos	**XVII** - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante; celebrar compromissos e acordos
Educação e Orientação	**VIII** - promover ações de conscientização; **XII** - elaborar relatórios de gestão; XIV - comunicar-se com o público
Articulação Interinstitucional	**XXIII** - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; **Art. 55-J, § 3º, LGPD:** A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. **Art. 55-J, § 4º, LGPD:** A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

2. Instrumentos de Coordenação

A compreensão das tensões entre a ANPD e os reguladores setoriais exige uma base teórica sólida sobre o funcionamento do Estado Regulador na era digital. A proteção de dados não é uma disciplina isolada; ela é um elemento constitutivo da prestação de serviços contemporâneos. Não há telecomunicações, serviços financeiros, saúde suplementar ou distribuição de energia elétrica inteligente sem o tratamento massivo de dados pessoais.

A ANPD detém a competência primária e exclusiva para interpretar a LGPD e zelar pelo seu cumprimento. No entanto, a regulação setorial frequentemente impõe obrigações de tratamento de dados que precedem a própria existência da ANPD. O desafio hermenêutico reside na aplicação do critério da especialidade. Enquanto a ANPD é a autoridade *geral* em dados, mas *especialista* na proteção da personalidade, a agência setorial é a autoridade *geral* no setor, mas *especialista* na regulação técnica do serviço ou produto disponibilizado no mercado.

A transversalidade da atuação da ANPD gera uma possibilidade elevada sobreposição regulatória. Ela ocorre quando a regulação técnica do serviço implica, necessariamente, uma forma específica de tratamento de dados que pode estar em desacordo com os princípios de minimização ou necessidade da LGPD. Por exemplo, normas de segurança pública que exigem a retenção indiscriminada de logs de conexão conflitam com a privacidade; normas de transparência bancária podem conflitar com o sigilo de dados.

A gestão eficaz da sobreposição de competências regulatórias exige a utilização de um portfólio diversificado de instrumentos de coordenação, que podem variar em grau de formalidade, intensidade e propósito. A experiência nacional e internacional demonstra que não há uma solução única, mas sim uma combinação de ferramentas que, utilizadas de forma estratégica, podem mitigar conflitos, otimizar recursos e aumentar a coerência e a qualidade da regulação. A seguir, detalham-se os principais instrumentos aplicáveis à coordenação entre a ANPD e os demais órgãos e entidades da Administração Pública.

.

2.1. Acordos de Cooperação Técnica (ACTs)

O dever de coordenação, decorrência do princípio da eficiência administrativa[24] e previsto na LGPD,[25] materializa-se na prática por meio de atuações conjuntas que visam mitigar sobreposições normativas e garantir a segurança jurídica. A formalização de Acordos de Cooperação Técnica (ACTs) representa o nível mais elevado de maturidade na coordenação interinstitucional. Por meio desses acordos, é possível que os agentes reguladores estabeleçam fluxos contínuos de diálogo, compartilhamento de informações e harmonização de entendimentos antes que conflitos regulatórios se agravem.

Exatamente por isso, o ACT é o instrumento formal mais comum para iniciar e estruturar a colaboração entre órgãos públicos no Brasil. Regulamentados pelo Decreto n° 11.531, de 16 de maio de 2023, os ACTs estabelecem um arcabouço jurídico para o compartilhamento de informações, a realização de estudos e fiscalizações conjuntas, bem como para o intercâmbio de pessoal. Para serem efetivos, devem ir além de declarações genéricas, estabelecendo regras

[24] Art. 37, *caput* da Constituição da República.
[25] Art. 55-J, §3°.

claras para a troca de informações (especialmente confidenciais), procedimentos de consulta, mecanismos de coordenação de investigações e, crucialmente, planos de trabalho detalhados com metas, produtos e cronogramas.

Um ponto crucial levantado pela ANPD é a limitação de um fórum amplo para tratar de temas sensíveis, como as atividades de fiscalização e sancionamento. Devido às restrições legais de sigilo, a troca de informações em processos investigativos não poderia ocorrer em um ambiente coletivo e aberto. Para a ANPD, a cooperação em matéria de *enforcement* continuará a depender de instrumentos bilaterais, como os Acordos de Cooperação Técnica (ACTs). Esses acordos oferecem a segurança jurídica necessária para o compartilhamento de informações sigilosas e para a coordenação de atuações específicas em processos sancionadores.

De acordo com a Diretora Miriam Wimmer, os ACTs desempenham um papel essencial no modelo de governança de múltiplos nível adotado pela ANPD. No *nível estratégico-regulatório*, eles facilitam a coordenação para uniformização de teses e entendimentos normativos, principalmente em fóruns e comitês já existentes, onde a pauta de proteção de dados seria integrada. No *nível operacional-fiscalizatório*, por sua vez, eles garantem a confidencialidade e a segurança jurídica necessárias na cooperação em atividades de fiscalização, investigação e sancionamento.

Desde a sua criação (2019), a ANPD já firmou ACTs com os seguintes agentes reguladores: a) Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae); b) Agência Nacional de Mineração (ANM); c) Secretaria Nacional do Consumidor (SENACON); d) Conselho Administrativo de Defesa Econômica (CADE); e) Núcleo de Informação e Coordenação do Ponto BR (NIC.br); f) Tribunal Superior Eleitoral (TSE); g) Controladoria-Geral da União (CGU); h) Controladoria-Geral do Estado de Minas Gerais (CGE/MG); i) Agência Nacional de Saúde Suplementar (ANS); e j) Agência Nacional de Transportes Aquáticos (ANTAQ).[26] Embora essenciais para dar segurança jurídica à cooperação, estudos demonstram que a mera existência de um ACT é insuficiente para garantir sua efetividade. A cooperação bem-sucedida depende criticamente de planos de trabalho detalhados, indicadores de desempenho e, sobretudo, do engajamento e da confiança mútua entre as equipes técnicas. De qualquer forma, esse é o instrumento que mais vem sendo utilizado pela ANPD para coordenar suas atividades com outras agências ou órgãos reguladores.

[26] Essa lista e os respectivos documentos podem ser encontrados aqui: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 11 mar 2026.

2.2. Diretrizes e Orientações Conjuntas

A emissão de diretrizes, guias ou orientações conjuntas (*joint guidelines*) é uma ferramenta poderosa para harmonizar a interpretação de normas e reduzir a insegurança jurídica para os regulados. Quando a ANPD e uma agência setorial publicam um documento conjunto sobre como a LGPD se aplica a um determinado setor (por exemplo, o tratamento de dados de saúde em conjunto com a ANS e a ANVISA), elas fornecem clareza, previsibilidade e evitam o risco de decisões conflitantes, harmonizando suas interpretações e sinalizando uma abordagem unificada. Este instrumento é particularmente útil para endereçar as chamadas "zonas cinzentas", onde a interação entre a norma geral de proteção de dados e a regulação setorial é mais complexa.[27]

Nesse particular, devem ser mencionadas três iniciativas. A primeira foi a publicação, em 10 de setembro de 2021, da cartilha "*Como proteger seus dados pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON*".[28] O seu objetivo declarado é orientar e conscientizar os consumidores sobre a proteção de seus dados pessoais, especialmente no contexto da LGPD, além de indicar como agir em caso de violação de dados. Entre os conhecimentos que constam do guia, estão esclarecidas as situações em que é possível realizar o tratamento de dados pessoais, quais informações são necessárias para tal e quem pode realizar esse tratamento, além de orientar o consumidor sobre o que deve ser feito em caso de violação que envolva o compartilhamento indevido de dados.

A segunda iniciativa foi a publicação, em 21 de julho de 2021, de dois fascículos da "Cartilha de Segurança para Internet" elaborados em parceria com o NIC.br/CERT.br.[29] O objetivo declarado do primeiro fascículo (sobre "Proteção de Dados") é orientar os usuários a adotar postura preventiva, reduzir a exposição indevida de informações, utilizar ferramentas de segurança e recorrer à legislação e aos canais institucionais quando necessário, ao passo que o segundo fascículo (sobre "Vazamento de Dados") busca oferecer orientações para a mitigação de prejuízos e para a adoção de medidas rápidas diante de incidentes de exposição indevida de dados. Em conjunto, esses materiais têm função eminentemente educativa e preventiva, pois difundem noções práticas de proteção de dados pessoais, esclarecem medidas de autoproteção

[27] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf, Acesso em 17 mar 2026.
[28] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/autoridade-nacional-de-protecao-de-dados-e-secretaria-nacional-do-consumidor-lancam-201ccomo-proteger-seus-dados-pessoais201d?utm_source=chatgpt.com, Acesso em 17 mar 2026.
[29] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/programas-projetos-acoes-obras-e-atividades/semana-da-protecao-de-dados-2022/sabe-qual-a-importancia-dos-acordos-de-cooperacao-tecnica-e-dos-guias-orientativos-feitos-pela-anpd, Acesso em 17 mar 2026

digital e reforçam a cultura de segurança da informação e de conscientização sobre direitos relacionados à LGPD.

Por fim, a publicação, no dia 3 de janeiro de 2022, do *"Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral"*,[30] em conjunto com o TSE, um documento que destaca a relevância prática da proteção de dados no ambiente eleitoral. A cartilha enfatiza que, no contexto da globalização e da cultura digital, a dinâmica do processo eleitoral passou a depender de fluxos informacionais mais intensos e complexos, elevando a necessidade de conformidade com a LGPD. Nesse cenário, a migração das campanhas do rádio, TV e materiais impressos para redes sociais e aplicativos de mensagens ampliou o tratamento massivo de dados pessoais, redefinindo as formas de engajamento social com as eleições.

2.3. Comissões de Resolução de Conflitos

Quando os instrumentos de cooperação interinstitucional (acordos, grupos de trabalho, orientações conjuntas) não são suficientes para prevenir ou superar divergências de competência — típicas de ambientes regulatórios com atribuições transversais e setoriais — torna-se recomendável que exista um mecanismo pré-definido, procedimentalizado e tecnicamente orientado para dirimir impasses, antes que eles se convertam em litigância estratégica ou em judicialização em massa. Esse tipo de arranjo reduz incertezas, evita "decisões concorrentes" entre órgãos do Estado e favorece previsibilidade para os regulados, ao transformar conflitos em um fluxo administrativo estruturado, com prazos, contraditório e motivação. Um precedente relevante no Brasil é a Resolução Conjunta n° 2, de 27 de março de 2001,[31] por meio da qual ANEEL, ANATEL e ANP aprovaram um regulamento conjunto de resolução administrativa de conflitos e instituíram uma Comissão permanente, com dois representantes de cada Agência e formação variável conforme os setores envolvidos (composição "tripartite" adaptada ao caso concreto). Até o momento do fechamento deste relatório, não há qualquer notícia sobre a utilização deste instrumento pela ANPD.

2.4. Grupos de Trabalho

A criação de grupos de trabalho temáticos (e.g. *open finance*, saúde digital etc.) permitiria uma troca técnica mais aprofundada e contínua da ANPD com outros órgãos reguladores

[30] Vide: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_lgpd_final.pdf, Acesso em 07 jan 2026

[31] Vide: https://informacoes.anatel.gov.br/legislacao/resolucoes/resolucoes-conjuntas/85-resolucao-conjunta-2, Acesso em 07 jan 2026

setoriais, permitindo o compartilhamento estruturado de evidências, metodologias e experiências regulatórias, além de viabilizar a formação de expertise conjunta em domínios de alta complexidade e rápida evolução. Esses grupos podem funcionar, por exemplo, como motor operacional dos fóruns permanentes, porque traduzem objetivos amplos de coordenação em planos de trabalho, entregas verificáveis e rotinas de acompanhamento (prazos, responsabilidades, validação e registro de decisões). Por meio dessa dinâmica, a ANPD poderia fortalecer sua atuação transversal ao harmonizar entendimentos e reduzir assimetrias regulatórias, produzindo entregas concretas – como guias, notas técnicas, recomendações e modelos de procedimento – que aumentam a previsibilidade para os agentes de tratamento e diminuem o risco de conflitos de competência e judicialização.

2.5. Comitês Permanentes

Como já demonstrado acima, o Brasil não consolidou um órgão interinstitucional com funções decisórias e vinculantes. A experiência nacional mais relevante é o PRO-REG, seja na sua versão original (Decreto n° 6.062, de 16 de março de 2007), seja na sua versão atual (Decreto n° 11.738, de 18 de outubro de 2023), que redesenha o programa para apoiar ativamente a implementação de boas práticas regulatórias (com destaque para a AIR) e amplia significativamente seu alcance para abranger toda a Administração Pública federal direta, autárquica e fundacional. Ainda assim, mesmo após 2023, o PRO-REG permanece distante de modelos internacionais, pois não realiza revisão prévia obrigatória de atos normativos, não dispõe de poder de veto e não opera como instância decisória para resolver impasses jurisdicionais, mantendo um perfil predominantemente pedagógico e de *soft law* para coordenação regulatória.

Note-se que o artigo 55-J, § 4º da LGPD determina que a ANPD "manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD." Inspirado no DRCF britânico, o fórum da ANPD deve ter um regimento interno, um plano de trabalho anual e a capacidade de publicar produtos concretos, servindo como o principal *hub* de coordenação da política de proteção de dados no país. Até o momento, não há notícias sobre a criação deste Fórum Permanente pela ANPD.

Durante a entrevista com representantes da ANPD, a Diretora Miriam Wimmer expressou um certo ceticismo quanto à criação do Fórum Permanente, previsto pela LGPD. Esse ceticismo não decorre de uma discordância sobre a necessidade de operacionalização do comando normativo, mas sim pela sua potencial inefetividade, o que levaria a uma ofensa ao princípio da efetividade administrativa, previsto pelo artigo 37, *caput* da Constituição da República. A uma, porque, dada a natureza transversal da ANPD com o escopo de atuação das demais entidades e

órgãos regulatórios, haveria um (natural) baixo interesse na adesão dessa instância coletiva por parte dos agentes setoriais. A duas, porque a criação de mais um colegiado fatalmente iria gerar uma estrutura burocrática duplicada, com baixa efetividade. Por isso, depois de muitas conversas internas, a ANPD adotou uma solução mais ágil e inteligente: o aproveitamento de instâncias de governança já existentes, ao invés de criar mais uma instância coletiva do zero. De fato, ao invés de criar mais uma camada burocrática – que, provavelmente, iria dificultar, em vez de facilitar, a cooperação –. a inserção da pauta da proteção de dados em comitês e fóruns interministeriais ou corregulatórios já operantes pode trazer resultados mais eficazes em múltiplos espaços já consolidados, dependendo do tema em discussão.

2.6. Intercâmbio de Pessoal

Outro instrumento interessante é intercâmbio temporário de servidores da ANPD com autoridades setoriais e órgãos de controle (*staff exchanges* ou *secondments*), que pode funcionar como instrumento de capacitação aplicada, permitindo que suas equipes compreendam, com maior granularidade, os processos, riscos e estruturas decisórias dos setores regulados que tratam intensivamente dados pessoais. Além de favorecer a transferência bidirecional de conhecimento técnico (por exemplo, metodologias de fiscalização, gestão de incidentes, auditoria e avaliação de impacto), esse arranjo fortalece redes de contato e relações de confiança indispensáveis para respostas coordenadas e tempestivas em casos complexos. Ao reduzir a lógica de "silos" institucionais, a ANPD poderia a ganhar em coerência regulatória e efetividade de *enforcement*, harmonizando entendimentos e diminuindo fricções que frequentemente resultam em sobreposição de atuações e judicialização.

2.7. *Sandboxes* Regulatórios

O último instrumento da nossa lista é o *sandbox* regulatório. Esse ambiente poderia funcionar não apenas como um instrumento de fomento à inovação, mas também como um ambiente de coordenação supervisionada em que se testam, com rastreabilidade e salvaguardas, rotinas de cooperação com reguladores setoriais (por exemplo, em projetos de *healthtech*, *open finance* ou IA aplicada à saúde).[32] Nesse desenho, o valor central para a ANPD é transformar casos-piloto em protocolos replicáveis (fluxos de supervisão conjunta, critérios de risco, deveres de transparência e parâmetros de responsabilização), prevenindo falhas e reduzindo incertezas antes da regulação de escopo geral. Para garantir segurança jurídica na implementação

[32] A própria ANPD descreve o sandbox como uma "experimentação colaborativa" em ambiente controlado, na qual pode haver flexibilização orientativa de requisitos, com vistas a produzir aprendizado regulatório e calibrar a resposta institucional a tecnologias disruptivas. Vide: https://www.gov.br/anpd/pt-br/assuntos/projetos-acoes-iniciativas/sandbox/o-sandbox-regulatorio, Acesso em 07 jan 2026.

de *sandboxes* regulatórios no Brasil, o artigo 11 da Lei Complementar n° 182, de 1º de junho de 2021, instituiu que "órgãos e as entidades da administração pública com competência de regulamentação setorial poderão, individualmente ou em colaboração, no âmbito de programas de ambiente regulatório experimental (*sandbox* regulatório), afastar a incidência de normas sob sua competência em relação à entidade regulada ou aos grupos de entidades reguladas".

Em diferentes países, Autoridades Supervisoras de Proteção de Dados (APDs) vêm estruturando iniciativas de sandbox regulatório voltadas especificamente à privacidade. No Reino Unido,[33] o *Information Commissioner's Office* (ICO) inaugurou, em 2019, um programa orientado a apoiar projetos na incorporação de proteção de dados desde a concepção (*data protection by design*). Em Singapura, a *Personal Data Protection Commission* (PDPC) desenvolveu, em parceria com a *Infocomm Media Development Authority* (IMDA), um sandbox iniciado em 2017 com a finalidade de promover aprendizado regulatório e subsidiar a modernização do regime nacional de proteção de dados,[34] e, posteriormente, em julho de 2022, as duas instituições lançaram uma nova iniciativa concentrada no desenvolvimento e no uso de *Privacy Enhancing Technologies* (PETs).[35] No Brasil, alguns programas setoriais ilustram mecanismos interessantes: a CVM[36] prevê autorizações temporárias acompanhadas de dispensas regulatórias para viabilizar testes, enquanto a SUSEP[37] organiza seu sandboxes com base em atos normativos próprios. Em 2023, a ANPD[38] abriu consulta para um *sandbox* de IA e proteção de dados, sinalizando uma abordagem estruturada para colher subsídios e orientar eventual regulação, justamente em um domínio de forte sobreposição regulatória.

Como exemplo de precedente brasileiro em matéria de coordenação regulatória, é importante registrar o Comunicado Conjunto de 13 de junho de 2019,[39] em que Ministério da Economia, Banco Central, CVM e SUSEP declararam intenção de implantar sandboxes no Brasil e afirmaram que coordenariam atividades e buscariam atuar conjuntamente quando as iniciativas "perpassem mais de um mercado regulado". Até o presente momento, não há noticias de

---

[33] Vide: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/?utm_source=chatgpt.com, Acesso em 12 jan 2026

[34] Vide: https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox?utm_source=chatgpt.com, Acesso em 12 jan 2026

[35] Vide: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/speeches/2017/personal-data-protection-seminar-2017?utm_source=chatgpt.com, com acesso em 12 jan 2026

[36] Vide: Resolução CVM n° 29, de 11 de maio de 2021. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol029.html, Acesso em 12 jan 2025

[37] Vide: Resolução CNSP n° 381, de 4 de março de 2020. https://www.in°gov.br/en/web/dou/-/resolucao-n-381-de-4-de-marco-de-2020-246507718, Acesso em 12 jan 2026; e Circular SUSEP n° 598, de 19 de março de 2020, https://www.in°gov.br/en/web/dou/-/circular-n-598-de-19-de-marco-de-2020-249021945, Acesso em 12 jan 2026.

[38] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/publicado-edital-para-participacao-em-sandbox-regulatorio-em-inteligencia-artificial, Acesso em 12 jan 2026.

[39] Vide: https://www.gov.br/cvm/pt-br/assuntos/noticias/2019-1/comunicado-conjunto-de-13-de-junho-de-2019-8dd7407271404b5ebe04f5150d3aa36c, Acesso em 12 jan 2026.

instalação de sandboxes regulatórios da ANPD em parcerias com outras agências ou órgãos regulatórios. Em um ambiente controlado, a ANPD e uma agência setorial poderiam testar modelos de cooperação e supervisão conjunta de novas tecnologias (e.g. *openfinance, healthtechs* etc.), aprendendo a trabalhar juntas antes de aplicar as lições em regulação de escopo geral. Aliás, um estudo da própria ANPD sobre o tema reconhece a necessidade de "coordenação das flexibilizações entre as diferentes autoridades envolvidas"[40] em sandboxes multissetoriais.

3. Atuação Interinstitucional

A consolidação da ANPD não pode ser compreendida apenas como um processo de produção normativa ou desenvolvimento estrutural, mas, também, como o seu posicionamento como uma autoridade transversal, cuja efetividade depende da sua capacidade de articulação com outros órgãos e entidades estatais, notadamente aqueles que exercem função regulatória. Desde o seu planejamento estratégico inicial, a ANPD vinculou o fortalecimento da cultura de proteção de dados não apenas à edição de normas, à fiscalização e à orientação, mas também "à promoção do diálogo com entidades governamentais e não governamentais, com vistas à construção de parcerias estratégicas", à atuação conjunta e à incorporação de melhores práticas.[41] Nessa perspectiva, a atuação interinstitucional não constitui elemento acessório de sua trajetória institucional, mas dimensão estrutural do próprio modo pelo qual a ANPD busca cumprir sua missão de zelar pela proteção dos dados pessoais e afirmar-se como órgão de referência nacional e internacional na matéria.

Essa centralidade da articulação institucional torna-se ainda mais evidente quando se observa que a proteção de dados pessoais, por sua própria natureza, incide de modo transversal sobre setores regulados por múltiplas autoridades públicas. O relatório do GT3 identifica, precisamente, que a ANPD desenvolveu uma visão pragmática, segundo a qual a coordenação com reguladores setoriais e órgãos de controle deve priorizar matérias finalísticas – especialmente normatização, fiscalização e harmonização interpretativa –, evitando que a cooperação se reduza a iniciativas periféricas ou meramente capacitadoras. Foi nesse contexto que a celebração de ACTs com entes como SENACON, CADE, CGU, TSE e ANS passou a funcionar como instrumento de ordenação institucional da aplicação da LGPD, buscando prevenir sobreposições indevidas, reduzir insegurança jurídica e transformar potenciais conflitos de competência em complementaridade funcional.

---

[40] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Sandbox Regulatório: Estudo Técnico*. Versão pública. 2023, p. 10. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sandbox_regulatorio__estudo_tecnico__versao_publica_.pdf. Acesso em 12 jan. 2026.

[41] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Planejamento Estratégico 2021-2023*. 2021, p. 6. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-anpd-2021-2023. Acesso em 26 mar. 2026.

As agendas regulatórias da ANPD, por sua vez, revelam que esse esforço de coordenação não se limita à gestão de casos concretos, mas integra um processo mais amplo de amadurecimento institucional. Desde a agenda 2021-2022, a ANPD passou a organizar suas prioridades regulatórias de forma progressiva e monitorável, vinculando-as à formulação das diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade.[42] No ciclo seguinte (2025-2026), embora não haja uma atenção específica à interinstitucionalidade regulatória, observa-se a incorporação de temas que, por sua natureza, exigem interlocução intensa com outros órgãos públicos, como compartilhamento de dados pelo Poder Público, diretrizes para a política nacional, inteligência artificial e tratamento de dados de alto risco.[43] Assim, a atuação interinstitucional da ANPD deve ser lida como expressão de uma governança em rede: uma autoridade que, sem renunciar a sua centralidade interpretativa na LGPD, depende crescentemente de mecanismos estáveis de cooperação para assegurar coerência regulatória, eficiência administrativa e proteção efetiva dos titulares de dados.

3.1. Estratégia Adotada

Para subsidiar os trabalhos deste GT, foi realizada, em 05 de dezembro de 2025, uma reunião estratégica com representantes da ANPD, com o objetivo de colher a sua visão sobre o estado atual e o futuro da coordenação interinstitucional. A análise a seguir apresenta e consolida as percepções, estratégias e preocupações expressas pela ANPD durante o encontro, fornecendo um panorama robusto da sua perspectiva para a construção de um ecossistema regulatório coeso e eficiente. A visão da ANPD sobre a matéria pode ser caracterizada por um pragmatismo calculado. Longe de uma abordagem casuística, foi evidenciado que a ANPD possui um plano bem definido – apesar de não-formalizado – para guiar suas relações interinstitucionais, ao mesmo tempo em que expressa ceticismo em relação a "soluções" que, ao invés de potencializar a sinergia regulatória, acabem gerando apenas mais burocracia.

Nessa reunião, a representante da ANPD, Diretora Miriam Wimmer, enfatizou que a celebração de ACTs seguiu, desde a sua criação, uma lógica estratégica e não aleatória. A escolha dos primeiros parceiros institucionais foi cuidadosamente calculada para endereçar os desafios mais urgentes daquele momento inicial. Essa abordagem direcionada teve como objetivo construir uma base sólida para a futura atuação da ANPD, estabelecendo desde cedo seu papel central no complexo cenário regulatório brasileiro, em matéria de proteção de dados pessoais. Na

[42] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Planejamento Estratégico 2021-2023*. 2021, p. 6. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-anpd-2021-2023. Acesso em 26 mar. 2026.
[43] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Planejamento Estratégico 2024-2027*. 2024, p. 13. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-2024-2027. Acesso em 26 mar. 2026.

visão da ANPD, a clareza dessa estratégia inicial foi fundamental para posicioná-la como um ator central na governança de dados do país.

O princípio fundamental que norteou a sua estratégia é a cooperação em matérias finalísticas. Trata-se – principalmente – da busca por parcerias capazes de alinhar atividades de normatização e fiscalização, e não apenas para realizar atividades-meio, como a capacitação de servidores de outros órgãos etc. Essa distinção, no entanto, revelou-se – de início – um desafio prático, pois algumas instituições procuraram a ANPD com a expectativa de obter treinamento, frustrando o objetivo principal de cooperação regulatória. Esse desalinhamento inicial evidenciou a necessidade de maior foco na celebração dos instrumentos de cooperação, de modo a garantir que os esforços se concentrassem nos objetivos finalísticos da proteção de dados.

3.2. Tipologias de Interação Institucional Identificadas

A coordenação interinstitucional da ANPD depende de um exame preciso das competências legais, dos instrumentos normativos e das práticas regulatórias dos órgãos que, direta ou indiretamente, tratam dados pessoais ou exercem poder sancionatório sobre agentes de tratamento. Com base nisso, este item apresenta uma análise individualizada de 16 entidades consideradas estratégicas pelo GT, selecionadas pela relevância de seus setores, pela intensidade do tratamento de dados sob sua jurisdição e pelo potencial de sinergia ou sobreposição com a atuação da ANPD. A avaliação seguirá, para cada órgão, um conjunto padronizado de elementos:

a) Setores Regulados: Identifica o campo material de incidência de cada órgão e descreve como o funcionamento desses setores depende do tratamento de dados pessoais (por exemplo, redes inteligentes de energia, cadastros de usuários, prontuários eletrônicos, bases financeiras, ou dados eleitorais).

b) Competências Relacionadas a Dados: Examina as atribuições legais que envolvem coleta, armazenamento, compartilhamento ou supervisão de dados, destacando onde tais competências podem interferir com os princípios e deveres da LGPD.

c) Normas sobre Proteção de Dados Pessoais: Apresenta o arcabouço normativo setorial já existente e identifica regras de privacidade, segurança da informação ou gestão de incidentes que dialogam — ou colidem — com a LGPD.

d) Áreas de Interface com a ANPD: Localiza zonas de contato institucional, evidenciando onde a convergência entre regulação setorial e proteção de dados exige harmonização interpretativa, atuação conjunta ou construção de entendimentos comuns.

e) Pontos de Sobreposição: Identifica tensões regulatórias e potenciais conflitos de competência, especialmente em temas como sanções, incidentes de segurança, compartilhamento compulsório de dados, standards técnicos e regimes específicos de fiscalização.

f) Oportunidades de Sinergia: Mapeia espaços de cooperação virtuosa, nos quais a expertise técnica setorial pode complementar a atuação da ANPD, ampliando eficiência fiscalizatória, segurança jurídica e inovação responsável.

g) Acordos de Cooperação Técnica (ACT): Indica a existência, vigência e escopo de ACTs já celebrados, assim como lacunas institucionais onde tais instrumentos são ausentes, insuficientes ou aguardam formalização.

Esses critérios permitem compreender, de forma sistemática, as dinâmicas regulatórias que influenciam a proteção de dados no Brasil, revelando tanto os riscos de fragmentação normativa quanto as oportunidades estratégicas para consolidar uma governança cooperativa orientada pela LGPD. A leitura comparada dos órgãos analisados evidencia por que a institucionalização da coordenação prevista nos §§ 3º e 4º do art. 55-J da LGPD é condição indispensável para evitar o *bis in idem* administrativo, reduzir conflitos de interpretação e aumentar a eficácia regulatória de todo o ecossistema público.

3.3. Análise Individualizada

De acordo com a Diretora Miriam Wimmer, a ANPD sempre teve o entendimento de que seria necessário estabelecer ACTs com todas as agências e diversos órgãos reguladores federais, tendo em vista a importância de uma atuação coordenada para a eficácia da LGPD. Todavia, a celebração desses acordos não depende exclusivamente da vontade da ANPD, havendo diversas outras variáveis que podem influenciar esse resultado, tais como o grau de urgência na corregulação de um setor específico, a capacidade institucional dos entes correguladores, o interesse e a disponibilidade dos demais agentes regulatórios em firmar os ACTs etc. Embora não se possa negar o empenho da ANPD e a importância dos ACTs celebrados,[44] diversos setores importantes ainda se encontram fora do escopo de uma corregulação previamente concertada.

[44] Desde a sua criação (2019), a ANPD já firmou ACTs com os seguintes agentes reguladores: a) Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae); b) Agência Nacional de Mineração (ANM); c) Secretaria Nacional do Consumidor (SENACON); d) Conselho Administrativo de Defesa Econômica (CADE); e) Núcleo de Informação e Coordenação do Ponto BR (NIC.br); f) Tribunal Superior Eleitoral (TSE); g) Controladoria-Geral da União (CGU); h) Controladoria-Geral do Estado de Minas Gerais (CGE/MG); e i) Agência Nacional de Saúde Suplementar (ANS). Essa lista e os respectivos documentos podem ser encontrados aqui: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Aacesso em 11 mar 2026.

E a ausência de parâmetros claros da atuação conjunta acarreta uma significativa insegurança e riscos regulatórios como: duplicação de esforços investigativos, potenciais tensões em torno do *non bis in idem* administrativo, aumento dos custos de conformidade para os regulados e insegurança jurídica quanto à autoridade competente para definir parâmetros interpretativos ou sancionatórios em matérias de fronteira.

Obviamente, não seria razoável exigir que a ANPD já tivesse celebrado ACTs, nem que venha a celebrá-los em curto espaço de tempo com todas as agências e órgãos reguladores federais. Exatamente por isso, o GT3 elaborou uma lista de agências e órgãos regulatórios federais que, no seu entendimento, deveriam ser considerados prioritários para o desenvolvimento e aprimoramento das relações regulatórias interinstitucionais da ANPD. Essa lista foi apresentada à Diretora Miriam Wimmer, que validou a pertinência e a relevância estratégica de cada uma das agências e órgãos listados.[45] Essa validação reforça o alinhamento entre a percepção do GT3 e a estratégia adotada pela ANPD, consolidando uma lista de interlocutores preferenciais para o desenvolvimento das suas relações regulatórias interinstitucionais.

O mapeamento realizado pelo GT3 buscou identificar as atribuições legais da ANPD potencialmente em confronto com as agências e órgãos setoriais a seguir listados: a) Agência Nacional de Energia Elétrica (ANEEL), b) Agência Nacional de Saúde Suplementar (ANS), c) Agência Nacional de Telecomunicações (ANATEL), d) Agência Nacional de Vigilância Sanitária (ANVISA), e) Banco Central do Brasil (BCB), f) Comitê Gestor da Internet no Brasil (CGI.br), g) Conselho Administrativo de Defesa Econômica (CADE), h) Conselho Nacional de Justiça (CNJ), i) Conselho Nacional do Ministério Público (CNMP), j) Controladoria-Geral da União (CGU), k) Gabinete de Segurança Institucional (GSI), l) Ministério da Ciência, Tecnologia e Inovação (MCTI), m) Ministério da Educação (MEC), n) Secretaria Nacional do Consumidor (SENACON/MJSP), o) Tribunal de Contas da União (TCU) e p) Tribunal Superior Eleitoral (TSE).[46] A análise busca identificar não apenas as áreas de fricção, mas as sinergias latentes que, se devidamente exploradas, podem amplificar a eficácia da Política Nacional de Proteção de Dados. Ademais, verifica-

[45] A lista inicialmente apresentada pelo GT3 possuía as seguintes agências ou órgãos reguladores federais: i) Agência Nacional de Energia Elétrica (ANEEL), ii) Agência Nacional de Saúde Suplementar (ANS), iii) Agência Nacional de Telecomunicações (ANATEL), iv) Agência Nacional de Vigilância Sanitária (ANVISA), v) Banco Central do Brasil (BCB), vi) Comitê Gestor da Internet no Brasil (CGI.br), vii) Conselho Administrativo de Defesa Econômica (CADE), viii) Conselho Nacional de Justiça (CNJ), ix) Conselho Nacional do Ministério Público (CNMP), x) Controladoria-Geral da União (CGU), xi) Gabinete de Segurança Institucional (GSI), xii) Ministério da Ciência, Tecnologia e Inovação (MCTI), xiii) Secretaria Nacional do Consumidor (SENACON/MJSP), xiv) Tribunal de Contas da União (TCU) e xv) Tribunal Superior Eleitoral (TSE). Por sugestão da Diretora Miriam Wimmer, o Ministério da Educação (MEC) foi adicionado à lista.

[46] Averbe-se que o presente Relatório não irá analisar o potencial conflito de atribuições entre a ANPD e todos os demais órgãos regulatórios brasileiros. Essa tarefa, além de ser por demais abrangente e complexa, exigiria tempo e recurso dos quais o presente este GT3 não dispõe. As dezesseis agências/órgãos foram escolhidos devido ao potencial conflitivo das respectivas atuações com a ANPD.

se o *status quo* dos acordos de cooperação já firmados, oferecendo um panorama da maturidade atual da articulação institucional da ANPD.

3.3.1. Agência Nacional de Energia Elétrica (ANEEL)

A Agência Nacional de Energia Elétrica (ANEEL) é a autarquia federal criada pela Lei n° 9.427, de 26 de dezembro de 1996, vinculada ao Ministério de Minas e Energia e responsável por regular e fiscalizar a geração, transmissão, distribuição e comercialização de energia elétrica no Brasil. Sua missão é proporcionar condições favoráveis para que o desenvolvimento do mercado de energia elétrica ocorra com equilíbrio entre os agentes e em benefício da sociedade, garantindo tarifas justas, qualidade do serviço e a sustentabilidade do setor.

Setores Regulados

O setor regulado pela ANEEL abrange toda a cadeia produtiva de energia elétrica, incluindo empresas de geração (hidrelétricas, termelétricas, eólicas, solares), transmissão e distribuição, além dos consumidores e agentes de comercialização. Com a modernização do setor, a regulação se estende a novas tecnologias como redes inteligentes (*smart grids*) e sistemas de medição inteligente, que são intrinsecamente baseados em dados.

Competências Relacionadas a Dados

As competências da ANEEL relacionadas a dados incluem a regulação de tarifas, que exige o tratamento de dados de consumo; a fiscalização de concessionárias, com acesso a dados operacionais e de consumidores; a gestão de cadastros de unidades consumidoras, incluindo dados para a Tarifa Social; e, de forma emergente, a regulação de medidores inteligentes (smart meters), que coletam dados granulares de consumo em tempo real, revelando hábitos privados dos consumidores.

Normas sobre Proteção de Dados Pessoais

A ANEEL ainda não possui um marco normativo consolidado e específico sobre proteção de dados. Suas resoluções sobre qualidade do serviço e medição inteligente tangenciam o tema, mas a regulação da privacidade e segurança dos dados coletados por *smart grids* ainda é uma lacuna a ser preenchida em coordenação com a ANPD.

Áreas de Interface com a ANPD

A principal área de interface com a ANPD é de natureza sinérgica e preventiva, focada na regulação de novas tecnologias. A ANPD deve subsidiar a ANEEL na definição de quais dados podem ser coletados pelos medidores inteligentes, por quanto tempo podem ser retidos e como o consentimento do consumidor deve ser obtido, incorporando os princípios de *Privacy by Design* desde a concepção dos sistemas.

Pontos de Sobreposição

A sobreposição é potencial e futura, podendo ocorrer na fiscalização de incidentes de segurança em sistemas de medição inteligente. Um vazamento de dados de consumo, por exemplo, poderia ser visto como uma falha na prestação do serviço (competência da ANEEL) e um incidente de segurança de dados pessoais (competência da ANPD), demandando coordenação para evitar o *bis in idem* administrativo.

Oportunidades de Sinergia

A sinergia reside na complementaridade funcional: a ANEEL, com sua expertise técnica, pode definir os padrões de segurança cibernética para a infraestrutura elétrica (o 'como'), enquanto a ANPD define os limites e finalidades para o tratamento dos dados de consumo (o 'o quê'), garantindo que a modernização do setor respeite os direitos dos titulares.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.2. Agência Nacional de Saúde Suplementar (ANS)

A Agência Nacional de Saúde Suplementar (ANS) é a agência reguladora federal vinculada ao Ministério da Saúde criada pela Lei n° 9.961, de 28 de janeiro de 2000 (Lei de Criação da ANS) e responsável pela regulação, normatização, controle e fiscalização das atividades que garantem a assistência suplementar à saúde no Brasil. Sua função é promover a defesa do interesse público, regulando as operadoras de planos de saúde e a relação com prestadores e consumidores, visando assegurar a qualidade e a sustentabilidade do setor.

Setores Regulados

A ANS regula o setor de saúde suplementar, que inclui operadoras de planos de saúde (medicina de grupo, cooperativas, autogestões, seguradoras), a rede de prestadores de serviços (hospitais, clínicas, laboratórios) e a relação com os milhões de beneficiários de planos de saúde no país.

Competências Relacionadas a Dados

As competências da ANS são profundamente ligadas ao tratamento de dados pessoais sensíveis. A agência gerencia o Padrão TISS (Troca de Informação na Saúde Suplementar), que estrutura o fluxo de dados clínicos e administrativos entre operadoras e prestadores. Além disso, regula prontuários eletrônicos, fiscaliza o tratamento de dados de beneficiários e gerencia sistemas de informação como o SIB e o DIOPS, que contêm vastos volumes de dados de saúde.

Normas sobre Proteção de Dados Pessoais

A ANS possui normas relevantes como a Resolução Normativa n° 553/2024 (Padrão TISS) e a Instrução Normativa n° 71/2022 (Prontuário Eletrônico). O Acordo de Cooperação Técnica firmado com a ANPD em dezembro de 2024 é o principal instrumento normativo que formaliza a coordenação entre as agências para harmonizar a aplicação da LGPD no setor.

Áreas de Interface com a ANPD

A interface com a ANPD é uma das mais críticas e complexas, envolvendo tanto sinergia quanto sobreposição. As áreas de contato incluem a regulação de dados sensíveis de saúde, a fiscalização de operadoras, o compartilhamento de dados entre os atores do setor, a segurança da informação em sistemas de saúde e a garantia dos direitos dos titulares (beneficiários) de acesso, correção e portabilidade de seus dados.

Pontos de Sobreposição

O ponto de sobreposição mais evidente está na fiscalização e sanção pelo uso indevido de dados de saúde. O uso de dados para seleção de risco (risk scoring) ou negativa de cobertura, por exemplo, viola tanto a LGPD quanto a Lei dos Planos de Saúde, podendo ensejar atuação de ambas as agências. A coordenação é vital para definir qual órgão lidera a investigação e como as sanções são aplicadas para evitar o *bis in idem*.

Oportunidades de Sinergia

A sinergia se manifesta na possibilidade de a ANS, com sua expertise em saúde, atuar como 'braço técnico' da ANPD na fiscalização de operadoras, enquanto a ANPD fornece a interpretação sobre os limites da LGPD. A cooperação também é fundamental para o desenvolvimento do *Open Health* (Saúde Aberta), garantindo que a interoperabilidade de dados seja segura e centrada nos direitos do titular.

Acordo de Cooperação Técnica

- Data de Assinatura: 20 de dezembro de 2024[47]

- Vigência: Dezembro/2024 a dezembro/2027

- Escopo: Estabelecer canal de cooperação para desenvolvimento de ações conjuntas que promovam a segurança da informação e a conscientização sobre boas práticas no setor de saúde suplementar.

- Resumo Executivo: Este é o primeiro Acordo de Cooperação Técnica (ACT) firmado entre a ANPD e uma agência reguladora, representando um marco histórico na coordenação interinstitucional para proteção de dados no Brasil. O acordo foi resultado de um ano inteiro de trabalho conjunto entre as duas organizações ao longo de 2024.

- Ações Previstas: a) Compartilhamento de conhecimentos técnicos entre ANPD e ANS, b) Suporte na elaboração de materiais educativos sobre proteção de dados no setor de saúde, c) Sensibilização e conscientização da população sobre direitos relacionados a dados de saúde, d) Maior eficácia no acompanhamento do cumprimento da LGPD no setor de saúde suplementar, e) Promoção de segurança jurídica e transparência no tratamento de dados sensíveis de saúde

- Observações: O acordo reconhece que dados de saúde são classificados como dados sensíveis pela LGPD e demandam tratamento adequado para garantir a privacidade e segurança dos titulares. A parceria visa aumentar o grau de proteção dos titulares de dados no âmbito dos serviços de saúde suplementar, incluindo operadoras de planos de saúde e prestadores de serviços.

[47] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros. Acesso em 02 jun 2026.

3.3.3. Agência Nacional de Telecomunicações (ANATEL)

A Agência Nacional de Telecomunicações (ANATEL) foi criada pela Lei Geral de Telecomunicações (Lei n° 9.472, de 16 de julho de 1997), é vinculada ao Ministério das Comunicações e tem como finalidade regular, fiscalizar e implementar políticas públicas no setor de telecomunicações, incluindo a gestão do espectro de radiofrequências, a outorga e acompanhamento de concessões, permissões e autorizações, a definição de padrões técnicos, a proteção dos direitos dos usuários e a promoção da competição. Sua função central é assegurar que o mercado opere de forma eficiente, contínua, adequada e em conformidade com o marco normativo, atuando como autoridade administrativa independente, com competências sancionatórias e normativas previstas em lei.

Setores Regulados

A ANATEL regula o setor de telecomunicações, que abrange prestadoras de serviços de telefonia fixa e móvel, internet (banda larga fixa e móvel), TV por assinatura e radiodifusão. Sua atuação impacta diretamente a infraestrutura crítica que viabiliza a economia digital.

Competências Relacionadas a Dados

As competências da ANATEL relacionadas a dados são vastas, incluindo a regulação de cadastros de usuários, a portabilidade numérica, a fiscalização de incidentes de segurança e vazamentos de dados em redes, e a aplicação do Marco Civil da Internet em aspectos de infraestrutura, como a guarda de registros de conexão.

Normas sobre Proteção de Dados Pessoais

As principais normas são a Resolução ANATEL n° 767, de 7 de agosto de 2024 (Regulamento de Segurança Cibernética)[48], que estabelece a obrigação de notificação de incidentes à ANPD, e a Resolução ANATEL n° 632, de 7 de março de 2014 (Regulamento Geral de Direitos do Consumidor), que já previa regras de privacidade e sigilo.

[48] A Resolução ANATEL n° 767, de 7 de agosto de 2024, alterou o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), originalmente aprovado pela Resolução ANATEL n° 740, de 21 de dezembro de 2020, ampliando, entre outros pontos, as hipóteses de notificação de incidentes, inclusive a comunicação à ANPD. Vide: https://informacoes.anatel.gov.br/legislacao/resolucoes/2024/1965-resolucao-767. Acesso em 2 jun. 2026.

Áreas de Interface com a ANPD

A interface com a ANPD é de alta complexidade e envolve sobreposição e sinergia. As áreas de contato incluem a regulação de incidentes de segurança, a fiscalização de operadoras, a aplicação de sanções por violações de dados (competência concorrente) e a regulação de tecnologias emergentes como 5G e Internet das Coisas (IoT).

Pontos de Sobreposição

A principal zona de sobreposição ocorre na regulação do tratamento de dados pessoais no setor de telecomunicações, especialmente porque operadoras tratam grandes volumes de dados sensíveis à privacidade – como registros de conexão, localização, metadados de tráfego e informações cadastrais. Enquanto a ANATEL fiscaliza obrigações setoriais de segurança, sigilo e guarda de dados decorrentes do regime de telecomunicações, compete à ANPD supervisionar a conformidade com os princípios e regras gerais da LGPD; na prática, ambas podem atuar sobre temas como bases legais para tratamento, medidas de segurança, incidentes de dados, compartilhamento com terceiros e direitos dos titulares, exigindo coordenação para evitar duplicidade de exigências e conflitos regulatórios. Um ponto crítico de sobreposição reside na fiscalização de incidentes de segurança. Um vazamento de dados de uma operadora de telefonia é, simultaneamente, uma falha na prestação do serviço (competência da ANATEL, sujeita a multas por má qualidade) e um incidente de segurança de dados pessoais (competência da ANPD, sujeita a sanções da LGPD). Sem coordenação, a operadora pode ser punida duas vezes pelo mesmo fato material, ferindo o princípio do *non bis in idem*.

Oportunidades de Sinergia

A sinergia reside na possibilidade de a ANATEL atuar como 'braço sensorial' da ANPD no setor, utilizando sua capilaridade fiscalizatória e expertise em segurança de redes para verificar requisitos técnicos, enquanto a ANPD fornece a dosimetria da sanção e a análise jurídica da violação de dados sob a ótica da LGPD.

Acordo de Cooperação Técnica

Não identificado até maio de 2025. Note-se, no entanto, que a Resolução ANATEL n° 767, de 7 de agosto de 2024, criou um fluxo de informação com ANPD sobre incidentes, mas não há ACT formal.

3.3.4. Agência Nacional de Vigilância Sanitária (ANVISA)

A Agência Nacional de Vigilância Sanitária (ANVISA) é uma autarquia federal criada pela Lei n° 9.782, de 26 de janeiro de 1999, vinculada ao Ministério da Saúde e responsável pelo controle sanitário de produtos e serviços submetidos à vigilância sanitária, incluindo medicamentos, alimentos, cosméticos, saneantes, derivados do tabaco, produtos médicos, sangue, hemoderivados e serviços de saúde.

Setores Regulados

A ANVISA regula uma vasta gama de setores, incluindo a indústria farmacêutica, de alimentos, de cosméticos e de produtos para a saúde. Sua atuação abrange desde a aprovação de novos medicamentos e dispositivos médicos até a fiscalização de serviços de saúde e a regulação de pesquisas clínicas.

Competências Relacionadas a Dados

As competências da ANVISA relacionadas a dados estão em plena expansão com a digitalização da saúde. Elas incluem a regulação de *Software as a Medical Device* (SaMD) e outros dispositivos médicos conectados que coletam dados de saúde, além da regulação de ensaios clínicos, que envolvem a coleta e o tratamento massivo de dados sensíveis de pacientes.

Normas sobre Proteção de Dados Pessoais

A ANVISA possui regulamentações específicas para pesquisa clínica (RDC n° 09/2015) e está desenvolvendo o marco regulatório para softwares médicos. A harmonização dessas normas com a LGPD e com as regras do sistema CEP/CONEP (Comitê de Ética em Pesquisa) é um desafio central.

Áreas de Interface com a ANPD

A interface com a ANPD é de natureza complementar e sinérgica. A ANVISA foca na segurança clínica e eficácia dos produtos, enquanto a ANPD deve focar na privacidade e segurança dos dados coletados por esses produtos. A atuação conjunta é crucial para garantir que um dispositivo médico seja seguro tanto do ponto de vista clínico quanto de dados.

Pontos de Sobreposição

A sobreposição pode ocorrer na definição de requisitos de segurança para dispositivos médicos conectados. Um dispositivo pode ser aprovado pela ANVISA por sua segurança clínica, mas possuir vulnerabilidades de software que o tornem inseguro sob a ótica da LGPD. A coordenação é necessária para que os critérios de ambas as agências sejam considerados na aprovação de novos produtos.

Oportunidades de Sinergia

A oportunidade de sinergia está na possibilidade de a ANPD auxiliar a ANVISA a incluir requisitos de *Privacy by Design* e *Security by Design* no processo de aprovação de novos dispositivos médicos digitais, garantindo que a inovação em saúde digital seja responsável e segura desde sua concepção.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.5. Banco Central do Brasil (BCB)

O Banco Central do Brasil (BCB) é uma autarquia federal autônoma, criada pela Lei nº 4.595, de 31 de dezembro de 1964 e principal executora das políticas monetária, cambial e de crédito do país. Sua missão é assegurar a estabilidade do poder de compra da moeda, zelar por um sistema financeiro sólido, eficiente e competitivo, e fomentar o bem-estar econômico da sociedade.

Setores Regulados

O BCB regula e supervisiona o Sistema Financeiro Nacional (SFN), incluindo bancos, cooperativas de crédito, instituições de pagamento, administradoras de consórcio e outras instituições financeiras. Sua regulação abrange desde a solidez das instituições até a segurança de sistemas como o PIX e o *Open Finance*.

Competências Relacionadas a Dados

As competências do BCB relacionadas a dados são centrais para sua atuação, especialmente na era digital. O BCB regula o compartilhamento de dados no *Open Finance*, estabelece regras de

segurança cibernética para instituições financeiras e supervisiona o tratamento de dados em sistemas de pagamento como o PIX. Além disso, é o guardião da Lei do Sigilo Bancário (LC 105/2001).

Normas sobre Proteção de Dados Pessoais

As principais normas são a Resolução Conjunta n° 1, de 4 de maio de 2020, que dispõe sobre o *Open Banking* (agora *Open Finance*), e a Resolução CMN n° 4.893, de 26 de fevereiro de 2021, que estabelece a política de segurança cibernética. Essas normas coexistem com a LGPD e a Lei do Sigilo Bancário.

Áreas de Interface com a ANPD

A interface com a ANPD é de alta complexidade, envolvendo a tensão entre o sigilo bancário, a necessidade de compartilhamento de dados para inovação (*Open Finance*) e a proteção da privacidade dos clientes. A atuação coordenada é essencial para definir padrões de consentimento, segurança e portabilidade de dados no sistema financeiro.

Pontos de Sobreposição

A sobreposição pode ocorrer na definição de padrões de consentimento. O consentimento para o *Open Finance* deve seguir os rigores da LGPD (livre, informado, inequívoco). Se o BCB definir um padrão de interface (UX) que induza o usuário ao erro (dark patterns), a ANPD deve intervir. Além disso, a fiscalização de um vazamento de dados em uma instituição financeira pode ser de competência de ambos.

Oportunidades de Sinergia

A sinergia reside na estrutura de supervisão sofisticada do BCB. A ANPD pode confiar na supervisão do BCB em questões de segurança cibernética, focando sua atuação nos direitos dos titulares e na finalidade do uso dos dados. A cooperação é fundamental para o desenvolvimento seguro do Real Digital (Drex) e outras inovações financeiras.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.6. Comitê Gestor da Internet no Brasil (CGI.br)

O Comitê Gestor da Internet no Brasil (CGI.br), que tem como braço operacional o Núcleo de Informação e Coordenação do Ponto BR (NIC.br),[49] é uma entidade multissetorial criada pela Portaria Interministerial n° 147, de 31 de maio de 1995, e reestruturada pelo Decreto Presidencial n° 4.829, de 3 de setembro de 2003. Ele define orientações estratégicas para o uso e o desenvolvimento da Internet no Brasil, inclusive diretrizes para o registro de nomes de domínio sob ".br", a alocação de endereços IP, sendo também responsável por propor procedimentos e padrões que garantam a segurança, a resiliência e a interoperabilidade da rede no país.[50] Sua principal característica é o modelo de governança multissetorial, que reúne representantes do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica para estabelecer diretrizes estratégicas para o uso e desenvolvimento da internet no país.

Setores Regulados

Diferente de uma agência reguladora setorial, o CGI.br não regula um setor econômico específico, mas estabelece as diretrizes para a governança e o uso da Internet em todo o território nacional. Sua atuação abrange a infraestrutura técnica e lógica da Internet, incluindo a administração do registro de nomes de domínio ".br" e a alocação de endereços IP, funções executadas por seu braço técnico e operacional, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

[49] O Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço operacional do Comitê Gestor da Internet no Brasil (CGI.br), é um órgão federal que, entre outras atribuições, é responsável pela operação do "Registro.br" (registro e manutenção de domínios ".br"), pela distribuição de números de Sistema Autônomo e endereços IPv4/IPv6, pelo CERT.br (tratamento de incidentes de segurança), pelo Ceptro.br/IX.br/NTP.br (infraestrutura de rede), pelo Cetic.br (pesquisas e indicadores sobre internet) e pelo Ceweb.br (participação brasileira no desenvolvimento da Web). São órgãos vinculados ao "CGI.br": a) "Registro.br": é a unidade responsável pelo registro e manutenção dos nomes de domínio sob o ccTLD ".br"; b) "CERT.br": atua como CSIRT nacional de último recurso, coordenando notificações e resposta a incidentes de segurança, além de produzir conscientização, boas práticas e capacitação; c) "Cetic.br": produz estatísticas, indicadores e estudos sobre o acesso e o uso das tecnologias da informação e comunicação, além de funcionar como Centro de Categoria 2 da UNESCO voltado ao monitoramento das sociedades da informação e do conhecimento; d) "Ceptro.br": desenvolve projetos para melhorar a qualidade da Internet e difundir seu uso, com ênfase em infraestrutura e aspectos técnicos, incluindo medições, sincronização de tempo, capacitação e promoção de tecnologias como IPv6 e RPKI; e) "Ceweb.br": promove estudos, experimentação e difusão de tecnologias e padrões Web, além de subsidiar políticas públicas relacionadas à Web; f) "IX.br": provê a infraestrutura de interconexão direta entre sistemas autônomos, permitindo a troca de tráfego em pontos de troca e, com isso, reduzindo custos, latência e aumentando a resiliência da rede; e g) "W3C" : exerce funções de articulação, disseminação e fortalecimento dos padrões da Web no Brasil, em alinhamento com a missão do W3C de desenvolver protocolos e diretrizes para o crescimento de longo prazo da Web. Vide: https://nic.br/sobre/?utm_source=chatgpt.com, Acesso em 01 abril 2026.

[50] Vide: Decreto n° 4.829, de 3 de setembro de 2003.

Competências Relacionadas a Dados

As competências do NIC.br relacionadas a dados são cruciais. Ele gerencia a base de dados do WHOIS, que contém informações de contato dos titulares de domínios.br. Além disso, o CERT.br trata de incidentes de segurança na internet brasileira, e o Cetic.br produz as principais pesquisas sobre o uso de tecnologias da informação no país.

Normas sobre Proteção de Dados Pessoais

O CGI.br possui um histórico de fomento ao debate sobre a proteção de dados, culminando na publicação da Resolução CGI.br/RES/2009/003/P, que estabeleceu os "Princípios para a Governança e Uso da Internet no Brasil". Este documento, que precede a LGPD, já consagrava a privacidade do indivíduo e a proteção de dados pessoais como pilares para o uso da Internet. Embora não emita normas com força de lei, suas resoluções e recomendações influenciam diretamente a criação de leis e políticas públicas.

Áreas de Interface com a ANPD

O CGI.br, por meio de suas entidades operacionais como o Cetic.br e o CERT.br, produz conhecimento técnico, pesquisas e estatísticas essenciais para subsidiar a atuação regulatória e fiscalizatória da ANPD. A expertise do CGI.br em segurança de redes, tratamento de incidentes e produção de indicadores sobre o ecossistema digital brasileiro fornece à ANPD insumos cruciais para a elaboração de normas, guias e para a compreensão dos desafios da proteção de dados no país.

Pontos de Sobreposição

A sobreposição é mínima e bem gerenciada pelo acordo de cooperação. O ponto nevrálgico é a gestão da base de dados do WHOIS, onde a necessidade de transparência para fins de segurança e investigação precisa ser equilibrada com o direito à privacidade dos titulares de domínios, um equilíbrio que é construído em conjunto. Enquanto a ANPD possui a competência legal para fiscalizar e aplicar sanções em casos de violação à LGPD, o CGI.br e seu braço operacional, o NIC.br, atuam na prevenção e no tratamento de incidentes de segurança em um nível técnico e na produção de conhecimento. Um incidente de segurança que envolva vazamento de dados pessoais, por exemplo, seria tecnicamente tratado e notificado pelo CERT.br, ao mesmo tempo em que seria objeto de investigação e eventual sanção por parte da ANPD, demandando uma atuação coordenada.

Oportunidades de Sinergia

A sinergia é potencialmente uma das mais fortes e produtivas para a ANPD. O NIC.br, por meio do CERT.br, oferece expertise técnica essencial para a análise de incidentes de segurança. O Cetic.br fornece dados e pesquisas que são vitais para que a ANPD entenda o cenário de privacidade no país e possa basear suas políticas em evidências. A parceria é um modelo de complementaridade funcional.

Acordo de Cooperação Técnica

- Data de Assinatura: Julho de 2021 (renovado em 25 de agosto de 2025)[51]

- Vigência: Agosto/2025 a agosto/2028

- Escopo: Cooperação técnica para fortalecimento da proteção de dados no país, envolvendo CERT.br, Cetic.br e OBIA (Observatório Brasileiro de Inteligência Artificial).

- Resumo Executivo: A parceria, renovada em agosto de 2025, prevê ações educativas, produção de estudos técnicos, compartilhamento de conhecimentos sobre segurança cibernética e incidentes de segurança, além de pesquisas sobre o uso de tecnologias e proteção de dados.

- Ações Previstas: a) Cooperação em incidentes de segurança envolvendo dados pessoais (CERT.br), b) Produção de pesquisas sobre proteção de dados e privacidade (Cetic.br), c) Estudos sobre impacto da IA na proteção de dados (OBIA), d) Desenvolvimento conjunto de materiais educativos e capacitações, e) Troca de informações sobre ameaças e segurança cibernética

- Observações: Esta é uma das parcerias mais longevas e abrangentes da ANPD, envolvendo múltiplos centros especializados do NIC.br. A renovação em 2025 demonstra a continuidade e relevância estratégica da cooperação.

3.3.7. Conselho Administrativo de Defesa Econômica (CADE)

O Conselho Administrativo de Defesa Econômica (CADE) é uma autarquia federal criada pela Lei n° 12.529, de 30 de novembro de 2011 (Lei de Defesa da Concorrência), vinculada ao Ministério da Justiça, e responsável por zelar pela livre concorrência no mercado. Sua missão é prevenir e reprimir as infrações contra a ordem econômica, exercendo funções preventiva (análise de fusões e aquisições) e repressiva (investigação de cartéis e outras condutas anticompetitivas).

[51] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros. Acesso em 02 jun 29026

Setores Regulados

O CADE não é um regulador setorial, mas uma autoridade de concorrência com atuação transversal sobre todos os setores da economia. Sua atuação é particularmente relevante em mercados digitais, onde a concentração de dados pode criar barreiras à entrada e gerar poder de mercado. Note-se, neste particular, que o CADE detém uma atribuição transversal semelhante à da ANPD.

Competências Relacionadas a Dados

As competências do CADE relacionadas a dados estão no centro da economia digital. O CADE analisa como a concentração de dados em posse de grandes plataformas digitais pode afetar a concorrência. Em análises de fusões e aquisições (Atos de Concentração), o CADE avalia o valor e o impacto concorrencial dos ativos de dados que estão sendo transferidos.

Normas sobre Proteção de Dados Pessoais

O Acordo de Cooperação Técnica firmado com a ANPD em junho de 2021 é o principal instrumento que formaliza a atuação conjunta. O CADE também publica guias e estudos sobre a relação entre defesa da concorrência e proteção de dados em mercados digitais.

Áreas de Interface com a ANPD

A interface com a ANPD é de natureza complementar e sinérgica. A ANPD protege o direito individual à privacidade, enquanto o CADE protege a estrutura competitiva do mercado. As duas áreas convergem quando práticas anticompetitivas envolvem o uso abusivo de dados pessoais, como a criação de barreiras à entrada por meio do acúmulo de dados.

Pontos de Sobreposição

A sobreposição é rara, pois as competências são distintas (proteção de dados vs. concorrência). No entanto, um mesmo fato, como a compra de uma empresa com uma grande base de dados, será analisado por ambos sob óticas diferentes: o CADE avaliará o impacto na concorrência, e a ANPD, os riscos à privacidade e os direitos dos titulares.

Oportunidades de Sinergia

A sinergia é exemplar e se materializa no acordo de cooperação. O CADE pode fornecer à ANPD análises econômicas sobre o valor dos dados, enquanto a ANPD pode subsidiar o CADE com pareceres técnicos sobre a legalidade do tratamento de dados em uma operação de fusão, garantindo que a análise concorrencial considere os princípios da LGPD.

Acordo de Cooperação Técnica

- Data de Assinatura: 2 de junho de 2021[52]

- Vigência: Junho/2021 a junho/2026 (5 anos)

- Escopo: Cooperação técnica destinada ao combate às atividades lesivas à ordem econômica e ao fomento e à disseminação da cultura da livre concorrência nos serviços que demandem a proteção de dados pessoais.

- Resumo Executivo: O acordo entre ANPD e CADE foi o segundo ACT celebrado pela ANPD e decorre do reconhecimento da importância econômica atribuída aos dados pessoais na atualidade e da possibilidade de sua conversão para os mais diversos fins, incluindo práticas anticompetitivas.

- Ações Previstas: a) Estabelecer atuação coordenada em casos de infração à ordem econômica que envolvam dados pessoais, b) Cooperação em análise de Atos de Concentração (fusões e aquisições) com transferência de dados, c) Compartilhamento de informações, conhecimentos e experiências nas respectivas áreas de atuação, d) Promoção de ações educativas conjuntas sobre procedimentos e práticas de difusão da livre concorrência nos serviços de proteção de dados pessoais, e) Análise do impacto concorrencial do tratamento de dados em mercados digitais e de Big Data.

- Observações: O acordo reconhece a proximidade crescente entre as esferas da concorrência e da proteção de dados, especialmente em um cenário de Big Data em que os dados possuem elevado valor econômico. Após a cerimônia de assinatura, foi apresentado estudo sobre *Benchmarking* Internacional sobre Proteção de Dados e Defesa da Concorrência.

3.3.8. Conselho Nacional de Justiça (CNJ)

O Conselho Nacional de justiça (CNJ) é um órgão federal criado pela EC nº 45/2004 (art. 103-108) que visa aperfeiçoar o trabalho do sistema judiciário brasileiro, principalmente no

[52] Vide : https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros. Acesso em 02 jun 2026.

que diz respeito ao controle e à transparência administrativa e processual. Sua missão é estabelecer normas e desenvolver políticas judiciárias que promovam a efetividade e a unidade do Poder Judiciário, orientando e fiscalizando os tribunais, inclusive em temas relacionados à gestão da informação. A atuação do CNJ também alcança os serviços notariais e de registro, por meio da Corregedoria Nacional de Justiça, à qual compete editar atos de regulação e disciplina administrativa das serventias extrajudiciais.

Setores Regulados

O CNJ não regula um setor econômico, mas exerce o controle administrativo, financeiro e disciplinar do Poder Judiciário, com exceção do Supremo Tribunal Federal. Sua atuação abrange todos os tribunais (superiores, federais e estaduais, à exceção do Supremo Tribunal Federal), conselhos superiores do Judiciário e os serviços notariais e de registro.

Competências Relacionadas a Dados

As competências do CNJ relacionadas a dados são vastas e incluem a gestão de sistemas nacionais de informação processual (como o Processo Judicial Eletrônico - PJe), a definição de regras para a publicidade de atos processuais e a anonimização de decisões judiciais, e a regulação do tratamento de dados nos cartórios extrajudiciais. A articulação entre CNJ e ANPD deve ser compreendida a partir da atribuição constitucional do CNJ de supervisionar administrativamente o Poder Judiciário, sendo que a efetividade da proteção de dados no sistema de justiça depende de atuação coordenada capaz de harmonizar a interpretação da LGPD e sua transversalidade com as especificidades da atividade jurisdicional e dos serviços extrajudiciais.

Normas sobre Proteção de Dados Pessoais

O CNJ editou a Resolução n° 363, de 12 de janeiro de 2021, que estabelece medidas para o processo de adequação à LGPD no âmbito do Poder Judiciário, e o Provimento n° 134/2022, que dispõe sobre o tratamento de dados nos serviços notariais e de registro. Mais recentemente, o Conselho editou a Portaria nº 369/2025, que estabelece diretrizes para as ações de planejamento e execução voltadas à proteção de dados pessoais no âmbito do próprio CNJ, e a Resolução nº 647/2025, que dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados do Conselho. Também devem ser consideradas a Resolução nº 574/2024 e a Portaria nº 316/2024, relativas ao acesso a dados judiciais públicos consolidados em repositório centralizado.

Áreas de Interface com a ANPD

A interface com a ANPD é crucial para harmonizar a publicidade dos atos processuais, necessária para a transparência, com o direito à privacidade das partes. A cooperação é fundamental para definir regras de acesso a bancos de dados judiciais e para a aplicação da LGPD nas atividades dos cartórios.

Pontos de Sobreposição

A sobreposição ocorre na definição de padrões para o tratamento de dados no Judiciário. A LGPD se aplica ao tratamento de dados realizado pelo Poder Público, mas o CNJ tem autonomia para regular a administração da justiça. O CNJ também exerce função orientativa voltada à indução de boas práticas na interpretação e aplicação da LGPD. A falta de um acordo formal pode gerar interpretações divergentes sobre a anonimização de sentenças ou o acesso a processos.

Oportunidades de Sinergia

A sinergia reside na possibilidade de o CNJ, com sua capilaridade e poder normativo sobre o Judiciário, disseminar as melhores práticas de proteção de dados em todos os tribunais e cartórios do país, atuando como um multiplicador das orientações da ANPD e garantindo a segurança jurídica na aplicação da LGPD no sistema de justiça.

Acordo de Cooperação Técnica

- Data de Assinatura: Em negociação[53]

- Vigência: Não aplicável - acordo ainda não firmado

- Escopo: Cooperação técnica para aplicação da LGPD nas atividades do Poder Judiciário, especialmente nas atividades cartorial e notarial

- Resumo Executivo: Em março de 2024, representantes do Comitê de Proteção de Dados do CNJ e da ANPD reuniram-se para dialogar sobre a atuação da ANPD e esclarecer dúvidas a respeito de aspectos legais da proteção de dados nas atividades cartorial e notarial.

[53] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-se-reune-com-o-comite-de-protecao-de-dados-do-conselho-nacional-de-justica, Acesso em 03 jun 2026

- Ações Previstas: a) Acesso aos bancos de dados judiciais,[54] b) Proteção à privacidade dos titulares falecidos, c) Mudanças nas informações decorrentes de decisões judiciais, d) Compartilhamento de dados entre o poder público e instituições privadas.[55]

- Observações: Durante a reunião, os representantes de ambas as instituições concordaram sobre a quão valiosa pode ser a celebração de um ACT. Para o Diretor-Presidente da ANPD, Waldemar Gonçalves, a iniciativa é muito positiva, pois a interação entre a Agência e o CNJ dará mais segurança jurídica à atuação do sistema extrajudicial.[56]

3.3.9. Conselho Nacional do Ministério Público (CNMP)

O Conselho Nacional do Ministério Público (CNMP) foi criado pela EC n° 45/2004 (art. 130-A) e é o órgão responsável pelo controle da atuação administrativa e financeira do Ministério Público brasileiro e pelo cumprimento dos deveres funcionais de seus membros. Sua missão é zelar pela autonomia do MP e fiscalizar sua atuação, visando a unidade e o aperfeiçoamento da instituição.

Setores Regulados

O CNMP não regula um setor econômico, mas exerce o controle sobre o Ministério Público da União e dos Estados. Sua atuação abrange a fiscalização disciplinar, administrativa e financeira de todos os ramos do Ministério Público.

Competências Relacionadas a Dados

As competências do CNMP relacionadas a dados incluem a edição de normas sobre o tratamento de dados pessoais no âmbito do Ministério Público, especialmente no que tange ao uso de dados em investigações criminais e inquéritos civis. O CNMP também orienta os membros do MP sobre como conciliar a atividade investigativa com os direitos fundamentais garantidos pela LGPD.

---

[54] Matéria já regulada pelas Resoluções CNJ n° 574/2024 e 647/2025
[55] Matéria já regulada pelas Resoluções CNJ n° 574/2024 e 647/2025
[56] AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. *ANPD se reúne com o Comitê de Proteção de Dados do Conselho Nacional de Justiça*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-se-reune-com-o-comite-de-protecao-de-dados-do-conselho-nacional-de-justica. Acesso em: 2 jun. 2026. ACT ainda não formalizado, mas em fase de aproximação institucional.

Normas sobre Proteção de Dados Pessoais

O CNMP publicou a Recomendação n° 88/2021, que dispõe sobre a adequação à LGPD no âmbito do Ministério Público, e a Resolução CNMP n° 281, de 12 de dezembro de 2023, que institui a Política de Proteção de Dados Pessoais do CNMP. Não há Acordo de Cooperação Técnica com a ANPD.

Áreas de Interface com a ANPD

A interface com a ANPD é crucial para definir os limites do tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, que são regidos por legislação específica, mas devem observar os princípios da LGPD.

Pontos de Sobreposição

A sobreposição pode ocorrer na interpretação do Art. 4º, III, da LGPD, que excetua o tratamento de dados para fins de investigação penal. A falta de uma lei específica sobre o tema pode gerar conflitos entre a necessidade de acesso a dados para investigações e o direito à privacidade, cabendo à ANPD e ao CNMP dialogarem para construir uma interpretação harmônica.

Oportunidades de Sinergia

A sinergia reside na possibilidade de o CNMP atuar como um canal de diálogo com todos os ramos do Ministério Público, disseminando as orientações da ANPD e garantindo que a atuação investigativa do MP respeite os direitos dos titulares de dados. Além disso, o próprio Ministério Público é um fiscal da lei e pode atuar na defesa dos direitos dos titulares, em cooperação com a ANPD.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.10. Controladoria-Geral da União (CGU)

A Controladoria-Geral da União (CGU) é o órgão do Poder Executivo Federal criado pela Lei n° 10.683, de 28 de maio de 2003, e responsável por assistir o Presidente da República nas funções de controle interno, auditoria pública, correição, prevenção e combate à corrupção, e

ouvidoria. Também é o órgão central do Sistema de Controle Interno e do Sistema de Transparência do Poder Executivo Federal.

Setores Regulados

A CGU não regula um setor econômico, mas atua de forma transversal sobre toda a Administração Pública Federal, fiscalizando a aplicação de recursos públicos e promovendo a transparência e a integridade.

Competências Relacionadas a Dados

A competência central da CGU relacionada a dados reside em sua função de órgão central da Lei de Acesso à Informação (LAI - Lei n° 12.527, de 18 de novembro de 2011). A CGU é responsável por orientar os órgãos federais sobre como garantir a transparência pública, o que frequentemente envolve a divulgação de dados que podem conter informações pessoais.

Normas sobre Proteção de Dados Pessoais

O Acordo de Cooperação Técnica firmado com a ANPD em maio de 2023 (vigente até 2026) é o principal instrumento para harmonizar a aplicação da LAI e da LGPD. Além disso, a CGU emite pareceres e orientações sobre a divulgação de dados no Portal da Transparência.

Áreas de Interface com a ANPD

A interface com a ANPD é uma das mais importantes no âmbito do Poder Público, focada em resolver a tensão fundamental entre o direito à privacidade (protegido pela LGPD) e o princípio da máxima publicidade (norte da LAI). A cooperação visa criar um equilíbrio para que a transparência não viole direitos de privacidade.

Pontos de Sobreposição

A sobreposição ocorre quando há dúvida sobre a divulgação de um dado pessoal em nome da transparência, como a remuneração de servidores públicos. A CGU pode ter uma interpretação mais favorável à publicidade, enquanto a ANPD pode ter uma visão mais protetiva da privacidade. O ACT é o fórum para resolver essas divergências.

Oportunidades de Sinergia

A sinergia é evidente e se materializa no acordo de cooperação. A CGU pode auxiliar a ANPD a disseminar a cultura de proteção de dados na Administração Pública, enquanto a ANPD pode fornecer à CGU as diretrizes técnicas para a anonimização e pseudonimização de dados em portais de transparência, garantindo que a publicidade seja feita de forma segura.

Acordo de Cooperação Técnica

- Data de Assinatura: 17 de maio de 2023[57]

- Vigência: Maio/2023 a maio/2026

- Escopo: Harmonização entre Lei de Acesso à Informação (LAI) e LGPD, apoio institucional mútuo, intercâmbio sobre fiscalização, elaboração de normas e capacitações.

- Resumo Executivo: Acordo de cooperação técnica para harmonização entre transparência (LAI) e proteção de dados (LGPD), garantindo que a publicidade de atos governamentais não viole direitos de privacidade.

- Ações Previstas: a) Apoio institucional mútuo e intercâmbio de informações sobre fiscalização, b) Orientação à APF com convergência de manifestações oficiais, c) Esclarecimento de casos concretos sobre transparência de dados pessoais em documentos públicos, d) Elaboração de normas e orientações conjuntas, e) Realização de capacitações para servidores públicos

- Observações: A CGU é o órgão central de controle interno, transparência e combate à corrupção, sendo responsável pela implementação e fiscalização da LAI na APF. A parceria com a ANPD é fundamental para harmonizar transparência e privacidade.

3.3.11. Gabinete de Segurança Institucional (GSI)

O Gabinete de Segurança Institucional da Presidência da República (GSI) é um órgão público do Poder Executivo Federal criado por meio da Medida Provisória n° 1.911-10, de 24 de setembro de 1999[58] e é o órgão responsável por assistir diretamente o Presidente da República em assuntos militares e de segurança, coordenar as atividades de inteligência federal e de segurança da informação, e zelar pela segurança pessoal do Presidente e das instalações presidenciais.

[57] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 16 mar 2026

[58] Essa medida provisória instituiu a denominação atual do órgão, substituindo a Casa Militar, e criou o cargo de Ministro-Chefe do GSI da Presidência da República. A estrutura atual do GSI também é prevista na Lei n° 13.502, de 1º de novembro de 2017, e no Decreto n° 9.031, de 12 de abril de 2017

Setores Regulados

O GSI não regula um setor econômico, mas tem competência normativa sobre a segurança da informação e a segurança cibernética no âmbito da Administração Pública Federal. O Departamento de Segurança da Informação do GSI é o órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

Competências Relacionadas a Dados

A principal competência do GSI relacionada a dados é a de estabelecer normas e padrões de segurança da informação e segurança cibernética para os órgãos federais. Isso inclui a gestão de incidentes de segurança, a definição de requisitos técnicos para a proteção de redes e sistemas, e a coordenação da defesa cibernética do governo.

Normas sobre Proteção de Dados Pessoais

Instrução Normativa GSI n° 1/2020 (Segurança da Informação); Instrução Normativa GSI n° 8/2025 (Segurança Cibernética); Portaria GSI sobre classificação de informações. Além disso, o GSI edita diversas Normas Complementares (NC) que estabelecem diretrizes de segurança da informação, como a NC 05/IN01/DSIC/GSIPR, que trata da gestão de incidentes.

Áreas de Interface com a ANPD

A interface com a ANPD é de natureza complementar. A LGPD exige que os agentes de tratamento adotem medidas de segurança técnicas e administrativas aptas a proteger os dados. No âmbito federal, as normas do GSI definem o que são essas medidas, fornecendo o parâmetro técnico para a conformidade com a LGPD.

Pontos de Sobreposição

A sobreposição pode ocorrer na gestão de um incidente de segurança em um órgão federal. O GSI será o responsável pela coordenação da resposta técnica ao incidente, enquanto a ANPD será a autoridade a ser notificada e que avaliará os danos aos titulares e a adequação das medidas de mitigação, podendo aplicar sanções.

Oportunidades de Sinergia

A sinergia é fundamental. O GSI, com sua expertise em segurança cibernética, pode fornecer à ANPD o suporte técnico para a análise de incidentes complexos e para a elaboração de guias de segurança. A ANPD, por sua vez, fornece o enquadramento jurídico e a perspectiva dos direitos dos titulares, garantindo que a segurança da informação seja um meio para proteger a privacidade.

Acordo de Cooperação Técnica

Não identificado até maio de 2025. Observação: Nota Técnica GSI n° 8/2025 menciona Acordo de Cooperação Técnica ainda a ser firmado.

3.3.12. Ministério da Ciência, Tecnologia e Inovação (MCTI)

O Ministério da Ciência, Tecnologia e Inovação (MCTI) é o órgão do governo federal responsável por formular e implementar a Política Nacional de Ciência, Tecnologia e Inovação. Sua missão é promover o avanço científico, a pesquisa tecnológica e a inovação como meios para o desenvolvimento social e econômico do país.

Setores Regulados

O MCTI não é um órgão regulador, mas um formulador de políticas públicas. Sua atuação abrange o fomento à pesquisa, o desenvolvimento de tecnologias estratégicas (como inteligência artificial, IoT, biotecnologia) e a coordenação do Sistema Nacional de Ciência, Tecnologia e Inovação.

Competências Relacionadas a Dados

As competências do MCTI relacionadas a dados estão ligadas ao fomento à inovação digital. O ministério é responsável pela Estratégia Brasileira de Inteligência Artificial (EBIA) e pela Estratégia Brasileira para a Transformação Digital (E-Digital), políticas que dependem intrinsecamente do acesso e tratamento de grandes volumes de dados.

Normas sobre Proteção de Dados Pessoais

Estratégia Brasileira de Inteligência Artificial (EBIA); Decreto n° 11.930, de 27 de fevereiro de 2024 (Regulamenta IA). O MCTI não edita normas de proteção de dados, mas suas políticas de

fomento à inovação, como a criação de sandboxes regulatórios, podem requerer a flexibilização de normas.

Áreas de Interface com a ANPD

A interface com a ANPD reside na necessidade de equilibrar o incentivo à inovação tecnológica com a proteção dos direitos fundamentais. A ANPD deve participar da formulação de políticas como a EBIA para garantir que o desenvolvimento da IA no Brasil seja ético e respeite a privacidade.

Pontos de Sobreposição

A sobreposição é mais uma tensão de políticas do que uma sobreposição normativa. Políticas de Open Data e inovação aberta, promovidas pelo MCTI, podem entrar em conflito com os princípios de minimização e finalidade da LGPD. A criação de sandboxes regulatórios sem a participação da ANPD pode levar a testes que violem direitos dos titulares.

Oportunidades de Sinergia

A sinergia está no fomento a Tecnologias de Aprimoramento de Privacidade (PETs). O MCTI pode financiar pesquisas e o desenvolvimento de padrões técnicos nacionais para anonimização, criptografia e identidade digital soberana, fornecendo as ferramentas tecnológicas para que o mercado possa se adequar à LGPD de forma inovadora.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.13. Ministério da Educação (MEC)

O Ministério da Educação (MEC) é o órgão da administração pública federal responsável pela formulação, coordenação e execução da Política Nacional de Educação, nos termos do art. 205 da Constituição da República e da Lei n° 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional – LDB). Sua atuação abrange todos os níveis e modalidades de ensino, incluindo educação básica, superior, profissional e tecnológica, bem como a regulação, supervisão e avaliação das instituições de ensino federais e privadas.

Setores Regulados

O MEC atua transversalmente sobre o sistema educacional brasileiro, envolvendo escolas públicas e privadas, instituições de ensino superior, sistemas de avaliação, políticas de financiamento estudantil e programas de acesso à educação. Trata-se de um setor intensivo em dados pessoais, especialmente de crianças, adolescentes e jovens adultos, o que confere especial sensibilidade às atividades reguladas.

Competências Relacionadas a Dados

As competências do MEC relacionadas a dados são amplas e estruturais. O ministério é responsável pela gestão e supervisão de grandes bases de dados educacionais, como o Censo Escolar, o Censo da Educação Superior, o ENEM, o SISU, o PROUNI, o FIES e plataformas digitais de aprendizagem e avaliação. Essas bases envolvem dados pessoais e, frequentemente, dados sensíveis, como informações socioeconômicas, dados biométricos, desempenho acadêmico e dados de menores de idade.

Normas sobre Proteção de Dados Pessoais

O MEC não possui um marco normativo próprio e sistematizado sobre proteção de dados pessoais. A adequação à LGPD ocorre de forma fragmentada, por meio de portarias, termos de uso de sistemas educacionais e diretrizes administrativas. Essa lacuna normativa aumenta o risco de assimetrias interpretativas e de práticas divergentes entre instituições federais, estaduais e privadas de ensino.

Áreas de Interface com a ANPD

A interface com a ANPD é direta e relevante, sobretudo no tratamento de dados de crianças e adolescentes (art. 14 da LGPD), na definição de bases legais para políticas públicas educacionais, no uso de dados para avaliação educacional em larga escala e na contratação de soluções de tecnologia educacional (EdTechs) que envolvem coleta massiva de dados. A atuação da ANPD é essencial para orientar o MEC quanto a limites, salvaguardas e boas práticas no uso desses dados.

Pontos de Sobreposição

A sobreposição pode ocorrer na fiscalização do tratamento de dados realizado por instituições de ensino e plataformas educacionais digitais. Um uso indevido de dados de estudantes pode

configurar, simultaneamente, descumprimento de diretrizes educacionais (competência do MEC) e violação à LGPD (competência da ANPD). A ausência de mecanismos formais de coordenação pode gerar insegurança jurídica e risco de respostas administrativas desarticuladas.

Oportunidades de Sinergia

A sinergia reside na possibilidade de a ANPD atuar como órgão orientador central em proteção de dados, enquanto o MEC incorpora tais diretrizes às políticas educacionais, programas federais e critérios de avaliação institucional. A cooperação é especialmente estratégica para o desenvolvimento seguro de ambientes digitais de aprendizagem, para a regulação de EdTechs e para a promoção de uma cultura de proteção de dados no sistema educacional brasileiro.

Acordo de Cooperação Técnica

Não identificado até maio de 2026.

3.3.14. Secretaria Nacional do Consumidor (SENACON/MJSP)

A Secretaria Nacional do Consumidor (SENACON) é um o órgão criado pelo Decreto n° 7.738, de 28 de maio de 2012, vinculado ao Ministério da Justiça e Segurança Pública e responsável por planejar, coordenar e executar a Política Nacional das Relações de Consumo. Sua missão é proteger e defender os direitos dos consumidores, atuando na harmonização e integração do Sistema Nacional de Defesa do Consumidor (SNDC).

Setores Regulados

A SENACON não regula um setor específico, mas atua de forma transversal em todas as relações de consumo, em todos os setores da economia. Ela coordena a atuação dos Procons e outras entidades de defesa do consumidor.

Competências Relacionadas a Dados

As competências da SENACON relacionadas a dados derivam do Código de Defesa do Consumidor (CDC), que já previa o direito à proteção contra práticas abusivas e o direito à informação. A SENACON fiscaliza o uso de dados pessoais em práticas de marketing, publicidade, cobrança e em contratos de adesão.

Normas sobre Proteção de Dados Pessoais

Lei n° 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor - CDC); Decreto n° 11.034, de 5 de abril de 2022 (Sistema Nacional de Defesa do Consumidor). Além disso, a SENACON emite notas técnicas e orientações sobre a aplicação do CDC em conjunto com a LGPD. O Acordo de Cooperação Técnica com a ANPD, firmado em abril de 2021 e prorrogado até 2025, é o principal instrumento para a atuação conjunta.

Áreas de Interface com a ANPD

A interface com a ANPD é de alta sinergia e complementaridade. Muitas violações à LGPD, como o uso não autorizado de dados para marketing ou a falta de transparência, são também violações ao CDC. A atuação coordenada é essencial para uma proteção integral do consumidor-titular de dados.

Pontos de Sobreposição

A sobreposição ocorre na fiscalização e sanção de práticas abusivas que envolvem dados pessoais. Um mesmo caso de telemarketing abusivo, por exemplo, pode ser sancionado pela SENACON (com base no CDC) e pela ANPD (com base na LGPD). O acordo de cooperação é fundamental para definir a atuação conjunta e evitar o *bis in idem*.

Oportunidades de Sinergia

A sinergia é evidente. A SENACON, com sua rede de Procons, possui uma capilaridade que a ANPD não tem, podendo receber denúncias e atuar na ponta. A ANPD, por sua vez, fornece a expertise técnica e jurídica sobre proteção de dados, subsidiando a atuação do Sistema Nacional de Defesa do Consumidor. A elaboração de guias conjuntos é um exemplo prático dessa sinergia.

Acordo de Cooperação Técnica

- Data de Assinatura: Abril de 2021 (publicado em 02/04/2021)[59]

- Vigência: Março/2021 a março/2023; 1º Termo Aditivo: Março/2023 a março/2025

[59] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 02 jan 2026.

- Escopo: Cooperação técnica para proteção de dados pessoais de consumidores, com foco na atuação conjunta em fiscalização, orientação e educação.

- Resumo Executivo: O ACT entre ANPD e SENACON estabelece mecanismos de cooperação para atuação coordenada na proteção de dados pessoais no contexto das relações de consumo. A parceria reconhece que violações à LGPD frequentemente afetam direitos dos consumidores, exigindo atuação articulada entre as duas entidades.

- Ações Previstas: a) Compartilhamento de informações sobre denúncias e investigações relacionadas a violações de dados de consumidores, b) Cooperação em fiscalização e aplicação de sanções em casos que envolvam tanto a LGPD quanto o Código de Defesa do Consumidor (CDC), c) Elaboração conjunta de guias e materiais educativos sobre direitos dos consumidores relacionados à proteção de dados, d) Realização de campanhas de conscientização sobre segurança e privacidade de dados pessoais, e) Intercâmbio de conhecimentos técnicos e experiências nas respectivas áreas de atuação.

- Observações: O acordo foi prorrogado por meio de Termo Aditivo em 2023, demonstrando a continuidade e relevância da parceria para a proteção dos direitos dos consumidores brasileiros.

3.3.15. Tribunal de Contas da União (TCU)

O Tribunal de Contas da União (TCU), disciplinado pelos artigos 70-75 da Constituição da República,[60] é o órgão de controle externo do governo federal que auxilia o Congresso Nacional na missão de acompanhar a execução orçamentária e financeira do país. Sua função é fiscalizar a legalidade, legitimidade e economicidade dos atos de gestão dos administradores públicos federais.

Setores Regulados

O TCU não regula um setor econômico, mas fiscaliza todos os órgãos e entidades da Administração Pública Federal, bem como a aplicação de recursos públicos federais por estados, municípios e entidades privadas.

[60] O TCU foi criado pelo Decreto nº 966-A, de 7 de novembro de 1890. A Constituição Federal de 1988 recepcionou e disciplinou o tribunal nos artigos 70-75, conferindo-lhe assento constitucional e ampliando suas competências de controle externo.

Competências Relacionadas a Dados

As competências do TCU relacionadas a dados são amplas e derivam de sua função de controle. O TCU realiza auditorias em sistemas de tecnologia da informação do governo, fiscaliza grandes contratos de TI e tem acesso a vastas bases de dados governamentais para realizar cruzamentos e identificar fraudes e irregularidades. Recentemente, o TCU tem incluído a conformidade com a LGPD como um item em suas auditorias.

Normas sobre Proteção de Dados Pessoais

O TCU emite acórdãos que estabelecem jurisprudência e orientações para a Administração Pública, incluindo decisões sobre a segurança e governança de dados em órgãos públicos. Não há Acordo de Cooperação Técnica formal com a ANPD.

Áreas de Interface com a ANPD

A interface com a ANPD é de natureza sinérgica. O TCU pode atuar como um importante aliado da ANPD na fiscalização da adequação dos órgãos públicos à LGPD. As auditorias do TCU podem verificar se os órgãos federais estão implementando as medidas de segurança e governança exigidas pela LGPD.

Pontos de Sobreposição

A sobreposição é improvável, pois as competências são distintas. O TCU fiscaliza a gestão pública e o uso de recursos, enquanto a ANPD fiscaliza o cumprimento da LGPD. No entanto, ambos podem auditar a segurança de um mesmo sistema de TI do governo, sendo desejável a coordenação para evitar duplicidade de esforços.

Oportunidades de Sinergia

A sinergia é muito alta. O TCU pode incorporar os critérios e orientações da ANPD em seus planos de auditoria, verificando a conformidade com a LGPD em todo o governo federal. Os relatórios de auditoria do TCU podem fornecer à ANPD um diagnóstico preciso sobre o nível de maturidade em proteção de dados da Administração Pública, subsidiando sua a atividade normativa e fiscalizatória.

Acordo de Cooperação Técnica

Não identificado até maio de 2025.

3.3.16. Tribunal Superior Eleitoral (TSE)

O Tribunal Superior Eleitoral (TSE), disciplinado pelos artigos 118-121 da Constituição da República[61], é o órgão máximo da Justiça Eleitoral brasileira, responsável por gerenciar as eleições em âmbito nacional, garantir a legitimidade do processo eleitoral e o exercício dos direitos políticos. Suas atribuições incluem a organização do alistamento eleitoral, a diplomação dos eleitos, o julgamento de recursos e a normatização das eleições, assegurando a soberania popular por meio do voto.

Setores Regulados

O TSE regula a Justiça Eleitoral, os partidos políticos, os candidatos e coligações, e todos os prestadores de serviços envolvidos no processo eleitoral. Sua jurisdição abrange desde o cadastro de eleitores até a propaganda eleitoral, incluindo o uso de tecnologias e dados em campanhas.

Competências Relacionadas a Dados

O TSE possui competências críticas relacionadas a dados, pois gerencia o Cadastro Eleitoral, um dos maiores bancos de dados pessoais do país, com mais de 150 milhões de registros, incluindo dados biométricos (impressões digitais e fotografias). Suas competências incluem a gestão e o compartilhamento desses dados, além da regulação do uso de dados pessoais em campanhas eleitorais por candidatos e partidos.

Normas sobre Proteção de Dados Pessoais

A principal norma é a Resolução TSE n° 23.659, de 26 de outubro de 2021, que trata da gestão do Cadastro Eleitoral e dos serviços eleitorais, incluindo disposições sobre o tratamento de dados. O Guia Orientativo ANPD/TSE de 2022 e o Acordo de Cooperação Técnica (vigente de 2022 a 2024) são os instrumentos que buscam harmonizar a aplicação da LGPD no contexto eleitoral.

[61] O TSE foi criado pelo Decreto nº 21.076, de 24 de fevereiro de 1932 (Código Eleitoral da época), que instituiu a Justiça Eleitoral no Brasil e criou o Tribunal Superior de Justiça Eleitoral, denominação original do atual TSE. A Constituição Federal de 1988 recepcionou e disciplinou o tribunal nos artigos 118-121.

Áreas de Interface com a ANPD

A interface com a ANPD é de natureza sinérgica e de alta relevância, focada na regulação do uso de dados no contexto eleitoral, na gestão segura do Cadastro Eleitoral e no compartilhamento de dados com outros órgãos, garantindo a conformidade com a LGPD. A cooperação visa educar candidatos e partidos sobre o uso lícito de dados em campanhas.

Pontos de Sobreposição

A sobreposição é mínima, pois a competência do TSE sobre o processo eleitoral é constitucionalmente bem definida. No entanto, pode haver zonas de atrito na interpretação sobre o uso de dados para microdirecionamento de propaganda política, onde a ANPD pode ter uma visão mais restritiva com base nos princípios da LGPD, enquanto o TSE regula as regras específicas da propaganda eleitoral.

Oportunidades de Sinergia

A sinergia é evidente na cooperação para a elaboração de guias e normas, onde a ANPD fornece a expertise em proteção de dados e o TSE, o conhecimento sobre as especificidades do processo eleitoral. A parceria é fundamental para garantir que a inovação no uso de dados em campanhas não comprometa a privacidade dos eleitores e a lisura das eleições.

Acordo de Cooperação Técnica

- Data de Assinatura: 24 de novembro de 2021[62]

- Vigência: Janeiro/2022 a janeiro/2024

- Escopo: Cooperação técnica para proteção de dados pessoais no contexto eleitoral.

- Resumo Executivo: Acordo firmado para trazer benefícios para a sociedade, candidatos, eleitores, partidos políticos e demais agentes de tratamento de dados no contexto do processo eleitoral brasileiro.

- Ações Previstas: a) Regulação do contexto eleitoral com cooperação para elaboração de guias sobre aplicação da LGPD, b) Gestão do Cadastro Eleitoral harmonizando regras anteriores à

[62] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 02 jun 2026.

LGPD, c) Compartilhamento de dados eleitorais definindo limites e requisitos, d) Educação e orientação com campanhas conjuntas de conscientização.

- **Observações:** O TSE gerencia o maior cadastro de dados pessoais do país (mais de 150 milhões de eleitores), incluindo dados biométricos. O acordo foi fundamental para harmonizar a gestão desse cadastro com as disposições da LGPD.

3.3.17. Panorama Interinstitucional

O mapeamento realizado evidencia que a coordenação interinstitucional prevista nos §§ 3º e 4º do Art. 55-J da LGPD ainda não foi formal e plenamente implementada. Dos 16 órgãos analisados, 6 possuem Acordos de Cooperação Técnica (ACT) formalizados com a ANPD: Agência Nacional de Saúde Suplementar (ANS), Conselho Administrativo de Defesa Econômica (CADE), Controladoria-Geral da União (CGU), Comitê Gestor da Internet do Brasil (CGI.br), Secretaria Nacional do Consumidor (SENACON) e Tribunal Superior Eleitoral (TSE), Isso representa cerca de 37,5% de cobertura sobre os entes ou órgãos regulatórios acima indicados.

A cooperação com a Secretaria Nacional do Consumidor (SENACON) foi o marco zero da estratégia da ANPD, sendo o primeiro ACT por ela firmado. A decisão foi consciente, motivada pela necessidade urgente de mitigar a profunda insegurança jurídica de uma eventual superposição regulatória entre a ANPD e o Sistema Nacional de Defesa do Consumidor. O objetivo era garantir que a aplicação do Código de Defesa do Consumidor em matérias de dados pessoais estivesse alinhada às futuras diretrizes da ANPD, diminuindo, com isso, a possibilidade de decisões conflitantes e viabilizando uma proteção homogênea dos titulares em todo o território nacional. Similarmente, seguiram-se os ACTs com o CADE, diante da relevância estratégica da interseção entre proteção de dados e defesa da concorrência na economia digital na economia de dados, e com a CGU, para alinhar a aplicação da LGPD e da Lei n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI).

Além disso, a ANPD confirmou a alta relevância de se aproximar das principais agências setoriais, cujas atividades possuem profunda interface com o tratamento de dados pessoais. Entre as mais importantes, foram destacadas: a) ANATEL, cuja cooperação é vista como essencial, dado o volume massivo de dados pessoais tratados no setor e a criticidade da infraestrutura de comunicação para a economia digital, b) Banco Central, cuja cooperação é considerada de máxima importância, especialmente diante da sua função de regulador em inovações no mercado financeiro (e.g. *Open Finance*), que normalmente se baseiam no compartilhamento intensivo de dados, c) ANS, cuja cooperação é indispensável para garantir a proteção dos dados sensíveis nos tratamentos de dados de saúde. Outros órgãos como a Agência Nacional de Ener-

gia Elétrica (ANEEL) e a Agência Nacional de Vigilância Sanitária (ANVISA) também foram mencionados, reconhecendo-se que a capilaridade da LGPD exige um diálogo permanente com todos os reguladores setoriais para garantir uma aplicação uniforme e coerente da lei.

Uma complexidade adicional deve ser apontada na relação com os órgãos de controle, que não figuram apenas como parceiros, mas também – eventualmente – como órgãos fiscalizadores da própria ANPD. A cooperação com o Tribunal de Contas da União (TCU) e o Ministério Público (MP), embora seja considerada como estratégica pela ANPD, exige um modelo de interação diferenciado devido à natureza de suas atribuições. A ANPD destacou que, embora a cooperação seja desejável, a sobreposição de papéis pode gerar conflitos de interpretação e disputas de competência, demandando um esforço adicional de alinhamento e construção de confiança mútua. Apesar das dificuldades, a ANPD já avançou na estruturação de parceria com alguns desses órgãos, como, por exemplo, com a CGU. [63]

Por fim, a ausência de acordos formais com órgãos estratégicos como Banco Central do Brasil (BCB), Agência Nacional de Telecomunicações (ANATEL), Agência Nacional de Vigilância Sanitária (ANVISA), Agência Nacional de Energia Elétrica (ANEEL), Tribunal de Contas da União (TCU), Conselho Nacional de Justiça (CNJ), Conselho Nacional do Ministério Público (CNMP), Gabinete de Segurança Institucional (GSI), Ministério da Ciência, Tecnologia e Inovação (MCTI) e Ministério da Educação (MEC) representa uma lacuna significativa na governança de dados no Brasil. Esses órgãos regulam setores com intenso tratamento de dados pessoais e possuem competências que frequentemente se sobrepõem às da ANPD, demandando mecanismos formais de coordenação para evitar conflitos normativos, duplicidade de fiscalizações e insegurança jurídica.

Tabela 2: Matriz de Sinergia e Sobreposição

Órgão/Agência	Grau de Superposição	Áreas-Chave de Interação
ANEEL	Médio	Smart grids, medidores inteligentes, dados de consumo de energia
ANATEL	Muito Alto	Incidentes de segurança em telecomunicações, dados de usuários, 5G e IoT

[63] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 16 mar 2026.

ANS	Muito Alto	Dados sensíveis de saúde, fiscalização de operadoras, prontuários eletrônicos
ANVISA	Médio	Farmacovigilância, ensaios clínicos, rastreabilidade de medicamentos
BCB	Crítico	Sigilo bancário vs. LGPD, Open Finance, segurança cibernética financeira, cadastro positivo, PIX
CADE	Alto	Atos de concentração com dados, práticas anticompetitivas, Big Data
CGI.br	Alto	Segurança cibernética (CERT.br), pesquisas (Cetic.br), IA (OBIA)
CGU	Alto	Harmonização LAI x LGPD, transparência e privacidade, orientação à APF
CNJ	Alto	Dados judiciais, sistemas processuais eletrônicos, cartórios e notários
CNMP	Alto	Dados em investigações do MP, compartilhamento interinstitucional
GSI	Alto	Segurança cibernética, informações classificadas, resposta a incidentes
MCTI	Médio	Inteligência Artificial, inovação, pesquisa científica com dados
MEC	Alto	Dados de crianças e adolescentes, EdTechs, sistemas de avaliação educacional (ENEM, SISU, FIES)
SENACON	Crítico	Direitos dos consumidores, fiscalização conjunta, sanções
TCU	Muito Alto	Auditoria de conformidade com LGPD, governança de dados na APF

TSE	Alto	Cadastro eleitoral, dados biométricos, regulação de campanhas

Tabela 3: Matriz de Acordos de Cooperação Técnica entre ANPD e Órgãos Reguladores

Dos 16 órgãos analisados, 6 possuem Acordos de Cooperação Técnica (ACT) formalizados com a ANPD, representando 37,5% de cobertura. O CNJ possui acordo em negociação. Os demais 8 órgãos (ANEEL, ANATEL, ANVISA, BCB, CNMP, GSI, MCTI, MEC, TCU) não possuem ACT formalizado até novembro de 2025.

Órgão	Nome Completo	Status do ACT	Data de Assinatura	Vigência	Escopo Principal
ANS	Agência Nacional de Saúde Suplementar	Ativo	20/12/2024	Dez/2024 a Dez/2027	Segurança da informação e conscientização sobre boas práticas no setor de saúde suplementar
CADE	Conselho Administrativo de Defesa Econômica	Ativo	02/06/2021	Jun/2021 a Jun/2026	Combate a atividades lesivas à ordem econômica e fomento da livre concorrência em serviços de proteção de dados
CGI.br	Comitê Gestor da Internet do Brasil	Ativo (Renovado)	25/08/2025	Ago/2025 a Ago/2028	Fortalecimento da proteção de dados, envolvendo CERT.br, Cetic.br e OBIA

CGU	Controladoria-Geral da União	Ativo	17/05/2023	Mai/2023 a Mai/2026	Harmonização entre LAI e LGPD, apoio institucional mútuo, intercâmbio sobre fiscalização
SENACON	Secretaria Nacional do Consumidor	Ativo (Prorrogado)	02/04/2021	Mar/2021 a Mar/2025	Proteção de dados pessoais de consumidores, fiscalização, orientação e educação
TSE	Tribunal Superior Eleitoral	Expirado	24/11/2021	Jan/2022 a Jan/2024	Proteção de dados pessoais no contexto eleitoral

3.4. Casos de Atuação Conjunta

A experiência recente evidencia que a coordenação interinstitucional entre a ANPD e agentes regulatórios setoriais ainda se desenvolve de maneira relativamente errática. Embora a existência de ACTs tenha sido importante para parametrizar a atuação conjunta em alguns casos de grande repercussão, em outros tantos a interação entre a ANPD e outros órgãos federais não decorreu de arranjos prévios e formalizados, mas de respostas institucionais reativas, motivadas pela urgência do caso concreto e pela necessidade de compatibilizar competências concorrentes ou complementares. A ausência de ACTs não constitui mero dado administrativo, mas fator que pode influenciar diretamente o grau de previsibilidade, eficiência e coerência da atuação estatal perante incidentes complexos ou mercados regulados intensivos em dados pessoais.

A análise de casos reais demonstra que essa articulação interinstitucional ocorre sob duas dinâmicas principais: de um lado, por meio de ações estruturadas com base em ACTs previamente firmados; de outro, por meio de ações reativas coordenadas diante de casos emergentes, sem a existência de um ACT prévio. A seguir, serão apresentadas algumas situações concretas de coordenação interinstitucional entre a ANPD e outros entes ou órgãos regulatórios.[64]

[64] Averbe-se que a presente análise limitou-se aos casos de atuação conjunta publicados no site oficial da ANPD ou nos sites oficiais das entidades ou órgãos regulatórios parceiros.

3.4.1. Casos Antecedidos por ACTs

No grupo dos casos acompanhados de ACT, o exemplo mais nítido é a cooperação entre ANPD e a SENACON, amparada por ACT desde março de 2021. O objetivo do acordo é dar maior agilidade às investigações de incidentes de segurança, mediante compartilhamento de informações sobre reclamações de consumidores e uniformização interpretativa nos casos concretos. Essa moldura cooperativa mostrou aplicação prática recente no caso Grok/X, amplamente noticiado no início de 2026,[65] no qual a ANPD, o MPF e a SENACON expediram recomendações conjuntas imediatas à empresa controladora para coibir a geração e circulação de conteúdos sexualizados indevidos produzidos por inteligência artificial a partir de imagens de pessoas reais, exigindo a implementação de medidas técnicas para impedir a geração de novos conteúdos ilícitos, a suspensão de contas infratoras e a elaboração de um relatório de impacto à proteção de dados.[66] Embora a atuação tenha sido tripartite, ela constitui exemplo expressivo de caso de grande repercussão no qual a participação conjunta da ANPD e da SENACON ocorreu já sob ambiente institucional previamente estruturado por ACT.

Outra ação regulatória concertada relevante da ANPD foi realizada com o CADE. Reconhecendo o elevado valor econômico dos dados pessoais e a proximidade crescente entre as esferas antitruste e de privacidade, a ANPD e o CADE assinaram um ACT em junho de 2021.[67] O objetivo principal foi instituir a cooperação para viabilizar ações conjuntas quando verificadas infrações à ordem econômica que envolvam dados pessoais, especialmente em Atos de Concentração com transferência massiva de dados. Após a solenidade de assinatura do ACT, foi lançado o documento de trabalho "*Benchmarking* internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados", que consiste em um estudo sobre as instituições de proteção de dados e de defesa da concorrência de doze jurisdições, além do Brasil, com análise das principais relações interinstitucionais e dos aspectos gerais das leis de proteção de dados. Nesse sentido, apresenta amplo panorama da estrutura e das funções das autoridades da União Europeia, França, Alemanha, Portugal, Reino Unido, Estados Unidos, Austrália, Canadá, Japão, Coréia do Sul, Singapura e Chile. [68]

Também merece destaque a atuação entre ANPD e TSE em matéria eleitoral. Formalizado em novembro de 2021, o ACT entre a ANPD e e o TSE para atuação conjunta na aplicação

[65] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-mpf-e-senacon-determinam-que-x-implemente-de-forma-imediata-medidas-para-corrigir-falhas-no-grok, Acesso em 27 mar 2026.
[66] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-mpf-e-senacon-recomendam-que-x-impeca-geracao-e-circulacao-de-conteudos-sexualizados-indevidos-por-meio-do-grok, Acesso em 30 mar 2026.
[67] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica, Acesso em 30 mar 2026.
[68] Vide: https://www.gov.br/cade/pt-br/assuntos/noticias/cade-firma-parceria-com-anpd-e-lanca-estudo-sobre-defesa-da-concorrencia-e-protecao-de-dados, Acesso em 30 mar 2026.

da LGPD no contexto eleitoral resultou em produção de materiais educativos, intercâmbio de conhecimentos e ações de capacitação. Na sequência, já em janeiro de 2022, foi publicado o "Guia Orientativo sobre a aplicação da LGPD no contexto eleitoral",[69] voltado a candidatos, partidos e coligações, "fruto de um trabalho em conjunto" entre a ANPD e o TSE.[70] Aqui há um caso real, de elevada relevância institucional social, em que a atuação conjunta não apenas foi precedida de ACT, mas se materializou em produto regulatório concreto, destinado a subsidiar as eleições gerais de 2022.

3.4.2. Casos Não-Antecedidos por ACTs

O primeiro caso relevante de atuação interinstitucional ocorreu a partir de um incidente relativo a vazamento de dados de operadoras de telefonia, apurado pela ANPD em fevereiro de 2021. Em nota oficial, a ANPD informou que oficiou outros órgãos para investigar o incidente e promover medidas de contenção, mitigação e eventual responsabilização. Embora a nota da ANPD não nomeie expressamente a ANATEL como destinatária dessa articulação, o caso situa-se precisamente no setor regulado por ela e ilustra, de modo empiricamente relevante, a necessidade de coordenação entre autoridade transversal de proteção de dados e regulador setorial de telecomunicações, sem que houvesse, à época – e tampouco posteriormente, segundo a lista oficial da própria ANPD – ACT formalizado entre as duas autarquias.[71]

O segundo caso interessante ocorreu em 2021, em função das mudanças da política de privacidade do WhatsApp que autorizaram o compartilhamento de dados dos usuários com empresas do grupo econômico do Facebook. A medida gerou forte preocupação sob as óticas da proteção de dados, defesa do consumidor e livre concorrência. Sem um ACT formal vigente à época, a ANPD, o CADE, o Ministério Público Federal (MPF) e a Senacon uniram forças e emitiram, em maio de 2021, uma recomendação conjunta para que a empresa adiasse a entrada em vigor da nova política.[72] A atuação coordenada e incisiva dos quatro órgãos forçou a plataforma a cooperar e ajustar seus termos, demonstrando a eficácia da frente unida do Estado brasileiro. Curiosamente, o sucesso dessa articulação pontual foi um dos catalisadores para a assinatura do ACT formal entre ANPD e CADE no mês seguinte.

---

[69] ANPD; TSE. *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. 2022. Disponível em: https://www.tse.jus.br/institucional/catalogo-de-publicacoes/lista-do-catalogo-de-publicacoes/publicacoes/g/guia-orientativo-aplicacao-da-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em 27 mar. 2026.

[70] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-tse-assinam-acordo-de-cooperacao-tecnica, Acesso em 27 mar 2026.

[71] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-apura-caso-de-vazamento-de-dados-de-operadoras-de-telefonia?utm_source=chatgpt.com, Acesso em 31 mar 2026

[72] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade, Acesso em 30 mar 2026.

Outro caso concreto, também sem ACT previamente formalizado, ocorreu em setembro de 2021. Trata-se de um incidente de vazamento de dados relacionado ao PIX, que foi comunicado pela instituição financeira controladora dos dados vazados conjuntamente a ANPD e o Banco Central. Na época, a ANPD realizou uma leitura preliminar das duas comunicações para identificar as responsabilidades, neste caso, de múltiplos agentes de tratamento. No âmbito das suas atribuições, atuou junto aos responsáveis para garantir que os titulares sejam devidamente informados, para que sejam adotadas todas as medidas técnicas para evitar novos incidentes semelhantes e para que sejam tomadas as ações cabíveis para reduzir o impacto do ocorrido sobre os titulares. No entanto, não há maiores detalhes sobre os rumos da investigação ou de uma eventual atuação regulatória concertada com o Banco Central, uma vez que, por força de lei, tramitam protegidas por segredo comercial e industrial.[73]

Por fim, o último caso relevante oficialmente publicado diz respeito a uma ação concertada entre a ANPD e a CGU. Nos primeiros anos de vigência da LGPD, observou-se um aparente conflito interpretativo entre a proteção de dados pessoais e o dever de transparência pública estabelecido pela Lei de Acesso à Informação (LAI). Esse cenário gerou insegurança jurídica, levando órgãos públicos a negarem indevidamente pedidos de acesso à informação sob a justificativa de proteção de dados. Para solucionar essa lacuna, a ANPD e a CGU estabeleceram, no biênio 2022-23, uma agenda conjunta de fortalecimento de ações de transparência e acesso à informação, bem como de proteção de dados pessoais. O objetivo do alinhamento entre a CGU e a ANPD foi avaliar e discutir as melhores alternativas para a proteção dos dados pessoais das bases públicas, de modo a maximizar a transparência das informações necessárias para o embasamento de políticas públicas e pesquisas, realizadas tanto pelo setor público quanto pelo setor privado.[74] Em maio de 2023, foi – finalmente – firmado um ACT para estabelecer uma atuação regulatória preventiva e harmonizada.[75]

Nessas hipóteses, o déficit de coordenação prévia projeta riscos conhecidos da literatura regulatória: duplicação de esforços investigativos, potenciais tensões em torno do *non bis in idem* administrativo, aumento dos custos de conformidade para os regulados e insegurança

---

[73] Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/a-anpd-apura-caso-de-vazamento-por-meio-do-sistema-de-pagamentos-instantaneos-pix, Acesso em 31 mar 2026

[74] Durante essas reuniões foram discutidos avanços normativos relacionados à LAI e à LGPD ocorridos em 2022, como a promulgação da Emenda Constitucional n° 115, de 10 de fevereiro de 2022, que acrescenta o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais ao cidadão (art. 5º da Constituição) e também a publicação do Enunciado CGU n° 4/2022, que reconhece a compatibilidade sistêmica entre a LAI e a LGPD, por meio da interpretação harmônica dessas leis. Também foram discutidas e alinhadas questões ligadas aos novos procedimentos adotados pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) para a divulgação de suas bases de dados. A discussão ocorreu em função de o Instituto ter passado a divulgar, em fevereiro deste ano, versões menos detalhadas das bases do Censo da Educação Básica e do Exame Nacional do Ensino Médio (ENEM). Vide: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-acordo-de-cooperacao-tecnica-com-a-cgu, Acesso em 27 mar 2026.

[75] Vide: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/repasses-e-transferencias-de-recursos-financeiros, Acesso em 16 mar 2026.

jurídica quanto à autoridade competente para definir parâmetros interpretativos ou sancionatórios em matérias de fronteira. O caso do vazamento de dados de operadoras de telecomunicações, por exemplo, tornou particularmente visível a coexistência de competências da ANPD e da ANATEL sobre o mesmo fato material, ao passo que os exemplos relacionados à saúde digital, ao *Open Finance*, à cibersegurança governamental e à fiscalização da conformidade estatal à LGPD reforçam que a insuficiência de mecanismos prévios de concertação tende a deslocar para o caso concreto a tarefa de definir, de modo improvisado, os limites de atuação de cada ente.

3.5. Considerações Parciais

Desse quadro resulta uma conclusão relevante para a arquitetura regulatória da proteção de dados no Brasil: a efetividade da coordenação interinstitucional não depende apenas do reconhecimento abstrato da transversalidade da LGPD, mas da construção de instrumentos concretos capazes de organizar, antecipadamente, o diálogo entre a ANPD e os reguladores setoriais. Onde inexistem ACTs, a cooperação tende a assumir feição episódica, fragmentária e dependente da capacidade contingente de articulação entre burocracias; onde esses instrumentos existem, torna-se mais viável transformar sobreposição potencial de competências em complementaridade funcional. Em termos institucionais, isso significa que a consolidação da ANPD como autoridade central do ecossistema brasileiro de proteção de dados exige não a supressão das competências setoriais, mas sua ordenação por meio de mecanismos estáveis de cooperação, aptos a reduzir conflitos, racionalizar a ação fiscalizatória e ampliar a proteção dos titulares.

4. Recomendações

Este capítulo apresenta dez recomendações destinadas ao aprimoramento da atuação interinstitucional da Autoridade Nacional de Proteção de Dados (ANPD). As propostas resultam do dados empírico realizado nos capítulos 1 a 3 deste Relatório, da análise (a) da literatura jurídica especializada, (b) do atual cenário do direito regulatório, do direito digital e do direito da proteção de dados pessoais no país, (c) dos precedentes regulatórios nacionais, (d) da prática regulatória concreta da ANPD, bem como (e) da experiência internacional, notadamente o *Coordinated Enforcement Framework* (CEF/EDPB) europeu, do *Digital Regulation Cooperation Forum* (DRCF) do Reino Unido, do *Office of Information and Regulatory Affairs* (OIRA) dos Estados Unidos e do *Digital Platform Regulators Forum* (DP-REG) da Austrália.

4.1. Celebração de ACTs com os Órgãos Prioritários

A análise empírica desenvolvida no Capítulo 3 evidenciou correlação direta entre o grau de maturidade da coordenação interinstitucional e a existência de instrumentos formais de cooperação. Onde a ANPD celebrou ACTs, observam-se três efeitos verificáveis: a) maior agilidade na resposta a incidentes, b) maior coerência entre as orientações expedidas pelos órgãos envolvidos e c) menor risco de conflito positivo de competência. Em sentido inverso, na ausência de tais instrumentos, a cooperação assume caráter reativo e episódico, dependente de articulações *ad hoc* que não asseguram previsibilidade nem continuidade institucional.

Diante desse diagnóstico, a primeira recomendação deste relatório consiste na celebração de ACTs com os nove órgãos identificados na Seção 3.3 que ainda não firmaram acordo formal com a ANPD, com prioridade para aqueles que atuam em setores de elevada intensidade no tratamento de dados pessoais e, portanto, de maior potencial de sobreposição regulatória.

Síntese Objetiva: celebrar ACTs com os 9 órgãos identificados no item 3.3. que ainda não firmaram acordo formal, priorizando, em razão da criticidade do volume e da sensibilidade dos dados pessoais tratados nos respectivos setores, BCB, ANATEL e ANVISA.

Fundamentação: A formalização de ACTs representa o nível mais elevado de maturidade na coordenação interinstitucional no direito administrativo brasileiro. Regulamentados pelo Decreto n° 11.531, de 16 de maio de 2023, os ACTs estabelecem um arcabouço jurídico para o compartilhamento de informações, a realização de estudos e fiscalizações conjuntas, bem como para o intercâmbio de pessoal. Conforme destacado no relatório do GT3, a ANPD já possui ACTs com órgãos como SENACON, CADE, CGU, TSE, ANS e CGI.br, o que tem se mostrado fundamental para a atuação conjunta em casos complexos, como o caso Grok/X (2026) e a mudança de política de privacidade do WhatsApp (2021).

A ausência de acordos com reguladores de setores intensivos em dados pessoais cria uma lacuna estrutural perigosa, com efeitos concretos demonstráveis. No setor financeiro, por exemplo, o regime regulado pelo BCB, é impulsionado pelo *Open Finance* e pelo PIX, que se baseiam no compartilhamento massivo de dados pessoais e financeiros. O incidente de vazamento de dados do PIX em setembro de 2021, que envolveu a exposição inicialmente reportada de 395.009 chaves PIX (número posteriormente revisado para aproximadamente 414,5 mil), foi comunicado conjuntamente à ANPD e ao BCB, sem que houvesse, à época, protocolo prévio de

coordenação. Essa lacuna persiste e foi posteriormente reiterada em incidentes sucessivos comunicados em 2023, 2024 e 2025.[76]

No setor de telecomunicações, regulado pela ANATEL, a infraestrutura crítica suporta, em dados consolidados pela própria Agência, mais de 270 milhões de acessos móveis ativos ao final de 2025, dos quais cerca de 216 milhões correspondem a acessos humanos — universo que torna o setor um dos maiores repositórios privados de dados cadastrais do país. O vazamento de dados associado a operadoras móveis divulgado em janeiro de 2021 evidenciou a coexistência fática de competências entre ANPD, ANATEL, SENACON e Ministérios Públicos sobre o mesmo evento, sem qualquer protocolo prévio de cooperação que permitisse atuação coordenada.[77]

No setor de saúde, supervisionado pela ANS e pela ANVISA, o tratamento rotineiro de dados pessoais sensíveis (art. 5º, II, da LGPD) demanda parâmetros operacionais específicos, especialmente em razão da expansão regulada da telemedicina (Resolução CFM n° 2.314, de 20 de abril de 2022 e Lei n° 14.510, de 27 de dezembro de 2022) e da consolidação dos prontuários eletrônicos do paciente. A ausência de ACTs com esses dois reguladores impede a edição de orientações harmonizadas sobre bases legais, retenção e compartilhamento de informações clínicas — temas em que a divergência interpretativa produz custos de conformidade desproporcionais e, paradoxalmente, risco regulatório agravado.

Dificuldades para Adoção: A negociação de ACTs com reguladores setoriais consolidados enfrenta três obstáculos identificáveis. O primeiro é a assimetria de maturidade institucional: o BCB, criado pela Lei n° 4.595, de 31 de dezembro de 1964, e a ANATEL, criada pela Lei n° 9.472, de 16 de julho de 1997, contam com décadas de atuação, quadros técnicos numerosos e culturas organizacionais consolidadas. A ANPD, transformada em agência reguladora apenas pela Lei n°

[76] Comunicado oficial do Banco Central do Brasil, divulgado em 30 de setembro de 2021: "Orientado pelo princípio da transparência, o Banco Central do Brasil (BC) vem a público informar a ocorrência de vazamento de dados de chaves Pix sob custódia e responsabilidade do Banco do Estado de Sergipe S.A (Banese), em razão de falhas pontuais em sistemas daquela instituição financeira." Disponível aqui: https://agenciabrasil.ebc.com.br/economia/noticia/2021-09/banese-sofre-falha-de-seguranca-e-invasores-acessam-chaves-pix. Acesso em 22 mai 2026. Sobre a sucessão de incidentes posteriores, v. AGÊNCIA BRASIL. BC comunica vazamento de dados de 238 chaves Pix, 24 ago 2023. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2023-08/bc-comunica-vazamento-de-dados-de-238-chaves-pix. Acesso em 22 mai 2026; e Banco Central comunica vazamento de dados de 3 mil chaves Pix, 18 abr 2024. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2024-04/banco-central-comunica-vazamento-de-dados-de-3-mil-chaves-pix. Acesso em 22 mai 2026.

[77] Dados consolidados em: ANATEL, Painéis de Dados. Disponível em www.gov.br/anatel. Acesso em 22 mai 2026. Sobre o incidente de 2021, v. PROCON-SP, notificações extrajudiciais às operadoras Vivo, Claro, Oi e TIM em fevereiro de 2021. Registre-se que a apuração administrativa não chegou a ser objeto de atuação coordenada formal entre os entes federais competentes, justamente pela ausência de instrumento prévio de cooperação.

15.352, de 25 de fevereiro de 2026, encontra-se em fase de estruturação de sua autoridade institucional e de seu quadro funcional.[78]

O segundo obstáculo é eventual desinteresse das demais agências e órgãos regulatórios em celebrar esses acordos. Tal desinteresse raramente se manifesta de forma explícita; ele pode ser constatado, por exemplo, pelo atraso das negociações, pela insistência em cláusulas de baixo conteúdo normativo que esvaziam o ACT ou pela delegação das tratativas a escalões técnicos desprovidos de poder decisório. Em depoimento ao GT3, a Diretora Miriam Wimmer reconheceu que a celebração de ACTs não depende exclusivamente da vontade da ANPD, havendo variáveis como o grau de urgência percebido pelo parceiro, a capacidade institucional dos entes e o interesse dos demais agentes regulatórios envolvidos.

O terceiro obstáculo é a complexidade jurídica do compartilhamento de informações sigilosas. Processos sancionadores da ANPD podem envolver segredos comerciais e industriais protegidos pelo art. 25 da LGPD e pelo art. 195 da Lei n° 9.279, de 14 de maio de 1996, além de informações sob regimes específicos de sigilo: o sigilo bancário (Lei Complementar n° 105/2001, art. 1º) no setor financeiro; o sigilo das comunicações (art. 5º, XII, da Constituição Federal, c/c arts. 3º, V, e 7º, III, do Marco Civil da Internet — Lei n° 12.965, de 23 de abril de 2014) nas telecomunicações; o sigilo médico (Código de Ética Médica, art. 73) no setor de saúde. A delimitação dos protocolos prévios que permitam o intercâmbio de informações relevantes sem comprometer essas proteções constitui desafio jurídico cuja solução não comporta cláusulas genéricas.

Medidas Concretas: A superação dos obstáculos identificados recomenda três linhas de ação, todas calibradas por precedentes regulatórios concretos.

> **(i)** *Adoção de arquitetura modular e progressiva nos ACTs:* Em vez de instrumentos exaustivos que pretendam exaurir, em um único texto, todas as hipóteses de sobreposição, recomenda-se modelo estruturado em três módulos: (a) módulo primário, contendo princípios de cooperação, definição de pontos focais e prazo de resposta a consultas técnicas; (b) módulo intermediário, contendo um plano de trabalho de curto prazo com entregas verificáveis, tais como a criação de canais diretos de comunicação entre as áreas técnicas (pontos focais designados), protocolos de notificação cruzada de incidentes e procedimentos de consulta prévia em atos normativos com potencial sobreposi-

[78] O artigo 9º da Lei n° 15.352, de 25 de fevereiro de 2026 autorizou a transformação de 797 cargos efetivos vagos no Poder Executivo federal em 200 cargos efetivos de Especialista em Regulação de Proteção de Dados e em 18 cargos em comissão e funções de confiança. O edital do concurso público não havia sido publicado até a data deste Relatório.

ção; e (c) módulo avançado, regulando fiscalização conjunta e compartilhamento probatório. Módulos mais complexos, como protocolos de fiscalização conjunta e compartilhamento de provas, podem ser adicionados por termos aditivos à medida que a confiança institucional se consolida. Esse desenho dialoga com a estrutura adotada no Ato Normativo Conjunto BCB-CADE n° 1, de 10 de dezembro de 2018, que disciplinou — após cerca de duas décadas de tratativas — a coordenação dos órgãos na análise de atos de concentração no Sistema Financeiro Nacional, na investigação de infrações à ordem econômica e no intercâmbio de informações entre as duas autoridades.[79]

(ii) *Ancoragem da negociação em possíveis ganhos mútuos* (*win-win*): A ANPD deve demonstrar como a sua expertise pode auxiliar as agências setoriais a resolverem seus próprios problemas regulatórios. De fato, a experiência internacional sugere que a cooperação entre reguladores se consolida quando organizada em torno de problemas comuns, e não em torno de declarações abstratas de competência.[80] No caso do BCB, por exemplo, a ANPD pode oferecer diretrizes claras sobre bases legais e princípios de minimização que deem segurança jurídica às instituições financeiras no desenvolvimento de novos produtos baseados em dados, reduzindo o risco de sanções futuras e, consequentemente, o risco sistêmico financeiro. Para a ANATEL, a ANPD pode contribuir com parâmetros de *privacy by design* para a regulação de redes 5G e IoT, temas nos quais a agência de telecomunicações reconhecidamente necessita de apoio especializado. Já para a ANVISA, a abordagem interinstitucional poderia dar prioridade, por exemplo, às questões de privacidade decorrentes de dados de farmacovigilância. E assim por diante.

(iii) *Tipificação minuciosa das hipóteses e dos níveis de compartilhamento sigiloso*: A experiência do ACT entre ANPD e CADE, ao prever expressamente os mecanismos de cooperação em atos de concentração envolvendo dados pessoais, oferece referencial inicial, mas insuficiente para os desafios mais agudos do setor financeiro e de telecomunicações. Recomenda-se que os ACTs a serem celebrados contenham, no mínimo: (a) lista taxativa de hipóteses de compartilhamento; (b) classificação dos níveis de sigilo dos documentos transferidos, em consonância com o art. 24 da Lei n° 12.527, de 18 de novembro de 2011 (LAI); (c) designação nominal dos servidores autorizados ao acesso (ou

[79] Artigo 1º do Ato Normativo Conjunto BCB-CADE n° 1/2018: "Este Ato Normativo Conjunto disciplina os procedimentos aplicáveis: I - à análise de atos de concentração econômica envolvendo instituições financeiras (...); II - à apuração de infrações à ordem econômica envolvendo instituições sujeitas à supervisão ou vigilância do BCB (...); III - ao intercâmbio de informações entre o BCB e o CADE". Disponível em: https://www.gov.br/cade/pt-br/assuntos/noticias/cade-e-banco-central-aprovam-ato-normativo-conjunto. Acesso em 22 mai 2026.

[80] Um exemplo do direito comparado é um bom exemplo dessa abordagem *win-win* é o *Digital Regulation Cooperation Forum* (DRCF), no Reino Unido – que reúne, desde 2020, a *Information Commissioner's Office* (ICO), a *Competition and Markets Authority* (CMA) e o Office of Communications (Ofcom), com adesão da *Financial Conduct Authority* (FCA) em 1º de abril de 2021 –, articulou sua atuação a partir de agenda concreta, contemplando, em seu *Workplan 2024/25*, áreas de trabalho como *AI and Digital Hub*, *AI assurance*, *age assurance* e práticas enganosas em interfaces digitais.

outro sistema que garanta acesso auditável); (d) protocolos de descarte ou devolução de informações após o encerramento do processo; e (e) regime sancionatório disciplinar específico aplicável aos servidores em caso de violação.[81]

4.2. Desenvolvimento de Guias Setoriais de Boas Práticas

A celebração de ACTs, por si só, não resolve o problema da fragmentação interpretativa da LGPD nos diferentes setores regulados. Uma vez constituído o arcabouço formal de cooperação, impõe-se um segundo desafio: traduzir os princípios gerais da LGPD (finalidade, adequação, necessidade, minimização etc.) em orientações operacionais concretas para cada contexto setorial.

De fato, o tratamento de dados pessoais num ambiente de *open finance*, por exemplo, regulado pelo BCB, coloca questões práticas substancialmente distintas daquelas que surgem na infraestrutura crítica de telecomunicações, área regulada pela ANATEL, ou dos contratos de saúde suplementar, área regulada pela ANS. Na ausência de diretrizes harmonizadas, os agentes regulados ficam sujeitos a interpretações divergentes entre a ANPD e os demais órgãos ou/entidades reguladoras setoriais, gerando insegurança jurídica e, paradoxalmente, incentivando o descumprimento.

A segunda recomendação deste relatório é, portanto, o desenvolvimento de Guias Setoriais de Boas Práticas elaborados conjuntamente pela ANPD e pelos órgãos competentes em cada área, de modo a oferecer clareza regulatória e reduzir as zonas de conflito normativo.

Síntese Objetiva: Desenvolver Guias Setoriais de Boas Práticas em cooperação com cada regulador parceiro, harmonizando a aplicação da LGPD com a regulação setorial específica e adotando, como referência metodológica, o modelo de co-criação já validado pela ANPD na elaboração do Guia Orientativo ANPD-TSE, de 2022.

Fundamentação: Como já se sabe, a LGPD é uma norma principiológica e transversal. Sua aplicação prática varia drasticamente dependendo do contexto setorial. O tratamento de dados em um hospital (regulado pela ANS/ANVISA) possui riscos, bases legais e finalidades substancialmente diferentes do tratamento realizado por uma operadora de telecomunicações (ANATEL)

[81] O modelo parcial dessa estrutura está presente no próprio Ato Normativo Conjunto BCB-CADE n° 1/2018, art. 6º, que disciplina o intercâmbio de informações entre as autoridades, prevendo expressamente a necessidade de consentimento dos interessados quando se tratar de dados protegidos por sigilo legal. O regime geral de classificação de informações sigilosas no Executivo federal é o do art. 24 da Lei n° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), regulamentado pelo Decreto n° 7.724, de 16 de maio de 2012.

ou por uma instituição financeira (BCB). Os princípios gerais da LGPD (como finalidade, adequação, necessidade, minimização etc.), bem como suas regras específicas, precisam ser traduzidos em requisitos operacionais concretos para cada setor, o que torna altamente recomendável a edição de guias conjuntos que consolidem, em texto único, a posição harmonizada das duas autoridades.

De fato, a publicação de diretrizes e guias conjuntos (*joint guidelines*) é uma ferramenta poderosa para harmonizar a interpretação de normas e reduzir a insegurança jurídica para os regulados. A experiência internacional tem bons exemplos, demonstrando que reguladores com mandatos distintos podem convergir em documentos únicos e coerentes. No Reino Unido, o *Digital Regulation Cooperation Forum* (DRCF) publicou, em 14 de julho de 2022, o Joint Statement *Online safety and competition in digital markets*, subscrito pela *Competition and Markets Authority* (CMA) e pelo *Office of Communications* (Ofcom); [82] já em novembro de 2022, também publicou o *Joint Statement entre Ofcom e Information Commissioner's Office* (ICO) sobre *Online safety and data protection*"[83]

No Brasil, há um precedente que comprova a eficácia e a viabilidade deste instrumento no nosso ordenamento. O "*Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*", publicado conjuntamente pela ANPD e pelo TSE, foi uma entrega concreta decorrente do ACT firmado entre as duas autoridades e ofereceu, aos candidatos, partidos, coligações e federações partidárias, parâmetros operacionais concretos para a campanha eleitoral de 2022. Ao publicar o documento, a ANPD afirmou que se tratava de uma primeira edição, aberta a comentários e contribuições — desenho que conjuga edição tempestiva e abertura à revisão participativa.[84]

A necessidade de guias setoriais é particularmente urgente em áreas onde a regulação setorial impõe obrigações de tratamento de dados que podem conflitar com os princípios da LGPD. Por exemplo, normas do BCB sobre prevenção à lavagem de dinheiro exigem a retenção

---

[82] Observe-se que o DRCF foi formado em julho de 2020 por Ofcom, CMA e ICO, tendo a *Financial Conduct Authority* (FCA) ingressado posteriormente como membro pleno. Portanto, embora os *Joint Statements* sejam assinados por pares de reguladores específicos, são produzidos "sob o guarda-chuva" do DRCF, conforme expressamente reconhecido nos próprios documentos. Vide: COMPETITION AND MARKETS AUTHORITY; OFFICE OF COMMUNICATIONS. *Online safety and competition in digital markets: a joint statement between the CMA and Ofcom*. London: CMA; Ofcom, 14 jul. 2022. Disponível em: https://www.gov.uk/government/publications/cma-ofcom-joint-statement-on-online-safety-and-competition. Acesso em: 27 maio 2026.

[83] Vide: OFFICE OF COMMUNICATIONS; INFORMATION COMMISSIONER'S OFFICE. *Online safety and data protection: a joint statement by Ofcom and the Information Commissioner's Office*. London: Ofcom; ICO, 25 nov. 2022. Disponível em: https://www.gov.uk/government/publications/online-safety-and-data-protection-a-joint-statement-by-ofcom-and-the-information-commissioners-office. Acesso em: 27 maio 2026.

[84] ANPD/TSE. *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. 1. ed. Brasília, jan 2022. A publicação foi lançada com base no Acordo de Cooperação Técnica firmado entre a ANPD e o TSE. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/em-ano-eleitoral-anpd-e-tse-publicam-guia-de-eleicoes. Acesso em 22 mai 2026.

prolongada de dados de clientes, o que pode tensionar o princípio da necessidade. Regulamentos da ANATEL sobre segurança cibernética impõem a coleta de *logs* de conexão, o que pode conflitar com princípios gerais do direito da proteção de dados. Guias setoriais permitem expor, com transparência, a compatibilidade entre obrigações setoriais legítimas e a disciplina geral da proteção de dados, afastando o falso dilema entre conformidade regulatória e conformidade à LGPD.[85]

Dificuldades para Adoção: A elaboração de guias setoriais exige um profundo conhecimento técnico tanto da LGPD quanto das minúcias operacionais do setor regulado. A principal dificuldade é a escassez de recursos humanos especializados. As equipes técnicas da ANPD e das agências setoriais já operam no limite de suas capacidades com as demandas rotineiras de fiscalização, normatização e atendimento ao público. Alocar servidores para a redação de guias conjuntos significa, necessariamente, reduzir a capacidade em outras frentes.

Há, também, o risco de que os guias se tornem documentos excessivamente genéricos. Isso porque, a busca pelo consenso entre órgãos com culturas e as distintas prioridades pode acabar resultando em textos de "mínimo denominador comum", que não abordam as questões mais controversas e relevantes e que, por isso, podem não trazer uma utilidade prática para o regulado. Por outro lado, se forem muito prescritivos, os guias podem engessar a inovação tecnológica ou induzir à burocracia desnecessária. A velocidade dos mercados, principalmente aqueles ligados à economia digital, frequentemente supera a capacidade de atualização dos documentos regulatórios, gerando o risco de obsolescência prematura.

Medidas Concretas: A superação das dificuldades acima recomenda quatro Medidas Concretas:, todas inspiradas em precedentes verificáveis.

> **(i)** *Instituição de grupos de trabalho bilaterais por portaria conjunta:* A ANPD e o regulador setorial parceiro devem formalizar a elaboração de cada Guia mediante portaria conjunta que especifique escopo, cronograma, produtos esperados, recursos alocados e responsáveis pela redação. A experiência do próprio CNPD demonstra que grupos com mandato delimitado e prazo determinado produzem resultados verificáveis e, por isso,

[85] Artigo 60 da Circular BCB n° 3.978, de 23 de janeiro de 2020: "As informações relativas ao processo de conhecimento dos clientes (...) e ao conhecimento dos empregados, parceiros e prestadores de serviços terceirizados devem ser arquivadas e mantidas pela instituição pelo prazo de 10 (dez) anos." Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50905/Circ_3978_v3_P.pdf; Artigo 13, *caput* da Lei n° 12.965, de 23 de abril de 2014: "Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano": Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 22 mai 2026.

podem servir de exemplo. Esse modelo dialoga, no plano internacional, com a prática do DRCF britânico, que estrutura cada *Joint Statement* a partir de equipes intercameradas com pontos focais nomeados de cada autoridade-membro.

(ii) *Adoção de uma abordagem baseada em riscos* (*risk-based approach*): Para evitar a obsolescência rápida, os guias devem adotar uma abordagem baseada em riscos, focando em princípios aplicados e exemplos de casos de uso, em vez de tentar microgerenciar tecnologias específicas. A estrutura do guia deve ser modular, permitindo a atualização de seções específicas sem a necessidade de revisão de todo o documento.

(iii) *Garantir a ampla participação:* É fundamental engajar o setor privado e a academia desde as fases iniciais. A realização de consultas públicas, workshops setoriais e chamadas de contribuições (*call for inputs*) permite que as próprias empresas reguladas apontem as "zonas cinzentas" que mais geram insegurança jurídica. Isso garante que o guia aborde questões reais e práticas, e não apenas preocupações teóricas dos reguladores.

(iv) *Publicação de versões preliminares:* A publicação de versões preliminares para consulta (*draft for consultation*), antes da versão final, garante que o documento seja realista e aplicável, além de reforçar a legitimidade democrática ao processo. O modelo adotado pelo EDPB, que publica *guidelines* em versão para consulta pública antes da adoção final, é uma excelente referência.

4.3. Construção de Protocolo de Definição da *Lead Authority* em Casos de Competência Concorrente

O mapeamento dos casos de atuação conjunta revelou um padrão recorrente: diante de um mesmo evento — um vazamento de dados, uma alteração de política de privacidade ou um ato de concentração com transferência massiva de informações —, a ANPD e os reguladores setoriais são simultaneamente chamados a atuar, sem que exista critério prévio para definir qual autoridade conduzirá a investigação e qual desempenhará papel auxiliar. Nos episódios examinados — o vazamento de dados de operadoras de telecomunicações (2021), a alteração da política de privacidade do WhatsApp (2021), o incidente do PIX (2021) e o caso Grok/X (2026) —, a repartição de tarefas foi definida no calor do caso concreto, de modo improvisado e reativo.

Essa indefinição não constitui problema meramente procedimental. Ela projeta pelo menos três riscos verificáveis, já identificados no diagnóstico: a) o conflito positivo de competência, em que duas ou mais autoridades instauram processos paralelos sobre o mesmo fato, com duplicação de esforços e risco de *bis in idem* administrativo; b) o conflito negativo, em que cada autoridade presume que a outra atuará, gerando vácuo de fiscalização; e c) a divergência

interpretativa, em que os regulados recebem orientações incompatíveis sobre a mesma conduta. A terceira recomendação deste relatório enfrenta diretamente esse problema.

Síntese Objetiva: Construir, no âmbito dos ACTs, um protocolo com critérios objetivos e previamente pactuados para a designação, em cada caso de competência concorrente, de uma autoridade condutora (*lead authority*), responsável por coordenar a instrução probatória e a interlocução com o agente regulado, e de uma ou mais autoridades coadjuvantes, preservada a competência sancionatória legal de cada ente. O desenho poderia inspirar-se, com as devidas adaptações funcionais, no mecanismo de balcão único (*one-stop-shop*) do art. 56 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD) e no modelo de procedimentos coordenados do Ato Normativo Conjunto BCB-CADE n° 1, de 5 de dezembro de 2018.

Fundamentação: A sobreposição de competências entre a ANPD e os reguladores setoriais não constitui acidente ou anomalia normativa, mas característica estrutural dos sistemas regulatórios contemporâneos. No caso da ANPD, a transversalidade da sua área de atuação implica que, em inúmeras situações, sua competência deve coexistir com a de um regulador setorial sobre o mesmo substrato fático. Trata-se de competência concorrente, e não exclusiva: ambas as autoridades dispõem de título jurídico para atuar. O problema, portanto, não é definir quem pode agir — pois ambas podem —, mas organizar como agem, de modo a impedir que a concorrência de títulos se converta em sobreposição desordenada.

Em diversos casos concretos relatados no item 3.4 deste Relatório, a sobreposição produziu insegurança operacional. No caso do vazamento de dados associado a operadoras móveis (fevereiro de 2021), tanto a ANPD quanto a ANATEL detinham competência material sobre o evento. O incidente do PIX-Banese (setembro de 2021) gerou comunicações simultâneas à ANPD e ao BCB sem protocolo prévio definindo a autoridade processualmente líder. O caso WhatsApp (2021-2022) demandou articulação *ad hoc* entre ANPD, CADE, MPF e SENACON, com Recomendação Conjunta e Nota Pública consolidando, *ex post*, a coordenação que deveria ter sido prévia. O caso Grok/X (2026) reuniu ANPD, MPF e SENACON em recomendações tripartites — modelo eficaz, mas dependente de articulação reativa.

A ausência de critério prévio de definição da autoridade líder produz três disfunções recorrentes: (a) duplicação de esforços investigatórios, com pedidos sucessivos das mesmas informações pelo agente regulado; (b) risco de *bis in idem* administrativo, na medida em que dois órgãos podem sancionar o mesmo fato sob qualificações jurídicas distintas; e (c) abertura de espaço para estratégias defensivas oportunistas dos regulados, que exploram divergências interpretativas entre as autoridades, fenômeno descrito na literatura nacional como captura processual.

No direito comparado, o precedente mais desenvolvido de organização da competência concorrente é o mecanismo de autoridade líder (*lead supervisory authority*) instituído pelo art. 56 do RGPD.[86] Embora concebido para resolver a concorrência territorial entre autoridades de proteção de dados de Estados-Membros distintos — e não a concorrência material entre autoridades de naturezas diversas, como ocorre no caso brasileiro —, o modelo oferece três lições transponíveis. A primeira é a adoção de um critério objetivo de designação: a autoridade do estabelecimento principal (*main establishment*), assim entendido o local em que se tomam as decisões sobre as finalidades e os meios do tratamento.[87] A segunda é a previsão de exceção fundada na preponderância do interesse local, autorizando que a autoridade local conduza o caso quando o objeto afete substancialmente apenas titulares do seu território[88]. A terceira é a institucionalização de um procedimento de cooperação, em que a autoridade líder submete projetos de decisão às autoridades interessadas, em busca de consenso antes da decisão final.[89]

No direito brasileiro, há dois precedentes interessantes. De um lado, deve ser destacado o Ato Normativo Conjunto BCB-CADE n° 1, de 5 de dezembro de 2018, que disciplinou — após cerca de duas décadas de disputa de competência sobre atos de concentração no Sistema Financeiro Nacional — a atuação coordenada das duas autarquias. O modelo ali adotado não suprime a competência de nenhum dos órgãos: os atos de concentração são submetidos a ambos, que os examinam de forma independente, em processos próprios.[90] Reserva-se ao BCB, con-

---

[86] RGPD, artigo 56(1): "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*." Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 29 maio 2026.

[87] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines for identifying a controller or processor's lead supervisory authority* (WP 244 rev.01), endossadas pelo European Data Protection Board (EDPB): "*A lead supervisory authority is the authority with the primary responsibility for dealing with a cross-border data processing activity (...). The 'main establishment' (...) will be the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented*." Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-identifying-controller-or-processors-lead_en°. Acesso em 29 maio 2026.

[88] RGPD, artigo 56(2): "*By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State*."

[89] RGPD, art. 60(1): "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other*."

[90] Artigo 2º do Normativo Conjunto n° 1, de 5 de dezembro de 2018 (BCB/CADE), art. 2º: "*Os atos de concentração econômica de instituições financeiras deverão ser submetidos tanto ao BCB quanto ao Cade, que os examinarão de forma independente, em processos próprios, observados os prazos e condições previstos na legislação que disciplina a atuação de cada uma das autarquias.*" Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Ato%20normativo%20conjunto%205_12_2018%20limpa.pdf. Acesso em 29 maio 2026.

tudo, a prerrogativa de aprovação unilateral quando aspectos de natureza prudencial indicarem riscos relevantes e iminentes à solidez e à estabilidade do Sistema Financeiro.[91] Esse desenho — competência preservada, instrução coordenada e critério de preponderância para a atribuição da condução — é diretamente transponível à relação entre a ANPD e os reguladores setoriais.

De outro lado, a Resolução Conjunta ANEEL/ANATEL/ANP n° 2, de 27 de março de 2001, aprovou o Regulamento Conjunto para Resolução Administrativa de Conflitos relacionados ao compartilhamento de infraestrutura — regulamento que, embora circunscrito ao seu objeto setorial, instituiu Comissão Permanente de Resolução de Conflitos composta paritariamente por dois representantes de cada Agência. O arranjo demonstra, em ambiente jurídico nacional, ser viável a criação de instâncias tripartites para deliberação coordenada, sem afronta às competências individuais.[92]

Dificuldades para Adoção: A adoção desta recomendação pode trazer algumas dificuldades de ordem prática e ordem jusdogmática. Uma vez que as competências administrativas de órgãos e entidades regulatórias são definidas por lei, elas são irrenunciáveis pelos seus titulares. Por isso, qualquer protocolo que venha a ser adotado, não pode haver atribuição a uma autoridade o poder de decidir matéria que a lei reservou a outra. Há, portanto, uma linha tênue entre coordenar a instrução — admissível — e delegar a decisão sobre matéria de competência exclusiva — vedada.[93] A formulação do protocolo exige precisão redacional para não incorrer em ilegalidade.

Além disso, a definição de critérios prévios para identificação da autoridade líder implica renúncia parcial de protagonismo regulatório, o que tende a gerar resistência institucional. Alguns órgãos regulatórios – como o BCB (em atividade desde 1964) e a ANATEL (desde 1997) – apresentam cultura organizacional fortemente vinculada à preservação integral de suas competências e tendem a resistir a fórmulas que possam conferir à ANPD a liderança em fatos materiais ocorridos nos setores que regulam. A designação de uma autoridade como condutora pode ser percebida pelas demais como subordinação ou perda de protagonismo, sobre-

[91] Artigo 6º do Normativo Conjunto n° 1, de 5 de dezembro de 2018 (BCB/CADE), art. 6º: "*O BCB poderá aprovar unilateralmente os atos de concentração envolvendo instituição financeira sempre que aspectos de natureza prudencial indiquem haver riscos relevantes e iminentes à solidez e à estabilidade do Sistema Financeiro Nacional*."

[92] Resolução Conjunta ANEEL/ANATEL/ANP n° 2, de 27 de março de 2001, antecedida pela Resolução Conjunta n° 1, de 24 de novembro de 1999, que aprovou o Regulamento Conjunto para Compartilhamento de Infraestrutura entre os Setores de Energia Elétrica, Telecomunicações e Petróleo. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/resolucoes-conjuntas/85-resolucao-conjunta-2. Acesso em 22 mai 2026.

[93] Lei n° 9.784, de 29 de janeiro de 1999, artigo 13: "Não podem ser objeto de delegação: I - a edição de atos de caráter normativo; II - a decisão de recursos administrativos; III - as matérias de competência exclusiva do órgão ou autoridade."

tudo por reguladores setoriais consolidados e ciosos de sua autonomia. A assimetria de maturidade institucional entre a ANPD (transformada em agência reguladora apenas em 2026) e seus pares setoriais tende a agravar essa resistência.

Medidas Concretas: A superação dos obstáculos identificados recomenda cinco medidas, todas calibradas por precedentes verificáveis.

(i) *Critério objetivo de preponderância material para designação da autoridade condutora:* O protocolo deve fixar, *ex ante*, um teste de preponderância que identifique, em cada caso, qual interesse é predominante. Quando o cerne do evento for a proteção de dados pessoais em si (e.g. um vazamento de dados sem repercussão prudencial sistêmica), a ANPD poderia conduzir o processo; quando o evento envolver risco setorial preponderante (e.g. risco à estabilidade do Sistema Financeiro), a condução caberia ao regulador setorial, atuando a ANPD como autoridade coadjuvante. Esse critério adapta funcionalmente a lógica do estabelecimento principal do art. 56 do RGPD, que localiza a competência no centro de gravidade da atividade, ao contexto brasileiro de concorrência material, e não territorial.

(ii) *Critério subsidiário de anterioridade da apuração:* Em hipóteses nas quais o critério principal não permita identificação inequívoca, o órgão que primeiro instaurou processo administrativo formal deverá preferência para liderar a investigação, mediante comunicação imediata aos demais órgãos potencialmente competentes, replicando-se, em escala doméstica, o modelo dos arts. 60 e 61 do RGPD sobre cooperação entre autoridades concorrentes.

(iii) *Preservação da competência e procedimento de consulta prévia:* Para conciliar a coordenação com a indisponibilidade da competência, o protocolo deve adotar a fórmula de processos independentes com instrução coordenada. Desse modo, cada autoridade manteria o seu processo e o seu poder decisório, mas a instrução probatória é unificada sob a condução da autoridade líder, e nenhuma decisão sancionatória é proferida sem prévia consulta à autoridade coadjuvante, à semelhança do procedimento de projetos de decisão do art. 60 do RGPD. Reduz-se, assim, o risco de decisões conflitantes sem que se incorra em delegação vedada de competência.

(iv) *Mecanismo escalonado de resolução de conflitos de competência:* O protocolo deve prever uma instância para a solução dos conflitos positivos e negativos. A primeira possibilidade poderia ser a submissão da questão à uma comissão bilateral de resolução de conflitos, previamente estabelecida. Em não havendo consenso, a questão poderia ser submetida a um terceiro, como o Ministério a qual elas estejam vinculadas ou, no caso de autoridades vinculadas a pastas distintas, a Casa Civil.

(v) *Incorporação do protocolo como módulo padrão dos ACTs e registro público de precedentes:* em coerência com a arquitetura modular recomendada na Seção 4.1, o protocolo de definição da autoridade condutora deve constar como módulo padronizado dos ACTs, replicável entre diferentes pares institucionais. Recomenda-se, adicionalmente, a manutenção de registro público das designações adotadas em cada caso, de modo a construir, por acréscimo, um repertório de precedentes que confira previsibilidade às designações futuras.

4.4. Adoção de Sistemas de Informação Compartilhado

A coordenação interinstitucional estruturada pelos ACTs, Guias Setoriais e Protocolos de Autoridade Líder são instrumentos que permanecem operacionalmente limitados na ausência de infraestrutura informacional comum. O mapeamento da atuação conjunta revelou que a cooperação entre a ANPD e os reguladores setoriais esbarra, de modo recorrente, em um obstáculo de infraestrutura: a insuficiência dos atuais canais existentes para o intercâmbio de informações entre as autoridades. Nos casos examinados, a comunicação interinstitucional dependeu de expedientes pontuais — ofícios, reuniões *ad hoc* e contatos informais —, sem suporte tecnológico que assegurasse rastreabilidade, padronização e segurança. A consequência foi a fragmentação informacional: cada autoridade pode ter operado a partir de um acervo parcial de dados do mesmo evento, com retrabalho na coleta de elementos e risco de decisões fundadas em quadros fáticos divergentes.

A quarta recomendação deste Relatório consiste, portanto, na adoção de Sistema de Informação Compartilhado entre a ANPD e os reguladores setoriais parceiros, destinado ao registro coordenado de denúncias, investigações em curso e sanções aplicadas — instrumento de redução da assimetria informacional intraestatal e de prevenção da duplicação de esforços. De fato, uma coordenação interinstitucional efetiva só produzem efeitos plenos se houver um substrato material que viabilize o fluxo coordenado de dados entre os entes cooperantes. A presente recomendação enfrenta esse pressuposto: a criação de um sistema de informação compartilhado como infraestrutura permanente da cooperação interinstitucional.

Síntese Objetiva: Desenvolver, no âmbito da cooperação entre a ANPD e os reguladores setoriais, um sistema de informação compartilhado, de arquitetura interoperável, que crie um ambiente eletrônico seguro destinado ao intercâmbio padronizado, rastreável e controlado de informações sobre incidentes, investigações e atos de regulação de interesse comum, com arquitetura de níveis de acesso diferenciados.

Fundamentação: A assimetria de informação entre órgãos do próprio Estado constitui um dos obstáculos centrais à eficiência regulatória. No estado atual, a ANPD pode instaurar processo administrativo contra determinada empresa sem conhecimento de que a SENACON, o CADE ou a ANATEL já conduzem investigação avançada sobre o mesmo fato ou agente — duplicação que desperdiça recursos públicos e produz risco de decisões contraditórias, comprometendo a coerência sistêmica da atuação estatal. Sistema de informação compartilhado opera como repositório centralizado de inteligência regulatória, permitindo: (a) cruzamento de dados sobre denúncias; (b) mapeamento de infratores reincidentes em múltiplos setores; (c) coordenação de agendas de fiscalização; e (d) identificação precoce de padrões de violação.

A experiência internacional fornece dois modelos consolidados. No direito europeu, o RGPD institucionaliza a cooperação informacional entre autoridades por meio de dois mecanismos. O primeiro é o dever de assistência mútua do art. 61, que obriga as autoridades a prestarem-se informações úteis e cooperação recíproca,[94] a serem realizadas, sempre que possível, por meios eletrônicos e em formato padronizado.[95] O segundo é a previsão de operações conjuntas do art. 62, que admite a atuação coordenada de autoridades de diferentes Estados-Membros em investigações comuns.[96] O suporte material desses mecanismos é o Sistema de Informação do Mercado Interno (IMI), plataforma eletrônica europeia de intercâmbio de informações entre autoridades, originalmente instituída pelo Regulamento (UE) n° 1024/2012.[97] O IMI demonstra que um ambiente eletrônico comum, com fluxos padronizados e níveis de acesso controlados, é a infraestrutura que torna operacional a cooperação que, sem ela, permaneceria meramente declaratória.

Nos Estados Unidos, o *Consumer Sentinel Network*, operado pela *Federal Trade Commission* (FTC), agrega reclamações de consumidores e relatórios de fraude provenientes de múltiplas fontes e os torna acessíveis exclusivamente a autoridades de aplicação da lei (federais, estaduais, locais e internacionais selecionadas). O sistema recebeu 6,5 milhões de reportes em

[94] RGPD, artigo 61(1): "*As autoridades de controlo facultam mutuamente as informações úteis e prestam-se assistência mútua a fim de aplicar e dar execução ao presente regulamento de forma coerente, e tomam medidas para uma cooperação efetiva mútua*."
[95] RGPD, artigo 61(5): "*As autoridades de controlo dão resposta aos pedidos [...] por via eletrônica, utilizando um formato normalizado sempre que possível.*"
[96] RGPD, artigo 62(1): "*As autoridades de controlo conduzem, sempre que adequado, operações conjuntas, incluindo investigações conjuntas e medidas de execução conjuntas, nas quais participem membros ou pessoal das autoridades de controlo de outros Estados-Membros*."
[97] O Sistema de Informação do Mercado Interno (Internal Market Information System — IMI) foi instituído pelo Regulamento (UE) n° 1024/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à cooperação administrativa através do IMI, constituindo a plataforma eletrónica de intercâmbio de informações entre autoridades dos Estados-Membros.

2024 e oferece, aos órgãos integrantes, ferramentas de identificação de tendências, mapeamento de práticas questionáveis e coordenação de investigações.[98]

No plano infralegal, o precedente brasileiro mais consolidado de arquitetura de compartilhamento de dados entre órgãos públicos é o Decreto n° 10.046, de 9 de outubro de 2019, que instituiu a Plataforma de Interoperabilidade e estabeleceu três níveis de compartilhamento, graduados pela sensibilidade da informação: a) o compartilhamento amplo, para dados públicos sem restrição de acesso; b) o restrito, para dados protegidos por sigilo, entre órgãos previamente autorizados; e c) o específico, para dados sob sigilo, entre órgãos expressamente identificados em razão de finalidade determinada.[99] Esse desenho escalonado oferece modelo diretamente transponível ao sistema ora proposto, ao demonstrar que é juridicamente viável conciliar o compartilhamento com a observância dos diversos regimes de sigilo.[100]

Dificuldades para Adoção: Algumas dificuldades podem ser apresentar na tentativa de adoção desta recomendação. Algumas dificuldades são de natureza técnica: a) a arquitetura do sistema, que deve ser capaz de acomodar bases de dados de natureza e finalidades distintas; b) a segurança do sistema, uma vez que um repositório que concentra informações sensíveis de múltiplas autoridades constitui, por definição, alvo de elevado valor e, portanto, ponto único de falha, tornando o instrumento de cooperação em vetor de altíssima vulnerabilidade

Outras dificuldades têm natureza operacional: a) o desenvolvimento e a manutenção de um ambiente eletrônico seguro demandam investimento tecnológico e capacitação contínuos, recursos cuja escassez é especialmente sensível para a ANPD, agência de criação recente e estrutura ainda em consolidação; b) a integração de bases de dados heterogêneas (construídas em diferentes plataformas, com padrões distintos de arquitetura) constitui desafio técnico de primeira ordem, que demanda investimento significativo em infraestrutura e em quadro técnico qualificado; c) a compatibilização com os diversos regimes de sigilo também deve ser en-

[98] FEDERAL TRADE COMMISSION. *Consumer Sentinel Network*. Disponível em: https://www.ftc.gov/enforcement/consumer-sentinel-network e https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024. Acesso em 22 mai 2026.

[99] Artigo 4º do Decreto n° 10.046, de 9 de outubro de 2019, art. 4º: "*O compartilhamento de dados [...] será classificado nas seguintes categorias: I - compartilhamento amplo, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso [...]; II - compartilhamento restrito, quando se tratar de dados protegidos por sigilo, nos termos da legislação, e para órgãos e entidades [...] previamente autorizados [...]; e III - compartilhamento específico, quando se tratar de dados protegidos por sigilo, nos termos da legislação, entre órgãos e entidades expressamente identificados, em razão de finalidade determinada [...].*"

[100] A governança desse modelo é, ademais, atribuída a uma instância colegiada: compete ao Comitê Central de Governança de Dados (CCGD) deliberar sobre as orientações e diretrizes para a categorização dos níveis de compartilhamento amplo, restrito e específico.

frentada, uma vez que informações de interesse comum frequentemente se encontram protegidas por sigilo bancário, fiscal, das comunicações ou médico, cada qual com regime legal próprio.

Além disso, a questão a governança do sistema também deve ser resolvida: a) titularidade da plataforma, b) repartição dos custos de desenvolvimento; c) manutenção e definição das políticas de acesso. A experiência brasileira com grandes projetos federais de TI demonstra que a governança compartilhada é o aspecto mais desafiador, superando, em regra, as dificuldades técnicas propriamente ditas.[101]

Medidas Concretas: A construção do sistema deve adotar uma abordagem deliberadamente conservadora quanto à ambição inicial (sob pena de inviabilidade) e deve ser calibrada por precedentes verificáveis e por um princípio de implementação progressiva.

(i) *Interoperabilidade via APIs*: A construção de uma plataforma monolítica é tecnicamente arriscada e institucionalmente improvável. Uma estratégia viável seria a interoperabilidade entre os sistemas de processo eletrônico já em operação nos órgãos, mediante interfaces de programação de aplicações (APIs) padronizadas. O Sistema Eletrônico de Informações (SEI), regulamentado pelo Decreto n° 8.539, de 8 de outubro de 2015, e construído conforme os Padrões de Interoperabilidade de Governo Eletrônico (ePING), pode servir como referência operacional relevante, muito embora, por si só, não cubra as funcionalidades de inteligência cruzada exigidas, podendo servir como camada de transporte documental entre os sistemas dos diferentes reguladores.[102]

(ii) *Implementação modular e escalável:* Em vez de um sistema integral e imediato (de elevado custo e risco), recomenda-se a construção incremental, iniciando-se por um módulo de menor sensibilidade e maior utilidade, como, por exemplo, um repositório comum de notificações de incidentes de segurança de interesse compartilhado. Esse painel poderia conter os metadados compartilhados, exibindo, no mínimo, o nome da

[101] O TCU, por exemplo, constatou que o Sistema Nacional de Acompanhamento e Avaliação das Políticas de Segurança Pública e Defesa Social (SINAPED), previsto pela Lei n° 13.675, de 11 de junho de 2018, não foi implementado nem o respectivo Plano Nacional submetido a avaliações. Sobre as deficiências de implementação do SUSP/PNSPDS, v. CGU, Relatório Diagnóstico sobre a Implementação da Política Nacional de Segurança Pública e Defesa Social, 2020; e TCU, auditorias realizadas no âmbito do SUSP (TC 037.642/2023-5, Acórdão apreciado na sessão plenária de 27 de novembro de 2024, rel. Min. Benjamin Zymler. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/acao-estrategica-do-plano-nacional-de-seguranca-publica-e-defesa-social-apresenta-falhas. Acesso em: 2 jun. 2026). A construção de infraestrutura de dados interagências mostrou-se, em retrospecto, projeto cuja maior dificuldade foi a governança institucional, não a engenharia tecnológica.

[102] Decreto n° 8.539, de 8 de outubro de 2015, art. 1º: dispõe "*sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional*". O SEI é produto do Processo Eletrônico Nacional (PEN). A interoperabilidade do SEI com outros sistemas depende de adequação aos padrões ePING. Vide: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8539.htm. Acesso em 22 mai 2026.

pessoa jurídica investigada (acompanhado de CNPJ), o órgão responsável, o tema da investigação e o status processual (em andamento, arquivado, sancionado). Mesmo nesse formato inicial (que dispensaria o compartilhamento de documentos sigilosos), o sistema já seria capaz de emitir alertas sobre atuações paralelas e redução de duplicações, criando a confiança operacional necessária e servindo de prova de conceito para a expansão futura do escopo para compartilhar níveis de maior sensibilidade.

(iii) *Controle de acesso baseado em funções (RBAC) e trilhas de auditoria imutáveis*: O sistema deve operar com modelo *Role-Based Access Control*, atribuindo permissões granulares conforme o perfil funcional do servidor. As trilhas de auditoria devem registrar, imutavelmente, quem acessou cada informação e quando, viabilizando responsabilização disciplinar específica em caso de vazamento, um modelo análogo ao adotado pelo *Consumer Sentinel Network* norte-americano,[103] que limita o acesso exclusivamente a autoridades de aplicação da lei. No Brasil, o Decreto n° 10.046, de 9 de outubro de 2019 já exige que o sistema adote, desde a concepção, a estratificação do compartilhamento em níveis graduados pela sensibilidade da informação, replicando a lógica dos compartilhamentos amplo, restrito e específico. Dados públicos e metadados de incidentes poderiam circular em um nível amplo, enquanto informações sob sigilo seriam acessíveis apenas em níveis restrito ou específico, mediante autorização prévia e registro de finalidade, assegurando que o acesso de cada autoridade se limite ao estritamente necessário ao exercício de sua competência.

(iv) *Governança colegiada e infraestrutura na Nuvem de Governo*: Recomenda-se que a governança do sistema seja exercida por Comitê Gestor interinstitucional, com representação paritária dos órgãos participantes e mandato fixo, encarregado de definir políticas de classificação, perfis de acesso e atualização da arquitetura. Quanto à infraestrutura, a Nuvem de Governo operada pelo SERPRO e pela Dataprev (criada em decorrência da Portaria SGD/MGI n° 5.950, de 26 de outubro de 2023) oferece ambiente compatível com a exigência de soberania de dados e de *compliance* com a LGPD, dispensando contratação de provedores estrangeiros para infraestrutura crítica do Estado.[104]

---

[103] FEDERAL TRADE COMMISSION. *Consumer Sentinel Network*. Washington, D.C.: FTC, 1997. Vide: https://www.ftc.gov/enforcement/consumer-sentinel-network. Acesso em: 2 jun 2026. Note-se, no entanto, que o acesso à base de dados é restrito a autoridades de aplicação da lei (*law enforcement*) que celebrem acordo de confidencialidade e segurança de dados com a FTC

[104] Portaria SGD/MGI n° 5.950, de 26 de outubro de 2023, da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), que estabelece o novo marco para contratação de serviços de computação em nuvem pela administração pública federal. A Nuvem de Governo SERPRO foi formalmente lançada em outubro de 2023, com infraestrutura fisicamente localizada em território nacional e sob custódia de empresas estatais. Mais de 250 órgãos públicos federais já estão habilitados a utilizar o serviço. V. https://www.serpro.gov.br/menu/noticias/noticias-2023/serpro-lanca-nuvem-de-governo e https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/maio/gestao-serpro-e-dataprev-lancam-servicos-de-nuvem-de-governo-para-orgaos-federais. Acesso em 22 mai 2026.

4.5. Adoção de Protocolos de Notificação Compartilhados de Incidentes

Incidentes de segurança que envolvem dados pessoais raramente afetam apenas uma dimensão regulatória. Os casos mapeados evidenciaram que o incidente de segurança é o evento por excelência da atuação concorrente. Um único vazamento de dados em instituição submetida a regulação setorial faz nascer, simultaneamente, o dever de comunicar à ANPD e o dever de reportar ao regulador do setor, cada qual disciplinado por norma própria, com prazos, formulários e conteúdos distintos. O agente regulado vê-se, assim, diante de obrigações de notificação paralelas e não harmonizadas, ao passo que as autoridades recebem, sobre o mesmo fato, comunicações fragmentadas, em formatos incompatíveis e momentos diversos, com inevitável atraso na mitigação de danos aos titulares.

A presente recomendação enfrenta diretamente essa fragmentação, propondo o desenvolvimento de *Single Window* (balcão único) interinstitucional para notificação de incidentes envolvendo dados pessoais, com interoperabilidade técnica e harmonização normativa entre os regimes setoriais.

Síntese Objetiva: Estabelecer, no âmbito dos ACTs, protocolos de notificação de incidentes compartilhados que harmonizem prazos, conteúdos mínimos e canais de comunicação, de modo a permitir que uma única notificação, ou notificações mutuamente encaminhadas entre as autoridades, satisfaça os deveres concorrentes do agente regulado perante a ANPD e o regulador setorial.

Fundamentação: A fragmentação dos regimes de notificação de incidentes é estrutural e decorre da coexistência de normas setoriais que disciplinam autonomamente o tema. No regime geral de proteção de dados, o dever de comunicação de incidentes tem assento legal no artigo 48 da LGPD, que obriga o controlador a comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. O dispositivo, contudo, fixava apenas o critério aberto do prazo razoável, remetendo a concretização à ANPD. Essa concretização sobreveio com a Resolução CD/ANPD n° 15, de 24 de abril de 2024, cujo artigo 6º estabeleceu o prazo de três dias úteis para a comunicação à ANPD, contado do conhecimento, pelo controlador, de que o incidente afetou dados pessoais, além de detalhar o conteúdo mínimo da comunicação e prever a possibilidade de complementação no prazo de vinte dias úteis.

O regime da ANPD não opera, todavia, no vácuo. Como já foi dito, os mesmos fatos podem desencadear deveres de notificação setoriais autônomos. No sistema financeiro, por exemplo, a Resolução CMN n° 4.893, de 26 de fevereiro de 2021, limita-se a dispor que "os procedimentos adotados pelas instituições para gerenciamento de riscos previstos na regulamentação em vigor devem contemplar, no tocante à continuidade de negócios, (...) a comunicação *tempestiva* ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes (...)," não impondo um prazo previamente estabelecido para todos os casos.

Já no que tange especificamente ao sistema PIX, o artigo 5º da Instrução Normativa BCB n° 412, de 26 de setembro de 2023, impõe ao controlador o dever de comunicar aos usuários a ocorrência de incidentes de segurança envolvendo dados pessoais mantidos na infraestrutura do sistema no prazo "definido pelo Banco Central do Brasil a cada evento", de modo que o prazo concreto é estabelecido caso a caso pelo próprio BCB, e não por norma prévia. Como pode ser visto, essa regra está em conflito direto com a sistemática adotada pela ANPD, o que levanta dúvidas sobre a validade do seu escopo material. De qualquer forma, a coexistência desses regimes, sem coordenação, produz três efeitos disfuncionais já identificados no diagnóstico: a) a sobrecarga do regulado, obrigado a múltiplas notificações sobre o mesmo evento, b) a assimetria informacional entre as autoridades, que recebem versões parciais e desencontradas do incidente; e c) o risco de respostas regulatórias descoordenadas, quando não contraditórias.

Note-se, ademais, que o direito regulatório brasileiro já admite pelo menos uma hipótese de participação *ex post* da ANPD. Trata-se da Resolução ANATEL n° 767, de 7 de agosto de 2024, que prevê um fluxo institucional de comunicação com a ANPD em incidentes envolvendo dados pessoais. Nada impede que esse modelo de cooperação *ex post* seja estendido para a *fase ex ante*, mediante atos normativos conjuntos ou inserção de cláusulas nos ACTs setoriais de balcão único nos incidentes que envolvam tratamento de dados pessoais com potencial risco aos direitos fundamentais dos titulares como elemento material.

No direito europeu, o artigo 33 do RGPD[105] determina que o incidente de segurança que envolva dados pessoais deve ser comunicado à autoridade competente "sem demora injustificada e, sempre que possível, até 72 horas após seu conhecimento".[106] Já o artigo 23 do NIS-2,[107]

[105] 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, L 119, 4 maio 2016, p. 1-88. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 31 maio 2026.

[106] Quando o incidente assume caráter transfronteiriço, a articulação dessa notificação com o mecanismo de autoridade líder demonstra que a comunicação de incidentes e a coordenação interinstitucional são faces do mesmo problema: a notificação só cumpre sua função se chegar, de forma íntegra e tempestiva, a todas as autoridades competentes, sem impor um duplo ônus ao notificante.

[107] UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022. Diretiva NIS 2*. Jornal Oficial da União Europeia, L 333, 27 dez. 2022, p. 80-152. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Acesso em: 31 maio 2026.

determina que um modelo escalonado de notificação de incidentes de segurança, a serem dirigidas a um ponto de entrada determinado[108]: alerta precoce em vinte e quatro horas, notificação do incidente em setenta e duas horas e relatório final em um mês. Verifica-se, aqui, que a tendência é precisamente a oposta à fragmentação,[109] com a adoção de um ponto único de entrada (*single entry point*) que concentra o recebimento de todas as notificações, deixando a distribuição interinstitucional a cargo das próprias autoridades, e não do regulado.[110]

Dificuldades para Adoção: A dificuldade mais óbvia a ser superada é o desenho da arquitetura de um regime de notificações homogêneo para autoridades regulatórias, de um lado, e para os usuários/titulares de dados, de outro. Isso porque, os prazos, gatilhos e conteúdos exigidos pela ANPD e pelos reguladores setoriais foram concebidos com finalidades distintas – a proteção de dados, de um lado; a estabilidade ou a continuidade setorial, de outro – e nem sempre são redutíveis a um formato único. Eventual harmonização pode acabar sacrificando as especificidades que justificam cada regime regulatório.

Outro obstáculo, em tese mais simples, é de natureza normativa: a ressalva do art. 6º da Resolução CD/ANPD n° 15, de 24 de abril de 2024 preserva os prazos previstos em legislação específica, mas não autoriza, por si só, que a notificação a um regulador setorial substitua a comunicação à ANPD. A construção de um protocolo de notificação compartilhada que produza

[108] No contexto da NIS-2, cada Estado-Membro da União Europeia deve designar um ou mais CSIRTs (*Computer Security Incident Response Team*), que funcionam como o ponto de entrada para o recebimento das notificações obrigatórias de incidentes significativos.

[109] Considerando 108 da NIS 2 reconhece expressamente a necessidade de coerência com o RGPD e prevê a coordenação entre autoridades. No entanto, deve ser lembrado que o NIS-2 é uma Diretiva, e não um Regulamento, de modo que sua adoção pelos Estados-membros depende de incorporação ao direito interno por norma nacional.

[110] Isso não significa que não haja potencial conflito normativo entre o RGPD e o NIS-2 na definição do que deve ser reportado (*what*). De fato, parece haver uma dificuldade paralela e estruturalmente análoga nos dois regimes: tanto a NIS-2 quanto o RGPD exigem que o regulado avalie, em tempo real e sob incerteza, se um incidente de segurança atingiu o patamar que aciona a obrigação de notificar. Enquanto na NIS-2, o critério é o "incidente significativo" capaz de causar disrupção operacional severa, no RGPD o critério é a violação de dados pessoais que apresente "risco aos direitos e liberdades das pessoas singulares". Note-se que as próprias DPAs alemãs divergiram sobre se a mera existência de uma vulnerabilidade explorada sem comprovação de exfiltração de dados já ativava a obrigação de notificação das autoridades de proteção de dados, evidenciando que a vagueza dos limiares de ativação é um problema compartilhado por ambos os regimes e que se agrava quando o mesmo evento fático aciona simultaneamente as duas obrigações. Ao que parece, a extensão promovida pela NIS-2 (ao incluir incidentes onde o dano ainda não se materializou, mas é potencial) aproxima conceitualmente os dois instrumentos, embora os critérios de avaliação permaneçam distintos (disrupção de serviços *vs.* risco a direitos fundamentais), o que pode gerar incerteza jurídica para o regulado obrigado a decidir, nas primeiras horas após a detecção do incidente, se deve notificar apenas o CSIRT, apenas a DPA, ou ambos. Vide: SCHMITZ-BERNDT, Sandra. *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*. Journal of Cybersecurity, v. 9, n° 1, 2023. Disponível em: https://doi.org/10.1093/cybsec/tyad009. Acesso em 31 mai 2026. Sobre o conflito entre as DPAs alemães, vide: HEIDRICH, Joerg. Exchange-Hack: *unerfreuliche Positionen der Datenschutzbehörden zu Meldepflicht*. Heise Online, 11 mar. 2021. Disponível em: https://www.heise.de/news/Exchange-Hack-Unerfreuliche-Positionen-der-Datenschutzbehoerden-zu-Meldepflicht-5076453.html. Acesso em: 31 maio 2026.

efeito liberatório recíproco depende de base normativa adequada, e não apenas de ajuste bilateral.

Além disso, a eventual criação de um "balcão único" também deveria superar outros obstáculos, como, por exemplo: a) desafio tecnológico, pois os sistemas de processo eletrônico das autarquias foram construídos em plataformas distintas, com arquiteturas de dados incompatíveis; (ii) tensão de temporalidade, pois em incidentes graves as primeiras horas são críticas e qualquer intermediação central pode atrasar a resposta setorial específica, ao passo que a notificação simultânea descoordenada produz risco de ações contraditórias; (iii) sigilo técnico, pois informações sobre vulnerabilidades exploradas podem, se divulgadas prematuramente, ser instrumentalizadas por atacantes adicionais (o que exige definição rigorosa de quem acessa o quê e em que momento).

Medidas Concretas: A superação dos obstáculos identificados recomenda quatro medidas, calibradas por precedentes verificáveis.

(i) *Formulário unificado de notificação com núcleo comum e módulos setoriais:* O protocolo deve adotar (a) um formulário padrão de notificação estruturado em um núcleo comum (e.g. natureza do incidente, categorias de dados afetadas, número estimado de titulares, vetor de ataque presumido, medidas de contenção adotadas etc.) e (b) anexos específicos para exigências setoriais (parâmetros de continuidade do serviço, indicadores de risco sistêmico etc.). Com isso, estaria assegurada a padronização das informações essenciais sem a supressão das exigências próprias de cada regime, à semelhança da arquitetura modular já recomendada para os ACTs (Seção 4.1).

(ii) *Ponto único de entrada com encaminhamento interinstitucional (modelo NIS-2):* Em vez de impor ao regulado o dever de múltiplas notificações, o protocolo deve prever que a comunicação seja recebida por um ponto de entrada, incumbindo-se as próprias autoridades de encaminhar, entre si, as informações pertinentes. Esse desenho transpõe a lógica do *single entry point* do NIS-2 e desloca o ônus da distribuição do notificante para as autoridades, reduzindo a sobrecarga do regulado e a assimetria informacional entre os entes.

(iii) *Harmonização de prazos pelo critério do menor prazo aplicável:* Para conciliar regimes com prazos distintos, o protocolo deve adotar, como regra de coordenação, a observância do menor prazo aplicável ao caso em decorrência dos regimes jusregulatórios concorrentes. O cumprimento do prazo mais exíguo satisfaz, por consequência lógica, os prazos mais elásticos, evitando que a pluralidade de marcos temporais gere insegurança quanto ao termo final da obrigação.

(iv) *Salvaguardas de sigilo e canal seguro de encaminhamento em tempo real:* O encaminhamento interinstitucional das notificações deve transitar por canal seguro, com as salvaguardas de sigilo já delineadas para o sistema de informação compartilhado (Seção 4.4), preservando-se a faculdade de o controlador requerer o tratamento sigiloso de informações protegidas por lei, na forma do art. 7º da Resolução CD/ANPD n° 15, de 24 de abril de 2024. O canal deve operar em tempo real, de modo a compatibilizar a coordenação interinstitucional com a exiguidade dos prazos de notificação.

4.6. Adoção de Protocolos para Fiscalização Conjunta

O mapeamento revelou que determinados casos (pela escala, pela transversalidade técnica ou pela pluralidade de regimes incidentes) superam a capacidade de fiscalização isolada de uma única autoridade. Episódios como o vazamento de dados de operadoras de telecomunicações, o incidente do PIX e a controvérsia em torno do tratamento de dados para treinamento de inteligência artificial no caso Grok/X exigiram expertise simultânea em proteção de dados, em regulação setorial e em segurança da informação. Nesses casos, a fiscalização fragmentada não apenas duplica esforços, como compromete a própria qualidade da apuração, pois nenhuma autoridade detém, isoladamente, o quadro completo do ilícito.

A indefinição da autoridade condutora (Seção 4.3) resolve a questão da coordenação; falta, contudo, o instrumento operacional que permita às autoridades atuar materialmente em conjunto na instrução (partilhando equipes, diligências, provas etc.). A presente recomendação supre essa lacuna, propondo a construção de um protocolo de fiscalização conjunta para casos complexos.

Síntese Objetiva: Estabelecer, no âmbito dos ACTs, um protocolo de fiscalização conjunta aplicável a casos complexos, que discipline a constituição de equipes mistas de apuração, a realização de diligências coordenadas e o compartilhamento de provas entre a ANPD e os reguladores setoriais, preservada a competência sancionatória de cada ente.

Fundamentação: A coordenação entre a ANPD e os reguladores setoriais não é faculdade discricionária, mas dever legal. O art. 55-J, § 4º, da LGPD determina que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos coordenem suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência. De fato, a fiscalização conjunta é uma das formas mais adequadas para garantia da eficiência administrativa e legitimação da atuação regulatória concorrente. Não se está falando, aqui, de uma mera troca de informações, mas da atuação material

integrada na apuração, combinando expertises complementares (de um lado, o regulador setorial detém conhecimento aprofundado da arquitetura técnica e do modelo de negócios do mercado regulado; de outro lado, a ANPD domina a dogmática da proteção de dados e as metodologias de avaliação de impacto à privacidade). Desse desenho resultam investigações mais céleres e tecnicamente precisas e decisões sancionadoras com fundamentos mais robustos, atributos que também podem reduzir o risco de anulação em controle judicial subsequente.

No direito brasileiro, a Lei n° 13.848, de 25 de junho de 2019 (Lei Geral das Agências Reguladoras) oferece um bom repertório de instrumentos de articulação fiscalizatória entre reguladores. O art. 29 autoriza a edição de atos normativos conjuntos, que devem conter regras sobre a fiscalização de sua execução e prever mecanismos de solução de controvérsias. O art. 33 admite a celebração de convênios e acordos de cooperação visando, expressamente, à maior eficiência nos processos de fiscalização. Por fim, o seu artigo 34 contempla a descentralização das atividades fiscalizatórias mediante acordo de cooperação, embora circunscreva expressamente o seu alcance. Esses dispositivos demonstram que o ordenamento já dispõe de moldura para a fiscalização articulada entre órgãos e entidades regulatórias. Esse instrumento ganhou ainda mais relevo após a transformação da ANPD em agência reguladora pela Lei n° 15.352, de 25 de fevereiro de 2026.

No direito comparado, o artigo 62 do RGPD prevê expressamente as operações conjuntas entre autoridades supervisoras europeias, estabelecendo que estas devem realizar "sempre que adequado, operações conjuntas, incluindo investigações conjuntas e medidas de execução conjuntas em que estejam envolvidos membros ou pessoal das autoridades de controlo de outros Estados-Membros". A norma admite, ainda, que uma autoridade confira poderes investigativos — sob orientação e presença do anfitrião — a membros ou pessoal de outra autoridade, um modelo de mútua delegação procedimental relevante para o desenho aqui defendido. No plano operacional, o *Coordinated Enforcement Framework* (CEF)[111] do EDPB demonstra a viabilidade de uma fiscalização coordenada com metodologia comum: a cada ano, as autoridades elegem um tema prioritário e atuam de forma sincronizada, a partir de questionário ou guia de auditoria único, com posterior agregação e análise conjunta dos resultados.[112] O CEF é especialmente instrutivo por demonstrar que a coordenação fiscalizatória pode ser construída de forma incremental e voluntária, sem supressão da autonomia de cada autoridade. Já no Reino Unido, o *Digital Regulation Cooperation Forum* (DRCF) publicou, em 30 de abril de 2025, seu

[111] DIGITAL REGULATION COOPERATION FORUM. *DRCF Annual Report 2024/25*. 30 de abril de 2025. Disponível em: https://www.drcf.org.uk/publications/annual-reports/drcf-annual-report-2024-25. Acesso em 31 mai 2026

[112] O CEF é um órgão do Comitê Europeu de Proteção de Dados (EDPB), desenvolvido no âmbito da Estratégia 2021-2023. Anualmente, as autoridades de proteção de dados elegem um tema prioritário e conduzem, em bases voluntárias e de forma sincronizada, ação coordenada de fiscalização a partir de questionário ou guia de auditoria comum, com posterior agregação e análise conjunta dos resultados nos planos nacional e da União.

Annual Report 2024/25, no qual sintetiza as ações coordenadas entre CMA, ICO, Ofcom e FCA e inclui trabalhos sobre IA, *online safety* e proteção de dados.[113]

Dificuldades para Adoção: A adoção de um Protocolo para Fiscalização Conjunta, não é isento de obstáculos a serem superados. A primeira dificuldade é a heterogeneidade dos ritos processuais administrativos: prazos para defesa, instâncias recursais, metodologias de dosimetria, regras de prescrição e procedimentos de produção probatória, dentre outros, variam significativamente entre as agências e devem ser unificados. Além disso, a fiscalização conjunta deve coordenar a instrução, mas não pode resultar em transferência do poder de sancionar, que permanece próprio de cada autoridade.

Outro obstáculo é a coordenação das equipes de campo. Divergências sobre condução da investigação, liderança formal do processo ou interpretação das provas podem paralisar a fiscalização ou produzir conflitos internos que beneficiam o investigado. A experiência comparada sugere que, sem coordenação prévia, regulados sofisticados exploram divergências entre os reguladores para postergar a conclusão dos processos. Como se não bastasse, a equipe mista de apuração, por exemplo, (a) demanda recursos humanos especializados e disponibilidade simultânea de servidores de ambas as autoridades, o que pressiona estruturas ainda em consolidação, como a da própria ANPD, e (b) deve operar de modo que a prova produzida seja simultaneamente válida e aproveitável em processos regidos por normas distintas.

Por fim, as dificuldades operacionais relativas ao tratamento de provas sob sigilo (já apontadas nas Seções 4.1. e 4.4) e ao risco de captura processual (decorrentes da exploração de divergências interpretativas entre os reguladores) também demandariam atenção especial e uma arquitetura madura de coordenação interinstitucional.

Medidas Concretas: A viabilização das fiscalizações conjuntas requer arquitetura procedimental específica, a ser incorporada nos ACTs e seus anexos, a saber:

> **(i)** *Critérios objetivos de ativação para casos complexos:* para evitar a banalização da atuação regulatória concertada, o protocolo deve fixar gatilhos objetivos de ativação da fiscalização conjunta, tais como a pluralidade de regimes regulatórios incidentes, a escala

[113] Importante ressaltar, no entanto, que o DRCF opera como fórum voluntário sem poder próprio de *enforcement*, e a coordenação ali realizada não substitui a competência decisória individual de cada autoridade-membro. Para uma contextualização sobre as atividades do DRFC, vide: DIGITAL REGULATION COOPERATION FORUM. *About the DRCF*. Disponível em: https://www.drcf.org.uk/about-drcf. Acesso em 31 mai 2026

do número de titulares afetados ou a complexidade técnica que exija expertise combinada. A fiscalização conjunta reserva-se, assim, aos casos que efetivamente superam a capacidade de apuração isolada, devendo ter natureza excepcional.

(ii) *Adoção de um Termo de Referência para cada caso*: Antes de cada operação conjunta, sugere-se que os órgãos firmem um Termo de Referência específico para o caso sob investigação, que defina: (a) o escopo da investigação e os fatos sob apuração; (b) a divisão de tarefas e de responsabilidades; (c) o órgão líder, conforme os critérios do Protocolo de Definição de Autoridade Líder previsto na Seção 4.3; (d) um plano conjunto de diligências e de instrumentos padronizados de coleta (e.g. questionários e guias de auditoria comuns), de modo a assegurar a validade da prova nos processos de ambas as autoridades, a despeito da heterogeneidade dos ritos; (e) cronograma de atos processuais. A formalização desse instrumento antes da instauração de um processo administrativo confere previsibilidade tanto às autoridades quanto ao regulado e cria documento idôneo para dar subsídios para eventual controle judicial posterior.

(iii) *Formação de equipes mistas de apuração com instrução unificada:* o protocolo deve disciplinar a constituição de equipes mistas, integradas por servidores da ANPD e do regulador setorial, sob a coordenação da autoridade condutora definida na forma da Seção 4.3, incumbidas de conduzir, de forma unificada, a instrução probatória. Cada autoridade preserva o seu processo e o seu poder decisório, transpondo-se a lógica das operações conjuntas do art. 62 do RGPD sem incorrer em delegação vedada de competência sancionatória.

(iv) *Preservação da cadeia de custódia e criação de salvaguardas de sigilo na prova compartilhada:* o protocolo deve estabelecer cadeia de custódia rigorosa para a prova compartilhada, com registro de acesso e finalidade, e observar as salvaguardas de sigilo já delineadas para o sistema de informação compartilhado (Seção 4.4). A integridade e a rastreabilidade da prova são condição tanto de sua validade processual quanto da proteção dos direitos de terceiros.

4.7. Adoção de Matriz de Dosimetria Coordenada para Prevenção de *Bis in Idem* Administrativo

A consolidação da ANPD como agência reguladora e a sobreposição de competências sancionatórias entre a autoridade e os reguladores setoriais, bem como outros órgãos de controle, criam um risco concreto de duplicação de penalidades pelo mesmo fato. Um mesmo incidente de tratamento de dados pessoais pode, simultaneamente, configurar infração à LGPD e à regulação setorial, expondo o agente regulado à cumulação de sanções de idêntica natureza.

Quando duas autoridades, ainda que após coordenação investigativa, aplicam sanções autônomas sobre o mesmo fato gerador, abre-se espaço para violação ao princípio do *non bis in idem* administrativo e para desproporção do total sancionatório suportado pelo regulado.

A sétima recomendação deste Relatório enfrenta diretamente esse problema: a instituição de Matriz de Dosimetria Coordenada como cláusula obrigatória nos ACTs em vigor e nos futuros, com critérios técnicos para a fixação coerente da pena pecuniária quando houver concorrência sancionatória.

Síntese Objetiva: instituir, em coordenação com os reguladores setoriais, uma Matriz de Dosimetria Coordenada (a ser incorporada como cláusula obrigatória nos ACTs em vigor e nos futuros) destinada a assegurar que, na hipótese de sanções concorrentes relativas ao mesmo fato, as penalidades já aplicadas sejam consideradas na fixação das demais, de modo a preservar a proporcionalidade global da resposta sancionatória e a evitar a duplicação punitiva.

Fundamentação: No direito europeu, o artigo 83(3) do RGPD adota solução convergente ao estabelecer que, quando o responsável pelo tratamento infringe várias disposições do Regulamento no âmbito da mesma operação ou de operações ligadas, o montante total da coima não pode exceder o valor previsto para a infração mais grave. Embora o dispositivo europeu opere internamente a uma única autoridade, a lógica de teto unificado e de consideração conjunta das infrações ilumina o tratamento da pluralidade sancionatória. Neste particular, deve ser registrado que o Tribunal de Justiça da União Europeia já admitiu a duplicação de procedimentos punitivos apenas quando presentes fins complementares, coordenação suficiente entre as autoridades em um arco temporal próximo e proporcionalidade global das penalidades aplicadas.[114] A jurisprudência europeia, portanto, não veda a concorrência sancionatória, mas a condiciona à coordenação, precisamente o objeto da presente recomendação

O ordenamento brasileiro já oferece os alicerces normativos para a coordenação dosimétrica, embora dispersos e carentes de articulação operacional. No plano constitucional, a regra deflui dos princípios da proporcionalidade, da segurança jurídica e do devido processo legal substantivo (artigo 5º, inciso LIV). No plano infraconstitucional, o art. 22, § 3º, do Decreto-Lei n° 4.657, de 4 de setembro de 1942 (LINDB), com redação dada pela Lei n° 13.655, de 25 de abril de 2018, estabelece textualmente que “as sanções aplicadas ao agente serão levadas em

[114] Nesse precedente, o TJEU admitiu a duplicação de procedimentos e sanções de natureza administrativa pelo mesmo fato apenas se observadas condições estritas: fins complementares (objetivos de interesse geral distintos), coordenação suficiente entre as autoridades em um arco temporal próximo e proporcionalidade do conjunto das penalidades à gravidade da infração. Vide: TJUE. C-117/20, *bpost SA,* ECLI:EU:C:2022:202, j. em 22 mar 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62020CJ0117. Acesso em: 2 jun. 2026.

conta na dosimetria das demais sanções de mesma natureza e relativas ao mesmo fato", comando que cria, no direito positivo brasileiro, dever explícito de harmonização sancionatória entre autoridades administrativas. Já o artigo 52, § 1º, da LGPD condiciona a aplicação das sanções a um procedimento gradativo, isolado ou cumulativo, orientado por parâmetros e critérios objetivos, entre os quais a gravidade do fato, a vantagem auferida, a reincidência e o grau do dano.

Dificuldades para Adoção: O sincronismo decisório entre autoridades, condição necessária para a coordenação dosimétrica, esbarra em algumas dificuldades estruturais. A primeira é de natureza dogmática: a definição do que constitui "mesmo fato gerador" é tecnicamente complexa, dado que a mesma conduta empírica pode comportar valoração jurídica autônoma em cada regime (e.g. qualidade do serviço – ANATEL; resiliência operacional – BCB; defesa do consumidor – SENACON; e proteção de dados – ANPD). Neste particular, há pelo menos um precedente interessante do STJ, onde se afirma que o princípio do *non bis in idem* protege o sujeito de direito contra a repetição de processos (sucessivos) ou de punições de mesma natureza pelos mesmos fatos, mas não impede que diferentes legislações, com propósitos e com sanções distintas, sejam utilizadas conjuntamente para fundamentar uma ação judicial.[115]

Outras dificuldades têm natureza operacional. Isso porque, as agências guiam seus trabalhos por meio de regulamentos sancionadores autônomos, com prazos, instâncias recursais e critérios de dosimetria próprios. Este é o caso, por exemplo, da proteção de dados, uma vez que a Resolução CD/ANPD n° 4, de 24 de fevereiro de 2023, que regula a dosimetria das penas a serem aplicadas, opera com lógica setorialmente isolada, não prevendo, em sua redação atual, a aplicação prévia de sanção por outra autoridade administrativa apenas como circunstância modulatória da multa. Uma coordenação mais ampla da atuação sancionatória não só é possível, como já existe precedente no direito nacional, a saber, o Ato Normativo Conjunto BCB/CADE n° 1/2018, que demonstra a viabilidade doméstica da articulação dosimétrica entre autoridades concorrentes. Soma-se a isso a assincronia dos procedimentos administrativos: sanções relativas ao mesmo fato podem ser aplicadas em momentos distintos por autoridades diversas, dificultando a consideração recíproca exigida pelo artigo 22, § 3º da LINDB. Ademais,

[115] "(...) 2. A utilização conjunta das Leis n° 8.429/1992 (Lei de Improbidade Administrativa) e n° 12.846/2013 (Lei Anticorrupção) para fundamentar uma mesma ação civil não configura, por si só, violação ao princípio do *non bis in idem*. 3. É possível que as duas legislações sejam empregadas concomitantemente para fundamentar uma mesma ação ou diferentes processos, pois o que não é admissível é a imposição de sanções idênticas com base no mesmo fundamento e pelos mesmos fatos. (...) 4. A preocupação com a não sobreposição de penalidades deve ser devidamente examinada no momento da sentença, quando se analisará o mérito e a natureza das infrações, e não na fase preliminar da ação." BRASIL. Superior Tribunal de Justiça (Primeira Turma). REsp. n° 2.107.398/RJ, rel. Min. Gurgel de Faria. Brasília, j. em 18 fev. 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/07032025-Leis-Anticorrupcao-e-LIA-podem-ser-aplicadas-juntas--desde-que-nao-fundamentem-sancoes-identicas.aspx. Acesso em: 2 jun. 2026.

a inexistência de um cadastro compartilhado de penalidades agrava o problema, pois cada autoridade decide sem conhecimento sistemático das sanções já impostas pelas demais.

Por fim, acrescenta-se uma dificuldade institucional. A adoção de uma matriz comum pressupõe a autolimitação da atuação sancionatória de cada autoridade competente, bem como a superação de divergências metodológicas quanto à aferição da gravidade e do valor-base entre regimes sancionatórios setoriais heterogêneos. O fato é que cada autoridade tende a ver tais mecanismos como limitação de seu poder sancionatório, de modo que a coordenação dosimétrica exige um desenho institucional sensível a essa fronteira.

Medidas Concretas: A solução desses problemas exige a adoção de um protocolo interinstitucional de dosimetria,[116] seja por meio de ato normativo conjunto ou de previsão contratual específica, que articule os seguintes tópicos:

(i) *Cadastro compartilhado de sanções.* Criação de base de dados interinstitucional, com acesso restrito às autoridades signatárias, que registre as penalidades aplicadas em matéria de proteção de dados, permitindo a verificação tempestiva de sanções preexistentes antes da fixação de nova penalidade.

(ii) *Definição de arco temporal próximo:* A coordenação dos procedimentos sancionatórios deve ser realizada em arco temporal próximo, evitando-se uma indefinição prolongada das sanções regulatórias a serem aplicadas.

(iii) *Comunicação prévia de sanções regulatórias:* Quando houver aplicação de sanção regulatória sobre fato em coincidência material com competência do regulador parceiro, deve a autoridade sancionadora informar a autoridade concorrente sobre a decisão tomada, de modo que as sanções já aplicadas sejam consideradas na dosimetria subsequente, em concretização do art. 22, § 3º, da LINDB. Essa medida produz transparência sancionatória mútua e permite ajuste dosimétrico tempestivo, antes da formalização da decisão final.

[116] Diversos desses critérios foram expressamente adotados pelo TJUE, ao definir que duplicação de procedimentos sancionatórios sobre os mesmos fatos só é compatível com o princípio *ne bis in idem* quando estiverem reunidas, cumulativamente, as seguintes condições: (a) existência de regras claras e precisas que permitam prever quais atos ou omissões são suscetíveis de ser objeto de cúmulo de procedimentos e sanções, bem como prever que haverá coordenação entre as autoridades competentes; (b) que os dois procedimentos tenham sido conduzidos de forma suficientemente coordenada e num intervalo temporal próximo (*proximate timeframe*); e (c) que as sanções globalmente impostas correspondam à gravidade das infrações cometidas, devendo a penalidade eventualmente aplicada no primeiro procedimento ser levada em conta na fixação da segunda, de modo que o ônus resultante da duplicação se limite ao estritamente necessário. Além disso, foi sublinhado que essa apreciação de proporcionalidade global só pode ser plenamente realizada *ex post*, exigindo, em todo caso, a demonstração de um nexo suficientemente estreito, em substância e no tempo, entre os dois conjuntos de procedimentos envolvidos. TJUE. C-117/20, *bpost SA*, ECLI:EU:C:2022:202, j. em 22 mar 2022, par. 48-51, 53 e 58. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62020CJ0117. Acesso em 2 jun. 2026.

(iv) *Critério de absorção qualificada por preponderância*: Quando o desvalor material da conduta for inteiramente absorvido pelo enquadramento mais grave de uma das autoridades, a sanção deve ser aplicada exclusivamente por esta autoridade, conforme o critério da preponderância do bem jurídico tutelado, já adotado no Protocolo de Autoridade Líder (Seção 4.3). Trata-se de adaptação operacional do princípio do *non bis in idem* ao contexto de competências concorrentes, evitando a multiplicação sancionatória sobre o que é, materialmente, um único ilícito.

(v) *Previsão de compensação proporcional para bens jurídicos distintos, mas conexos:* Quando, ao revés, o fato afeta simultaneamente bens jurídicos distintos (e.g. qualidade do serviço de telecomunicações e proteção de dados pessoais), cada autoridade deve manter competência sancionatória autônoma, mas obriga-se contratualmente a considerar, na dosimetria, a sanção previamente aplicada pela outra. O total acumulado das sanções não deve, em qualquer hipótese, ultrapassar o limite que seria proporcional à gravidade total do fato.

4.8. Participação da ANPD nas Análises de Impacto Regulatório (AIRs) Setoriais com Repercussão sobre Dados Pessoais

A coordenação interinstitucional não se esgota na atuação repressiva ou na resolução de conflitos de competência (*ex post*). O ideal é que ela também seja exercida de forma preventiva, sobretudo, na fase pré-normativa, quando os reguladores setoriais concebem atos que repercutem sobre o tratamento de dados pessoais. De fato, a atuação da regulação setorial (e.g. sistema financeiro, telecomunicações, saúde suplementar, seguros etc.) frequentemente disciplina fluxos de dados pessoais sem a qualquer participação técnica da ANPD. Isso é ainda mais relevante quando uma intervenção normativa pode gerar um alto impacto nos mercados, casos em que a legislação costuma exigir a produção de uma Análise de Impacto regulatório (AIRs),[117] um processo sistemático que utiliza evidências para avaliar os possíveis impactos, custos e benefícios de novas regulamentações antes de sua aprovação, cujo objetivo é garantir que a intervenção do Estado seja necessária, eficiente e traga os melhores resultados para a sociedade.

A nossa oitava recomendação consiste, portanto, na institucionalização da participação da ANPD nas Análises de Impacto Regulatório (AIRs) setoriais cujo objeto envolva, direta ou indiretamente, o tratamento de dados pessoais, mediante a sua consulta prévia nas hipóteses materialmente relevantes.

[117] Vide: Artigo 6º da Lei n° 13.848, de 25 de junho de 2019 (Lei das Agências Reguladoras); Artigo 5º da Lei n° 13.874, de 20 de setembro de 2019 (Lei da Liberdade Econômica).

Síntese Objetiva: Articular, com os demais reguladores setoriais, mecanismos institucionais de participação da ANPD nas Análises de Impacto Regulatório (AIRs) sempre que a proposta normativa setorial envolva tratamento de dados pessoais e possa atingir direitos dos titulares, mediante consulta prévia.

Fundamentação: A AIR é instrumento já consolidado no ordenamento brasileiro. Ela foi instituída como obrigação legal às Agências Reguladoras pelo artigo 6º da Lei n° 13.848, de 25 de junho de 2019 (LAR), o qual estabelece que "a adoção e as propostas de alteração de atos normativos de interesse geral dos agentes econômicos, consumidores ou usuários dos serviços prestados serão, nos termos de regulamento, precedidas da realização de Análise de Impacto Regulatório (AIR), que conterá informações e dados sobre os possíveis efeitos do ato normativo". Esse dever foi reforçado pelo artigo 5º da Lei n° 13.874/de 2019 (Lei da Liberdade Econômica) e, no que diz respeito à ANPD, pelo artigo 55-J, inciso XXIII e §2°, que (a) determina sua articulação com as demais autoridades reguladoras para o exercício das suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação e (b) exige que as regulamentações e normas editadas pela ANPD deverão ser precedidas consulta e audiência públicas, bem como de análises de impacto regulatório.

De fato, a participação da ANPD nas AIRs ajudaria a concretizar os mandamentos legais, conferindo-lhe eficácia operacional na fase pré-normativa. Todavia, no atual cenário regulatório brasileiro, inexiste mecanismo formal que assegure a participação da ANPD nas AIRs realizadas por outros reguladores quando o setor regulado demande tratamento de dados pessoais. A lacuna é particularmente grave em quatro domínios específicos: (a) regulamentações da ANATEL sobre redes 5G, IoT e segurança cibernética, que envolvem tratamento massivo de dados de localização, conexão e cadastrais; (b) regulamentações do BCB sobre *Open Finance*, PIX e Drex, tecnologias estruturadas sobre compartilhamento intensivo de dados pessoais financeiros; (c) regulamentações da ANS sobre *Open Health*, prontuários eletrônicos e padrões TISS, que tratam dados sensíveis de saúde; (d) regulamentações da ANVISA sobre *Software as a Medical Device* (SaMD) e pesquisa clínica, alcançando dados genéticos e biométricos.

Em termos dogmáticos, a omissão na consulta a autoridade tecnicamente especializada acaba comprometendo a robustez motivacional do ato normativo. Lembre-se que o artigo 50, inciso II, da Lei n° 9.784, de 29 de janeiro de 1999 (Lei do Processo Administrativo) exige que os atos administrativos sejam motivados "com indicação dos fatos e dos fundamentos jurídicos, quando imponham ou agravem deveres, encargos ou sanções", exigência cuja densidade aumenta proporcionalmente à complexidade técnica do objeto regulado. Atos normativos setoriais que disciplinam tratamento massivo de dados pessoais sem oitiva prévia da autoridade competente em matéria de proteção de dados (no caso a ANPD) ficam expostos, no plano substantivo, à crítica de insuficiência motivacional.

A literatura especializada afirma que sistemas regulatórios maduros costumam operar por meio de mecanismos formais,[118] sendo o mecanismo de *cross-consultation* prévia entre autoridades um dos instrumentos mais poderosos de coordenação interinstitucional.[119] No direito europeu, o European Data Protection Board (EDPB) estabeleceu, recentemente, um subgrupo de trabalho dedicado a *cross-regulatory interplay and cooperation* e adotou, em parceria com a Comissão Europeia, as primeiras *joint guidelines* sobre a interação entre o *Digital Markets Act* (DMA) e o RGPD, modelo que demonstra a possibilidade institucional da coordenação *ex ante* entre autoridades com competências sobrepostas.[120] Esse desenho também corresponde ao papel desempenhado, nos Estados Unidos, pelo *Office of Information and Regulatory Affairs* (OIRA), no exame *ex ante* das regulações federais.[121]

Dificuldades para Adoção. A dificuldade mais óbvia para adoção desse modelo de *cross-consultation* é de natureza dogmática. Isso porque, a delimitação do critério de consulta obrigatória (ou seja, definir quando uma proposta "repercute sobre o tratamento de dados pessoais, colocando em risco direitos fundamentais dos titulares" comporta zona cinzenta, sujeita a controvérsia interpretativa. Como se não bastasse, quase toda regulação contemporânea envolve, em alguma medida, tratamento de dados pessoais, o que torna o critério potencialmente sobreincluivo. Quaisquer critérios objetivos que venham a servir de gatilho para a consulta da ANPD por de agências setoriais devem ser muito bem delimitados, inclusive para que o processo não seja banalizado.

Acrescente-se, aqui, a questão da capacidade institucional. Parece óbvio que participação tempestiva e qualificada em múltiplas AIRs setoriais exige da ANPD recursos técnicos e humanos que tendem a ser escassos na fase inicial de sua atuação como agência reguladora. É razoável, portanto, supor que a adoção integral e simultânea da medida em todos os setores seja inviável no curto prazo, recomendando-se implantação gradual e priorização por critérios de risco.

Por fim, há um problema de ordem operacional: a potencial morosidade do procedimento de consulta. A integração com o ciclo regulatório das demais agências exige sincroniza-

[118] Freeman, J., & Rossi, J. (2011). *Agency Coordination in Shared Regulatory Space*. Harvard Law Review, *125*, 1131-1211. https://doi.org/10.2139/ssrn°1778363. Acesso em 01 jun 2026.
[119] Wang, J., Ulibarri, N°, & Scott, T. A. (2024). *Agency consultation networks in environmental impact assessment*. Journal of Public Administration Research and Theory. https://doi.org/10.1093/jopart/muae008, Acesso em 01 mai 2026
[120] Sobre a iniciativa europeia, v. EUROPEAN DATA PROTECTION BOARD. *EDPB Conference "Cross-regulatory cooperation in the EU2*. Disponível em: https://www.edpb.europa.eu/. Acesso em 22 mai 2026.
[121] Sobre o papel do OIRA na arquitetura regulatória norte-americana e a importância da revisão interagência *ex ante*, v. SUNSTEIN, Cass R. *The Office of Information and Regulatory Affairs: Myths and Realities*. Harvard Law Review, vol. 126, 2013.

ção de prazos, calendários e critérios metodológicos, sem que exista, hoje, padronização correspondente. Além disso, a inserção de nova etapa consultiva pode ser percebida pelos reguladores setoriais como potencial ameaça às respectivas autonomias e como obstáculo ao seu fluxo normativo, sobretudo diante de prazos regulatórios exíguos.

Medidas Concretas: As possíveis soluções dos problemas acima arrolados devem ser, simultaneamente, desenhadas com respeito à autonomia decisória dos reguladores setoriais, capazes de produzir coordenação *ex ante*[122] efetiva e calibrada de acordo com as capacidades institucionais da ANPD:

(i) *Matriz objetiva de hipóteses de consulta obrigatória:* A adoção da consulta prévia obrigatória à ANPD por outros reguladores (seja por ato normativo conjunto ou por ACTs) de parâmetros objetivos que identifiquem as propostas com repercussão sobre dados pessoais deve restrita a casos materialmente relevantes definidos por matriz objetiva: a) regulamentos que prevejam tratamento de dados pessoais sensíveis em larga escala, b) tratamentos que envolvam dados de crianças e adolescentes; c) uso de sistemas de inteligência artificial com impacto sobre direitos fundamentais; d) compartilhamento compulsório de dados pessoais entre agentes regulados etc. A delimitação objetiva mitiga os riscos de sobrecarga acima indicadas e confere previsibilidade aos reguladores setoriais.

(ii) *Implantação gradual e priorização por risco.* Adoção em fase das hipóteses de participação, iniciando pelos setores de maior densidade de tratamento de dados pessoais e maior potencial de risco aos titulares, com expansão progressiva à medida que a capacidade institucional da ANPD se consolide.

(iii) *Parecer técnico na fase de AIR:* Inserção, no procedimento de AIR dos reguladores setoriais, de etapa de manifestação técnica da ANPD, com prazo definido, de modo que a perspectiva de proteção de dados integre o relatório submetido ao conselho diretor ou à diretoria colegiada.[123]

(iv) *Caráter recomendativo da manifestação*: A manifestação da ANPD deve ter caráter estritamente recomendativo, jamais vinculante. Esse desenho preserva, de um lado, a autonomia decisória do regulador setorial (em consonância com o artigo 3º da Lei n°

[122] Note-se que já há precedente normativo que adota um modelo *ex post* de participação da ANPD. A Resolução ANATEL n° 767, de 7 de agosto de 2024 prevê fluxo institucional de comunicação com a ANPD em incidentes envolvendo dados pessoais. Nada impede que esse modelo de cooperação *ex post* seja estendido para a *fase ex ante* de edição normativa, mediante cláusula nos ACTs setoriais obrigando a notificação à ANPD da abertura de processos regulatórios cuja AIR aponte tratamento de dados pessoais com potencial risco aos direitos fundamentais dos titulares como elemento material.

[123] Exigência contida no artigo 6º, § 3º da Lei n° 13.848, de 25 de junho de 2019 (LAR).

13.848, de 25 de junho de 2019) e evita, de outro, transformar a consulta em mecanismo de tutela administrativa indireta. Note-se, no entanto, que o não acolhimento das recomendações da ANPD deve ser devidamente fundamentada pelo regulador setorial, exigência derivada do próprio artigo 50, inciso II, da Lei n° 9.784, de 29 de janeiro de 1999.

4.9. Criação do Programa Estruturado de Capacitação Conjunta e Intercâmbio de Servidores

Todas as recomendações precedentes são focadas no esboço de uma arquitetura institucional, normativa e procedimental da coordenação interinstitucional da ANPD com outros agentes regulatórios. Todavia, o efetivo sucesso dessa coordenação depende, em larga medida, da existência de um substrato cognitivo comum entre as autoridades envolvidas: a qualificação técnica e do capital relacional dos servidores que o operam, variáveis habitualmente subestimadas nos desenhos formais de cooperação regulatória. De fato, a proteção de dados pessoais e a regulação setorial operam com vocabulários técnicos, métodos e culturas institucionais distintos, o que dificulta o diálogo qualificado nas relações coordenadas. A ausência de capacitação cruzada pode acabar convertendo a sobreposição de competências em assimetria de compreensão, comprometendo a qualidade das decisões interinstitucionais.

A nona recomendação deste relatório consiste, portanto, na criação de Programa Estruturado de Capacitação Conjunta e Intercâmbio de Servidores entre a ANPD e os reguladores setoriais prioritários, concebido em dois pilares articulados: capacitações conjuntas com metodologia ativa e intercâmbio temporário de servidores (*secondments*) por períodos definidos.

Síntese Objetiva: Instituir um Programa Estruturado de Capacitação Conjunta e Intercâmbio Temporário de Servidores entre a ANPD e os reguladores setoriais prioritários, que contenha (a) trilhas conjuntas de aprendizagem com metodologias ativas (e.g. estudos de caso, *tabletop exercises* etc.) e (b) intercâmbio temporário (*secondments*) por períodos definidos, valendo-se dos institutos da cessão e da requisição previstos no artigo 93 da Lei n° 8.112, de 11 de dezembro de 1990. Essa medida terá potencial de constitui a infraestrutura humana da coordenação, com a transferência bidirecional de conhecimento e a formação das redes de confiança interpessoal, indispensáveis à coordenação interinstitucional, sem o que os instrumentos formais de articulação tendem a permanecer subutilizados.

Fundamentação: A eficácia de qualquer arranjo institucional depende da qualificação técnica das pessoas que o operam. No entanto, a proteção de dados é disciplina relativamente recente

no ordenamento brasileiro, e sua interseção com regulações setoriais complexas exige perfil profissional altamente especializado. Por isso, seria normal esperar que os servidores das agências setoriais não tenham muita familiaridade com a LGPD, do mesmo modo que os servidores da ANPD não sejam devidamente capacitados para atuar nas áreas setorialmente reguladas.

Os programas de capacitação interinstitucional servem, portanto, a um duplo propósito estratégico. Primeiro, nivelam o conhecimento técnico em via dupla: servidores da ANPD assimilam as dinâmicas de mercado, os modelos de negócios e os riscos específicos dos setores regulados, ao passo que servidores das agências setoriais podem aprofundar seus conhecimentos na área da proteção de dados. Segundo – e operacionalmente decisivo – podem produzir redes informais de contato e relações de confiança interpessoal entre as burocracias, que servem como camada lubrificante quando a coordenação formal por ofícios e despachos é insuficiente para resposta tempestiva.

Esse intercâmbio de conhecimentos especializados pode ser realizado por duas modalidades operacionais, com lógicas distintas. De um lado, as capacitações conjuntas (e.g. cursos, workshops, simulações etc.) têm alcance amplo e baixo custo unitário, mas geram conhecimento mediado pela situação artificial do treinamento. De outro lado, o intercâmbio temporário (*secondments*) tem alcance restrito e custo institucional maior, mas produz aprendizagem imersiva, onde o servidor experimenta diretamente as restrições, prioridades e culturas decisórias do órgão receptor. Ambas as modalidades são complementares, e nenhuma substitui a outra.

O ordenamento brasileiro oferece base normativa para essa medida. O artigo 30 da Lei n° 13.848, de 25 de junho de 2019 autoriza as agências reguladoras a constituir comitês para o intercâmbio de experiências e informações entre si, com vistas a estabelecer orientações e procedimentos comuns para o exercício da regulação. Ademais, a matriz geral de desenvolvimento de pessoal no serviço público federal, criada pelo Decreto n° 9.991, de 20 de agosto de 2019 (Política Nacional de Desenvolvimento de Pessoas – PNDP), também reforça a viabilidade da proposta. Note-se, ainda, que os programas de capacitação conjunta podem ser realizado com o auxílio das escolas de governo (notadamente a Escola Nacional de Administração Pública – ENAP) e com o aproveitamento da estrutura de ações de desenvolvimento já previstas, o que reduz o custo institucional de implantação.

No direito comparado, o Comitê Europeu de Proteção de Dados (EDPB) mantém, desde 2022, o *Support Pool of Experts* (SPE), programa destinado a aumentar a capacidade de supervisão e *enforcement* das autoridades nacionais mediante desenvolvimento de ferramentas comuns e acesso a um corpo qualificado de especialistas, com ações de capacitação e produção de

material formativo.[124] Embora opere em contexto supranacional distinto, o SPE ilustra que a construção de capacidade técnica compartilhada é reconhecida internacionalmente como instrumento de coordenação regulatória—parâmetro que ilumina, sem importar acriticamente, a solução brasileira. Já no Reino Unido, o *Digital Regulation Cooperation Forum* (DRCF), além de operar com um quadro permanente de cerca de vinte servidores, integralmente cedidos pelos reguladores-membros ou contratados por arranjo com o Ofcom, instituiu, em seu *Workplan 2025/26*, um programa formal de mentoria de competências digitais (*digital skills mentoring programme*) entre as autoridades-membro, com previsão expressa de *secondments* cruzados como instrumento de coordenação institucional.[125]

Dificuldades para Adoção. A dificuldade mais óbvia é de natureza estrutural: o intercâmbio de servidores pressupõe disponibilidade de quadros e mecanismos de cessão ou movimentação que nem sempre dependem exclusivamente dos agentes regulatórios envolvidos ou são limitadas devido a restrições de lotação nas autoridades envolvidas, sobretudo da ANPD, ainda em fase de estruturação como agência reguladora.

Como se não bastasse, há sempre o risco de descontinuidade do programa. A uma, porque o contingenciamento de despesas discricionárias, recorrente na administração federal, alcança tipicamente os programas de capacitação. Outrossim, programas pontuais geram impacto limitado, e a rotatividade de servidores no governo federal (especialmente em cargos comissionados) exige institucionalização permanente, sob pena de perda do conhecimento adquirido a cada saída funcional.

Outro possível entrave decorre da heterogeneidade dos regimes jurídicos de pessoal e das culturas institucionais, que pode gerar resistências à mobilidade e dificuldades de reconhecimento recíproco das atividades desenvolvidas durante o intercâmbio. Ademais, é razoável supor que a ausência de incentivos formais à participação (na progressão funcional ou na avaliação de desempenho) tende a reduzir a adesão voluntária dos servidores ao programa.

Por fim, pode haver um obstáculo metodológico. Treinamentos excessivamente teóricos ou genéricos, limitados à apresentação do texto da LGPD sem conexão com as realidades setoriais, produzem baixo engajamento e pouca aplicação prática. O risco é tanto maior quanto

[124] De acordo com o objetivo declarado, o SPE tem por objetivo, "to help European Data Protection Authorities (DPAs) increase their capacity to supervise and enforce data protection rules by developing common tools and giving them access to a wide pool of experts". Sobre o assunto, vide: https://www.edpb.europa.eu/support-pool-experts-spe-programme_en. Acesso em 01 jun 2026.

[125] Sobre o DRCF, vide: *Workplan 2025/26,* esp. a área de trabalho *Skills and Capabilities*. Disponível em: https://www.drcf.org.uk/projects/projects/skills-and-capabilities. Acesso em 01 jun 2026

mais sofisticado é o público, pois servidores experientes desinteressam-se rapidamente de conteúdos descolados de sua rotina decisória.

Medidas Concretas: Esses problemas podem ser contornados ou mitigados por algumas medidas operacionais, gradativas e compatíveis com as restrições de pessoal da ANPD:

(i) *Aproveitamento da infraestrutura existente e curadoria de conteúdo:* A Escola Nacional de Administração Pública (ENAP) e algumas escolas de governo dos órgãos e entidades reguladores já dispõem de infraestrutura física e digital adequada. A Escola Virtual de Governo (EV.G), operada pela ENAP, já hospeda uma trilha de proteção de dados e segurança da informação. [126] A ANPD pode, em conjunto com os agentes setoriais, atuar como curadora de conteúdo, desenvolvendo trilhas setoriais específicas, sem necessidade de construção de plataforma própria.

(ii) *Metodologia ativa baseada em casos reais e simulações*: Trilhas e *workshops* conjuntos devem estruturar-se em torno de *tabletop exercises*, nos quais os servidores simulam a resposta a incidente real (e.g. vazamento de chaves PIX, exposição de dados cadastrais em operadora móvel, comprometimento de prontuário eletrônico etc.) e são compelidos a navegar pelas sobreposições normativas em ambiente controlado. O modelo *learning-by-doing* é qualitativamente superior à aula expositiva tradicional, com a vantagem de ajudar a construir laços de confiança recíproca e mapas mentais compartilhados.

(iii) *Programa de intercâmbio temporário.* Instituição de regime de intercâmbio por prazo determinado, mediante os instrumentos de movimentação e cooperação técnica admitidos em lei, que permita ao servidor atuar temporariamente na autoridade parceira, com clareza quanto à lotação, às atribuições e ao retorno ao órgão de origem. Os ACTs devem prever expressamente essa modalidade de cooperação, com duração padrão entre seis e doze meses (período suficiente para imersão efetiva no órgão receptor sem comprometimento prolongado do órgão cedente), definição de objetivos pedagógicos verificáveis, plano de trabalho do servidor cedido e relatório final de transferência de conhecimento à equipe de origem.

(iii) *Institucionalização permanente do Programa*: Recomenda-se que o Programa Permanente de Capacitação Interinstitucional contenha (a) calendário anual de atividades, (b) orçamento dedicado no Plano de Dados Abertos e na Lei Orçamentária Anual e (c) indicadores objetivos de participação, satisfação e aplicação prática do conhecimento

[126] Sobre os cursos atuais da EV.G/ENAP em proteção de dados, vide:. https://www.enap.gov.br/acontece/noticias/enap-lanca-trilha-de-aprendizagem-para-privacidade-e-seguranca-da-informacao/. Acesso em 22 mai 2026.

adquirido. Além disso, a participação em capacitações interinstitucionais deve ser considerada, nos termos da legislação aplicável, como critério de progressão funcional, criando incentivo institucional explícito ao engajamento e à institucionalização do conhecimento gerado, contramedida capaz de mitigar a perda informacional

4.10. Criação do Observatório Interinstitucional de Coordenação Regulatória da ANPD

As recomendações precedentes foram destinadas ao desenho da arquitetura institucional, normativa, procedimental e funcional da coordenação interinstitucional. Todas compartilham uma premissa básica: a coordenação interinstitucional é processo contínuo, não evento isolado. Sem a criação de uma instância reflexiva, os resultados das ações sugeridas não podem ser avaliados, com comprometimento do efetivo aperfeiçoamento regulatório coordenado. Sem a previsão de uma instância que monitore sua implementação, sistematize dados e produza conhecimento sobre a interação entre a proteção de dados e a regulação setorial, há risco de que os instrumentos de articulação permaneçam fragmentados e sem avaliação de efetividade da atuação regulatória coordenada. O fato é que a ausência de memória institucional e de métricas de coordenação tendem a perpetuar decisões *ad hoc*, refratárias ao aprendizado acumulado.

A décima e última recomendação deste relatório consiste, portanto, na criação de Observatório Interinstitucional de Coordenação Regulatória da ANPD, estrutura técnica permanente destinada a converter a coordenação interinstitucional, hoje exercida de modo fragmentário, em política institucional estruturada, monitorada e iterativamente aprimorada.

Síntese Objetiva: Instituir o Observatório Interinstitucional de Coordenação Regulatória, estrutura técnica permanente vinculado à ANPD, com a função de monitorar a implementação das medidas de articulação, sistematizar os dados sobre atuação conjunta, consolidar indicadores qualitativos e quantitativos, produzir o Relatório Anual de Coordenação Interinstitucional e fornecer subsídios para a atualização da sua Agenda Regulatória. O Observatório confere caráter reflexivo e cumulativo à coordenação, transformando práticas dispersas em política institucional avaliável.

Fundamentação: A ANPD já dispõe de instrumentos centrais de planejamento estratégico. O Mapa de Temas Prioritários para Fiscalização (biênio 2026-2027) e a Agenda Regulatória atualizada para o biênio 2025-2026 foram aprovados pelas Resoluções CD/ANPD n° 30 e n° 31, ambas de 24 de dezembro de 2025, e estruturam as prioridades em quatro eixos materiais: (a)

direitos dos titulares; (b) proteção de crianças e adolescentes no ambiente digital; (c) tratamento de dados pessoais por autoridades públicas; e (d) inteligência artificial e tecnologias emergentes. Esses instrumentos, embora robustos, ainda não contemplam de modo sistemático a dimensão da coordenação interinstitucional como eixo autônomo de planejamento, lacuna que o Observatório se propõe a preencher.

Não se deve esquecer, outrossim, que a transparência e a *accountability* são princípios constitucionais consagrados no artigo 37, *caput* da Constituição da República e, em matéria de proteção de dados, mandatários por força do artigo 6º, incisos VI e X da LGPD. O Observatório, por meio de um Painel Público e de seu Relatório Anual, atende simultaneamente a esses deveres legais e ao princípio republicano da prestação de contas, ampliando-os para a dimensão da função coordenadora exercida pela ANPD.

Ademais, parece óbvio que a ANPD é o como *locus* adequado para sediar tal instância reflexiva. A uma, porque compete à ANPD, por força de lei, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade,[127] bem como sistematizar o conhecimento sobre a coordenação regulatória.[128] A duas, porque a vinculação do Observatório à ANPD seria uma forma de dar alguma materialidade ao artigo 55-J, §4º da LGPD, que lhe impõe a manutenção de fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.[129]

A experiência comparada confirma a utilidade do instrumento. No direito europeu, o EDPB publica relatório anual com indicadores objetivos de cooperação entre as autoridades nacionais. O *Annual Report 2025* registra, por exemplo, 414 casos transfronteiriços, 1.299 procedimentos de *one-stop-shop* e 572 decisões finais,[130] dados que permitem a avaliação empírica do efetivo funcionamento dos mecanismos de atuação interinstitucional. Já o DRCF britânico publica um *Annual Report* estruturado por *workstreams* temáticos, com prestação de contas específica sobre cada eixo de cooperação.[131]

No Brasil, há precedente operacional verificado: o Painel da Lei de Acesso à Informação, operado pela Controladoria-Geral da União (CGU), cuja nova versão foi lançada em setembro

[127] Artigo 55-J, inciso VII da LGPD.
[128] Artigo 55-J, inciso XXIII da LGPD.
[129] Sobre as dificuldades enfrentadas pela ANPD na criação dessa instância, confira-se a Seção 2.5. do presente relatório
[130] EUROPEAN DATA PROTECTION BOARD. *EDPB Annual Report 2025: Clarity in Action – Supporting Stakeholders through Guidance and Dialogue*. Bruxelas: EDPB, 9 abr. 2026. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2025_en. Acesso em: 1 jun. 2026.
[131] DIGITAL REGULATION COOPERATION FORUM. *DRCF 2025/26 Annual Report*. Londres: DRCF, 27 abr. 2026. 23 p. Disponível em: https://www.drcf.org.uk/publications/annual-reports. Acesso em: 1 jun. 2026.

de 2025, demonstra a viabilidade técnica e o impacto institucional de painéis públicos sobre dados regulatórios sensíveis. O Acordo de Cooperação Técnica firmado entre ANPD e CGU em 17 de maio de 2023 fornece base institucional para articulação metodológica entre ambas as Autoridades.[132] Nada impede que esse modelo seja ser expandido para incluir os resultados da atuação coordenada da ANPD com todos os demais agentes regulatórios setoriais.

Dificuldades para Adoção: A primeira dificuldade é a sustentabilidade da estrutura no contexto de quadro funcional restrito. A criação de unidade técnica permanente exige alocação de servidores que poderiam ser destinados às atividades finalísticas de fiscalização e normatização, restrição agravada pelo fato de que os 200 cargos de Especialista em Regulação de Proteção de Dados autorizados pelo artigo 9º da Lei n° 15.352, de 25 de fevereiro de 2026 ainda dependem de concurso público para preenchimento.

Outro obstáculo é de natureza metodológica. A construção de indicadores demanda cuidado técnico significativo. Isso porque, indicadores excessivamente quantitativos (e.g. número de reuniões realizadas, ACTs assinados etc.) tendem a induzir comportamentos formais sem ganho substantivo (*goodhart effect*). Indicadores qualitativos, mais precisos quanto aos resultados, demandam expertise de avaliação ainda escassa no setor público brasileiro. Cada órgão parceiro mantém sistemas de registro distintos, métricas heterogêneas e calendários de prestação de contas divergentes, o que torna a consolidação de dados intrinsecamente difícil.

A governança e a partilha de dados também podem ser problemáticas. Isso porque, o monitoramento pressupõe acesso a informações das diversas autoridades, o que reintroduz as questões de sigilo, base legal e interoperabilidade tratadas na recomendação relativa ao sistema de informação compartilhado. É razoável supor que a adesão dos reguladores setoriais seja gradual, condicionada à percepção de benefício recíproco e à preservação de suas competências. Além disso, a publicação de informações sobre ações cooperativas pode gerar tensões entre reguladores, especialmente se a divulgação for percebida como ranking comparativo entre autoridades.

Por fim, deve ser colacionado o risco (operacionalmente crítico) de degeneração formal: tanto o Observatório quanto o Relatório Anual podem tornar-se estruturas produtoras de documentos sem efeito prático. A proliferação de relatórios meramente protocolares na Administração Pública é fenômeno documentado que o desenho do Observatório deve combater explicitamente. A utilidade da instância depende de sua capacidade de influenciar decisões, o que

[132] Sobre o Painel da Lei de Acesso à Informação, vide: https://centralpaineis.cgu.gov.br/visualizar/lai e https://www.gov.br/cgu/pt-br/assuntos/noticias/2025/09/cgu-lanca-novo-painel-lai, (CGU lança novo Painel LAI, set 2025). O ACT entre ANPD e CGU foi celebrado em 17 de maio de 2023, em evento comemorativo aos 11 anos da LAI, e está disponível aqui: https://basedeconhecimento.cgu.gov.br/items/942f1d24-0142-403b-adae-6ac972ba4bb0. Acesso em 22 mai 2026.

exige vínculo claro entre seus produtos analíticos e os processos de articulação examinados nos itens anteriores. Se o relatório não apresentar autocrítica honesta sobre os desafios da coordenação, ele perderá utilidade como instrumento de gestão e aprimoramento institucional.

Medidas Concretas: Recomendam-se as seguintes medidas, voltadas a assegurar efetividade e legítima governança compartilhada:

(i) *Escopo material bem definido.* Delimitação precisa das funções do Observatório, que devem incluir obrigatoriamente o monitoramento da implementação das recomendações, sistematização de conflitos de competência, produção de estudos e formulação de propostas.

(ii) *Indicadores em três dimensões complementares:* O sistema de monitoramento deve articular: a) indicadores de processo (e.g. ACTs vigentes, grau de implementação dos planos de trabalho, GTs ativos, reuniões realizadas etc.); b) indicadores de produto (guias setoriais conjuntos publicados, resoluções conjuntas editadas, *sandboxes* em operação, harmonizações normativas concretas etc.); c) indicadores de resultado (e.g. redução do tempo médio de resposta a incidentes multissetoriais, redução de divergências interpretativas mensuráveis por análise de litigância judicial, redução de conflitos de competência levados à apreciação superior, satisfação dos regulados aferida em pesquisas anuais etc.). Seria prudente que os indicadores sejam estabelecidos em conjunto com os órgãos parceiros desde o início de cada ciclo, assegurando comparabilidade e validação metodológica interinstitucional.

(iii) *Articulação do Observatório com outras recomendações:* na medida do possível, o Observatório deve ter acesso às informações geradas pelos outros instrumentos de coordenação regulatórias sugeridos neste relatório, como o sistema de informação compartilhado, os protocolos de incidentes e de fiscalização conjunta e a matriz de dosimetria coordenada, de modo que o monitoramento se nutra dos dados gerados por esses instrumentos e retroalimente seu aprimoramento.

(iv) *Governança compartilhada:* Na medida do possível, o Observatório deve operar como um Conselho Consultivo Interinstitucional, composto por representantes designados pelos órgãos parceiros nos ACTs, com reuniões trimestrais para validação dos dados e alinhamento metodológico. A composição colegiada mitiga o risco apontado na terceira dificuldade (ranking comparativo unilateral) e produz, simultaneamente, apropriação institucional do diagnóstico, condição operacional para que as recomendações do Relatório sejam efetivamente acolhidas no ciclo seguinte.

(v) *Relatório periódico de coordenação:* Publicação de relatório periódico, à semelhança do modelo do CEF europeu, que apresente indicadores de coordenação, achados e recomendações, conferindo transparência e *accountability* à política de articulação interinstitucional.

(vi) *Integração obrigatória com os demais instrumentos:* O Relatório Anual deve adotar estrutura padronizada contendo, pelo menos, quatro seções: a) balanço dos ACTs vigentes e seu grau de implementação; b) "Casos de Coordenação", com análise detalhada das atuações conjuntas do período; c) "Lições Aprendidas e Desafios", com exposição transparente das dificuldades (contramedida explícita ao risco de degeneração formal); e d) "Agenda Prospectiva", com as prioridades de cooperação para o ciclo seguinte. As conclusões do Relatório e os dados do Painel Público devem constituir, por norma expressa, insumos obrigatórios da elaboração das Agendas Regulatórias bienais e do Mapa de Temas Prioritários para Fiscalização, fechando o ciclo de aprendizado institucional.

Considerações Finais

As considerações finais deste relatório consolidam o diagnóstico empírico e as reflexões teóricas desenvolvidas ao longo do trabalho do Grupo de Trabalho sobre Coordenação Interinstitucional e Eficiência Administrativa (GT3), evidenciando que a transversalidade da proteção de dados pessoais no Brasil exige a superação de uma atuação isolada em prol de uma governança regulatória integrada e cooperativa. Isso porque, a implementação da LGPD inaugurou um novo paradigma normativo que irradia seus efeitos por todas as verticais da economia e da administração pública, interceptando competências consolidadas de agências reguladoras setoriais e órgãos de controle pré-existentes. Longe de ser um fenômeno patológico, a sobreposição de competências regulatórias (*regulatory overlap*) constitui uma característica inerente à organização administrativa contemporânea, cujos efeitos dependem crucialmente da maturidade dos mecanismos de coordenação adotados pelo Estado. Enquanto a sobreposição desordenada acarreta ineficiência administrativa, insegurança jurídica, elevação dos encargos de conformidade e o risco de *bis in idem* sancionatório, a cooperação estruturada é capaz de converter a redundância de controle em resiliência sistêmica, aproveitando a expertise especializada de cada órgão para garantir uma proteção mais robusta e homogênea aos titulares de dados.

O exame do cenário internacional revela um repertório consolidado de boas práticas para a gestão de competências concorrentes na economia digital, com destaque para fóruns permanentes de cooperação, como (a) o *Coordinated Enforcement Framework* (CEF/EDPB) eu-

ropeu, (b) o *Digital Regulation Cooperation Forum* (DRCF) do Reino Unido, (c) o *Office of Information and Regulatory Affairs* (OIRA) dos Estados Unidos e (d) o *Digital Platform Regulators Forum* (DP-REG) da Austrália. No contexto brasileiro, contudo, a arquitetura institucional ainda carece de uma estrutura de coordenação sistêmica e vinculante. A evolução do Programa de Fortalecimento da Capacidade Institucional para Gestão em Regulação (PRO-REG), desde sua concepção original em 2007 até sua reformulação pelo Decreto n° 11.738, de 18 de outubro de 2023, reflete uma opção nacional por modelos de coordenação baseados em *soft law*, capacitação e alinhamento metodológico, os quais, embora relevantes para a difusão de boas práticas como a Análise de Impacto Regulatório (AIR), mostram-se insuficientes para solucionar conflitos de competência complexos. Da mesma forma, a Lei Geral das Agências Reguladoras (Lei nº 13.848, de 25 de junho de 2019), apesar de estabelecer mecanismos importantes de articulação setorial com o Conselho Administrativo de Defesa Econômica (CADE), silencia por completo a respeito da interação com a Agência Nacional de Proteção de Dados (ANPD), perpetuando uma lacuna normativa que precisa ser preenchida por meio de arranjos institucionais voluntários e bilaterais.

Para navegar nesse ecossistema complexo, a ANPD tem adotado uma estratégia pragmática de coordenação, priorizando a celebração de Acordos de Cooperação Técnica (ACTs) voltados a matérias finalísticas — como normatização, fiscalização e harmonização interpretativa —, em detrimento de parcerias puramente voltadas a atividades-meio ou capacitação genérica. Diante das limitações práticas e do ceticismo quanto à eficácia de novas instâncias burocráticas coletivas, como o Fórum Permanente originalmente previsto na LGPD, a autoridade optou por uma solução mais ágil e inteligente, consistente no aproveitamento de comitês e fóruns interministeriais já existentes para a inserção da pauta de proteção de dados. Esse portfólio de coordenação é operacionalizado por uma diversidade de instrumentos que variam em formalidade e propósito, incluindo a edição de diretrizes e orientações conjuntas de caráter preventivo e educativo – como as cartilhas publicadas em parceria com a Secretaria Nacional do Consumidor (SENACON), o Comitê Gestor da Internet no Brasil (CGI.br) e o Tribunal Superior Eleitoral (TSE) –, além de grupos de trabalho temáticos, intercâmbio de pessoal e o desenvolvimento de sandboxes regulatórios como ambientes de inovação e cooperação supervisionada.

O mapeamento empírico realizado pelo GT3 junto a dezesseis órgãos e entidades estratégicos revelou que a institucionalização dessa coordenação ainda se desenvolve de maneira parcial e, por vezes, errática no Brasil. Dos órgãos analisados, apenas cerca de quarenta por cento possuem ACTs formalizados com a ANPD, compreendendo a ANS, o CADE, a CGU, o CGI.br, a SENACON e o TSE. A cooperação com a SENACON representou o marco zero dessa estratégia, motivada pela urgência de mitigar a superposição regulatória com o Sistema Nacional de Defesa

do Consumidor, seguida pelas parcerias estratégicas com o CADE, para articular as esferas antitruste e de privacidade na economia digital, e com a CGU, para harmonizar a aplicação da LGPD com a Lei de Acesso à Informação (LAI). Por outro lado, a ausência de acordos formais com reguladores de setores de altíssima intensidade no tratamento de dados pessoais – como o Banco Central do Brasil (BCB), a Agência Nacional de Telecomunicações (ANATEL) e a Agência Nacional de Vigilância Sanitária (ANVISA) – configura uma lacuna crítica na governança nacional de dados, expondo o ambiente regulatório a riscos severos de fragmentação e insegurança jurídica.

A análise de casos práticos de atuação conjunta confirma que a articulação interinstitucional no Brasil tem oscilado entre ações estruturadas por acordos prévios e respostas reativas a incidentes emergenciais. No âmbito dos casos antecedidos por ACTs, destacam-se a atuação tripartite entre ANPD, SENACON e Ministério Público Federal (MPF) no caso Grok/X em 2026, a elaboração de estudos de concorrência com o CADE e a publicação do Guia Orientativo sobre a aplicação da LGPD no contexto eleitoral de 2022 em conjunto com o TSE. Em contrapartida, os casos não antecedidos por acordos formais evidenciam o caráter improvisado das respostas estatais, como ocorreu na apuração do vazamento de dados de operadoras de telefonia em 2021, na recomendação conjunta emitida ao WhatsApp em 2021 para adiar suas alterações de política de privacidade e nas investigações de incidentes de segurança envolvendo chaves PIX junto ao Banco Central. Esse déficit de coordenação prévia projeta riscos graves, tais como a duplicação de esforços investigativos, a imposição de exigências contraditórias aos regulados, a assimetria de informações entre as autoridades e a vulnerabilidade ao fenômeno da captura processual, em que agentes exploram divergências interpretativas entre os órgãos fiscalizadores.

Diante desse diagnóstico, este relatório propõe um conjunto de dez recomendações estruturadas para transformar a sobreposição de competências em complementaridade funcional e consolidar a ANPD como a autoridade central do ecossistema de proteção de dados, a saber:

(i) Celebração prioritária de ACTs com os nove órgãos ainda sem acordo formalizado, com ênfase imediata no BCB, na ANATEL e na ANVISA, mediante arquitetura modular que permita o aprofundamento gradual das obrigações de cooperação;

(ii) Elaboração conjunta de Guias Setoriais de Boas Práticas que traduzam os princípios da LGPD para as realidades operacionais de cada setor regulado;

(iii) Construção de Protocolo de Definição da Autoridade Líder (lead authority) para ordenar a condução de investigações com competências concorrentes, evitando duplicidade de esforços e decisões contraditórias;

(iv) Adoção de Sistema de Informação Compartilhado que assegure o intercâmbio seguro de dados, evidências e documentos sigilosos entre as autoridades, com garantias de autenticidade e rastreabilidade;

(v) Instituição de Protocolos de Notificação de Incidentes Compartilhados com ponto único de entrada (single entry point), nos moldes da Diretiva NIS-2, para reduzir a carga de conformidade sobre os regulados e uniformizar os fluxos de comunicação entre autoridades;

(vi) Formulação de Protocolos para Fiscalização Conjunta, com constituição de equipes mistas de apuração capazes de concentrar a expertise técnica de cada órgão em investigações de alta complexidade;

(vii) Instituição de Matriz de Dosimetria Coordenada como cláusula obrigatória nos ACTs, assegurando que sanções já aplicadas por outros órgãos sejam consideradas na dosimetria de penalidades subsequentes, de modo a prevenir o bis in idem sancionatório;

(viii) Participação *ex ante* da ANPD nas Análises de Impacto Regulatório (AIRs) setoriais com repercussão sobre dados pessoais, mediante manifestação técnica prévia de caráter recomendativo;

(ix) Implementação de Programa Estruturado de Capacitação Conjunta e Intercâmbio de Servidores (*secondments*), para o desenvolvimento de competências especializadas e o adensamento das relações técnicas entre as equipes das autoridades cooperantes;

(x) Criação do Observatório Interinstitucional de Coordenação Regulatória da ANPD como instância técnica permanente para o monitoramento das interações interinstitucionais, a produção de indicadores de efetividade e a promoção da transparência e da *accountability* regulatória perante a sociedade.

Em conclusão, a efetividade da proteção de dados pessoais no Brasil não depende do isolamento institucional da ANPD ou da supressão das competências setoriais das demais agências, mas sim da construção de pontes sólidas e estáveis de cooperação. Onde a coordenação é deixada ao improviso do caso concreto, imperam a fragmentação e a insegurança jurídica; onde ela é estruturada preventivamente por meio de instrumentos formais e operacionais, viabiliza-se uma atuação estatal coerente, eficiente e verdadeiramente protetiva. A transformação da ANPD em agência reguladora pela Lei nº 15.352, de 25 de fevereiro de 2026 confere à autarquia a estatura necessária para liderar esse processo, cabendo ao Conselho Nacional de Proteção de

Dados Pessoais e da Privacidade (CNPD) e aos demais atores do ecossistema apoiar a implementação das recomendações deste relatório como caminho indispensável para a consolidação da segurança jurídica e da eficiência administrativa no Estado regulador brasileiro.

Referências Bibliográficas

ADMINISTRATIVE CONFERENCE OF THE UNITED STATES. *Recommendation 2012-4*, *Improving Coordination of Related Agency Responsibilities*. Disponível em: https://www.acus.gov/document/improving-coordination-related-agency-responsibilities, Acesso em 05 abr. 2026

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. *ANPD se reúne com o Comitê de Proteção de Dados do Conselho Nacional de Justiça*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-se-reune-com-o-comite-de-protecao-de-dados-do-conselho-nacional-de-justica. Acesso em: 2 jun. 2026.

AGÊNCIA BRASIL. *Banco Central comunica vazamento de dados de 3 mil chaves Pix*, 18 abr 2024. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2024-04/banco-central-comunica-vazamento-de-dados-de-3-mil-chaves-pix. Acesso em 22 mai 2026.

AGÊNCIA BRASIL. *BC comunica vazamento de dados de 238 chaves Pix,* 24 ago 2023. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2023-08/bc-comunica-vazamento-de-dados-de-238-chaves-pix. Acesso em 22 mai 2026.

ANATEL. *Painéis de Dados.* Disponível em www.gov.br/anatel. Acesso em 22 mai 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Planejamento Estratégico 2021-2023*. 2021, p. 6. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-anpd-2021-2023. Acesso em 26 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Planejamento Estratégico 2024-2027*. 2024, p. 13. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-2024-2027. Acesso em 26 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Sandbox Regulatório: Estudo Técnico*. Versão pública. 2023, p. 10. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/sandbox_regulatorio__estudo_tecnico__versao_publica_.pdf. Acesso em 12 jan. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; TRIBUNAL SUPERIOR ELEITORAL. *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. Brasília, jan 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/em-ano-eleitoral-anpd-e-tse-publicam-guia-de-eleicoes. Acesso em 22 mai 2026.

ARAUJO, Valter Shuenquener de; DIONÍSIO, Pedro de Hollanda. *A sobreposição de órgãos de controle e seus desafios à coordenação dos acordos substitutivos no Brasil*. Revista Quaestio Iuris, v. 16, n° 2, 2023, p. 530 e s. DOI: 10.12957/rqi.2023.64595

BENDOR, Jonathan B. *Parallel Systems: Redundancy in Government*. 2. ed. Berkley: University of California Press, 1985, p. 209 e ss.

BRASIL. Superior Tribunal de Justiça (Primeira Turma). REsp. n° 2.107.398/RJ, rel. Min. Gurgel de Faria. Brasília, j. em 18 fev. 2025. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/07032025-Leis-Anticorrupcao-e-LIA-podem-ser-aplicadas-juntas--desde-que-nao-fundamentem-sancoes-identicas.aspx. Acesso em: 2 jun. 2026.

CONTROLADORIA-GERAL DA UNIÃO. *Relatório Diagnóstico sobre a Implementação da Política Nacional de Segurança Pública e Defesa Social*. Brasília: CGU, 2020. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/auditoria-e-fiscalizacao/avaliacao-de-politicas-publicas/arquivos/pnspds.pdf. Acesso em: 2 jun. 2026.

COMPETITION AND MARKETS AUTHORITY; OFFICE OF COMMUNICATIONS. *Online safety and competition in digital markets: a joint statement between the CMA and Ofcom*. London: CMA; Ofcom, 14 jul. 2022. Disponível em: https://www.gov.uk/government/publications/cma-ofcom-joint-statement-on-online-safety-and-competition. Acesso em: 27 maio 2026.

DIGITAL PLATFORM REGULATORS FORUM. *Joint Statement on the ACCC Digital Platform Services Inquiry 2020-2025***.** Disponível em: https://www.accc.gov.au/about-us/news/media-updates/digital-platform-regulators-forum. Acesso em 9 dez. 2025.

DIGITAL REGULATION COOPERATION FORUM. *About the DRCF*. Disponível em: https://www.drcf.org.uk/about-drcf. Acesso em 31 mai 2026

DIGITAL REGULATION COOPERATION FORUM. *About Us*. Disponível em: https://www.drcf.org.uk/about-us. Acesso em 9 dez. 2025.

DIGITAL REGULATION COOPERATION FORUM. DRCF 2025/26 Annual Report. Londres: DRCF, 27 abr. 2026. 23 p. Disponível em: https://www.drcf.org.uk/publications/annual-reports. Acesso em: 1 jun. 2026.

ESPÍRITO SANTO, Paulo André. A cooperação entre a autoridade antitruste e as agências reguladoras nos mercados setoriais: critérios e formas. São Paulo: JusPodivm, 2025, p. 115.

EUROPEAN DATA PROTECTION BOARD. *EDPB Annual Report 2025: Clarity in Action – Supporting Stakeholders through Guidance and Dialogue*. Bruxelas: EDPB, 9 abr. 2026. Disponível

em: https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2025_en. Acesso em: 1 jun. 2026.

EUROPEAN DATA PROTECTION BOARD. *EDPB Conference "Cross-regulatory cooperation in the EU2"*. Disponível em: https://www.edpb.europa.eu/. Acesso em 22 mai 2026.

FEDERAL TRADE COMMISSION. *Consumer Sentinel Network*. Washington, D.C.: FTC, 1997. In: https://www.ftc.gov/enforcement/consumer-sentinel-network. Acesso em: 2 jun 2026.

FREEMAN, J., & ROSSI, J. (2011). *Agency Coordination in Shared Regulatory Space*. Harvard Law Review, 125, 1131-1211. https://doi.org/10.2139/ssrn.1778363. Acesso em 01 jun 2026.

GERSEN, Jacob E. *Overlapping and Underlapping Jurisdiction in Administrative Law*. The Supreme Court Review, v. 2006, p. 201-247, 2006.

HEIDRICH, Joerg. Exchange-Hack: *unerfreuliche Positionen der Datenschutzbehörden zu Meldepflicht*. Heise Online, 11 mar. 2021. Disponível em: https://www.heise.de/news/Exchange-Hack-Unerfreuliche-Positionen-der-Datenschutzbehoerden-zu-Meldepflicht-5076453.html. Acesso em: 31 maio 2026.

NATIONALER NORMENKONTROLLRAT. *Gute Gesetze, digitale Verwaltung und weniger Bürokratie*. Disponível em: https://www.normenkontrollrat.bund.de/Webs/NKR/DE/der-nkr/aufgabe/aufgabe_node.html. Acesso em 9 dez. 2025.

OFFICE OF COMMUNICATIONS; INFORMATION COMMISSIONER'S OFFICE. *Online safety and data protection: a joint statement by Ofcom and the Information Commissioner's Office*. London: Ofcom; ICO, 25 nov. 2022. Disponível em: https://www.gov.uk/government/publications/online-safety-and-data-protection-a-joint-statement-by-ofcom-and-the-information-commissioners-office. Acesso em: 27 maio 2026.

PROCON-SP. *Procon-SP notifica Claro, Oi, Tim, Vivo e Psafe*. São Paulo: Fundação Procon de São Paulo, 17 fev. 2021. Disponível em: https://www.procon.sp.gov.br/procon-sp-notifica-claro-oi-tim-vivo-e-psafe/. Acesso em: 2 jun. 2026.

SCHILLEMANS, Thomas; BOVENS, Mark. *The Challenge of Multiple Accountability: Does Redundancy Lead to Overload?* In: DUBNICK, Melvin J.; FREDERICKSON, H. George (Ed.). *Accountable Governance: Problems and Promises*. Armonk, NY: M. E. Sharpe, 2011, p. 18 e s.

SCHMITZ-BERNDT, Sandra. *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*. Journal of Cybersecurity, v. 9, n° 1, 2023. Disponível em: https://doi.org/10.1093/cybsec/tyad009. Acesso em 31 mai 2026.

SUNSTEIN, Cass R. *The Office of Information and Regulatory Affairs: Myths and Realities*. Harvard Law Review, v. 126, 2013. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2192639. Acesso em 9 dez. 2025.

TRIBUNAL DE CONTAS DA UNIÃO, *Auditorias realizadas no âmbito do SUSP* (TC 037.642/2023-5, Acórdão apreciado na sessão plenária de 27 de novembro de 2024, rel. Min. Benjamin Zymler. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/acao-estrategica-do-plano-nacional-de-seguranca-publica-e-defesa-social-apresenta-falhas. Acesso em: 2 jun. 2026).

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPÉIA. *C-117/20, bpost SA*, ECLI:EU:C:2022:202, j. em 22 mar 2022, par. 48-51, 53 e 58. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62020CJ0117. Acesso em 2 jun. 2026.

TURK, Matthew C. Overlapping Legal Rules in Financial Regulation and the Administrative State. Georgia Law Review, v. 54, n° 3, 2020, p. 791.

UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022*. Diretiva NIS 2. Jornal Oficial da União Europeia, L 333, 27 dez. 2022, p. 80-152. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Acesso em: 31 maio 2026.

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, L 119, 4 maio 2016, p. 1-88. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 31 maio 2026.

WANG, J., ULIBARRI, N., & SCOTT, T. A. (2024). *Agency consultation networks in environmental impact assessment*. Journal of Public Administration Research and Theory. https://doi.org/10.1093/jopart/muae008. Acesso em 01 mai 2026