Proteção de dados pessoais no Brasil em setores regulados

Gabriela Andrade Guimarães de Oliveira

Graduada pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio. Especialista em Proteção de Dados Pessoais pelo Instituto de Tecnologia e Sociedade. Pós-Graduanda em Direito Econômico e Regulatório pela Pontifícia Universidade Católica do Rio de Janeiro.

Resumo: O presente artigo tem como objetivo analisar a regulamentação de proteção de dados pessoais no Brasil em setores regulados, abordando as particularidades relacionadas a cada setor e os desafios que persistem.

Palavras-chave: Proteção de Dados Pessoais. Regulação. Setores econômicos regulados. Economia Digital.

Sumário: **1** Introdução – **2** Contexto: breve histórico da proteção de dados pessoais no Brasil – **3** Onde estamos? – **4** Abrangência do tema em setores regulados – **5** Considerações à relevância das normas setoriais sobre proteção de dados pessoais – **6** Desafios atuais e seus impactos na economia digital – Referências

1 Introdução

A proteção de dados pessoais surgiu como um tema de extrema importância na era digital, em que informações pessoais são coletadas, armazenadas e tratadas em uma escala sem precedentes.

No Brasil, muito embora o tema já fosse tratado anteriormente em diversas normas, de forma esparsa e não exaustiva, o assunto ganhou destaque após a entrada em vigor da Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018 ou "LGPD"), marco legal que visa estabelecer diretrizes para a coleta e tratamento de dados pessoais por pessoas jurídicas de direito público.

Em um cenário no qual dados pessoais são considerados ativos, sua proteção reside na salvaguarda de direito fundamental dos titulares, bem como na proteção à autonomia (seja pela autodeterminação informacional ou para o exercício de seus direitos) e à privacidade.

Além disso, em diversas indústrias, a proteção e regulamentação de dados pessoais têm implicações econômicas e comerciais, proporcionando um ambiente de maior segurança às relações entre pessoas jurídicas de direito privado e de direito público e os titulares de dados pessoais, impulsionando a inovação e o desenvolvimento econômico.

2 Contexto: breve histórico da proteção de dados pessoais no Brasil

A evolução da proteção de dados no Brasil ocorreu de forma gradual em resposta ao avanço tecnológico e às crescentes preocupações com a privacidade e segurança das informações pessoais. Embora a Constituição Federal de 1988 já assegurasse a privacidade como um direito fundamental,[1] as normas relacionadas ao assunto eram tratadas de forma esparsa em diferentes leis e regulamentações setoriais.[2]

Nas décadas de 1990 e 2000, algumas regulamentações setoriais (*e.g.*, no setor bancário e de telecomunicações) estabeleciam regras para o tratamento de informações e dados pessoais. No entanto, a ausência de uma legislação unificada resultava em lacunas e inconsistências, criando um ambiente de pouca segurança jurídica.

Com o avanço da tecnologia e o aumento do uso da Internet, a conscientização sobre a importância da proteção de dados cresceu. A sociedade passou a exigir maior controle sobre suas informações pessoais, especialmente diante do

1 Cf. incisos X e XII do artigo 5º da CF:

"Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(...)

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)".

2 A exemplo da: Lei nº 10.406 de 2002 ("Código Civil"); Lei nº 8.078 de 1990 ("Código de Defesa do Consumidor" ou "CDC"); Lei nº 12.414 de 2011 ("Lei do Cadastro Positivo"); Lei nº 12.527 de 2011 ("Lei de Acesso à Informação") e o Decreto nº 7.724 de 2012; Lei Complementar nº 105 de 2001 ("Lei do Sigilo Bancário"); Lei nº 12.965 de 2014 ("Marco Civil da Internet" ou "MCI") e o Decreto nº 8.771 de 2016, que regulamenta o MCI.

crescente tratamento desses dados e de incidentes de vazamento e uso indevido. Esse contexto levou a discussões sobre a necessidade de uma legislação abrangente no Brasil, alinhada com as iniciativas e avanços internacionais.

Esse contexto levou a discussões sobre a necessidade de uma legislação abrangente no Brasil, alinhada com as iniciativas e avanços internacionais. Em 2018, com a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que regula o tema na União Europeia com efeitos extraterritoriais, o debate global sobre normas gerais para proteção de dados foi reaquecido, inclusive no Brasil.

Compreendendo a importância do tema e em atenção às restrições impostas pela União Europeia aos países que não tivessem um grau de proteção similar ou superior ao estabelecido pelo GDPR, o Brasil, por meio de debate legislativo amplamente influenciado pelas normas internacionais, aprovou e promulgou a Lei Geral de Proteção de Dados Pessoais em 2018 (Lei nº 13.709 de 2018).

Em 2022, a Emenda Constitucional (EC) nº 115/2022 incluiu o direito à proteção de dados pessoais no rol constitucional de direitos e garantias fundamentais do cidadão, fixando a competência privativa da União para legislar sobre o tema, com objetivo de aportar mais segurança jurídica às normas basilares sobre o tema. Desde então, várias iniciativas de adequação, tanto no âmbito público quanto privado, foram propostas, conforme demonstrado no panorama geral e não exaustivo ora apresentado.

3 Onde estamos?

À luz do GDPR, a LGPD estabelece princípios e diretrizes claros para a coleta, tratamento e compartilhamento/transferência de dados pessoais, abrangendo os direitos dos titulares dos dados, as responsabilidades dos Agentes de Tratamento, do Encarregado, os parâmetros para segurança da informação, os requisitos para Transferência Internacional de Dados, e as instruções sobre a atuação da Autoridade Nacional de Proteção de Dados ("ANPD"), entre outras questões.

Desde a entrada em vigor da LGPD, diversas iniciativas setoriais têm sido propostas pelo Poder Público e pela iniciativa privada visando à adequação dos diferentes setores à legislação e, ainda, a proposição de normas específicas para garantir a proteção dos dados pessoais nos setores econômicos.

Em âmbito federal, destaca-se o Guia de Boas Práticas sobre a LGPD, publicado pelo Governo Federal ainda em agosto de 2020.[3] Outrossim, para além dos documentos e publicações da ANPD (*e.g.*, Guias Orientativos, Manuais, Cartilhas, entre outros) e de Análises de Impacto Regulatório (AIRs), Consultas Públicas e Tomadas de Subsídios propostas pela Autoridade, foram editados e publicados, nos últimos anos, Portarias, Enunciados, Resoluções e, ainda, Notas Técnicas[4] visando à regulamentação da proteção de dados pessoais em âmbito nacional.

Devido aos avanços no tema, em 2023, a ANPD divulgou o balanço de acompanhamento e execução da Agenda Regulatória referente aos anos 2021 e 2022,[5] publicou a Agenda Regulatória para o biênio de 2023-2024[6] e aprovou, por meio da Resolução CD/ANPD nº 5 de 2023, a Agenda de Avaliação de Resultado Regulatório para o período 2023-2026. Isso proporcionou ampla transparência, visibilidade e eficiência às ações regulatórias, permitindo a participação e o acompanhamento pela sociedade, e proporcionando maior segurança jurídica na relação com os agentes regulados.

4 Abrangência do tema em setores regulados

Com o objetivo de alinhar as atividades das diversas indústrias aos princípios e obrigações da LGPD e promover uma cultura de respeito à privacidade e segurança da informação, agentes reguladores de diferentes setores econômicos têm editado normas e diretrizes, observadas as competências legais que lhes são atribuídas e, também àquelas da alçada da ANPD. Essas normas visam assegurar a proteção de dados pessoais por meio de procedimentos específicos aplicáveis a cada setor.

---

3 Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

4 A exemplo de: Portaria nº 1 de março de 2021, que estabelece o Regimento Interno da ANPD; Portaria nº 16 de julho de 2021, que aprova o processo de regulamentação no âmbito da ANPD, Resolução CD/ANPD nº 1 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD; Resolução CD/ANPD nº 2 de janeiro de 2022, que aprova o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte; Resolução CD/ANPD nº 4 de fevereiro de 2022, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas; Enunciado CD/ANPD nº 1, maio de 2023, sobre o tratamento de dados pessoais de crianças e adolescentes, entre outros.

5 Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/auditorias-acoes-de-supervisao-e-correicao/balanco-agenda-regulatoria-2021_2022-2_2022_.pdf.

6 Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024/AgendaRegulatria20232024.pdf/view.

Paralelamente, é importante observar que o Poder Público tem incentivado a formação de conselhos consultivos compostos por especialistas do setor, organizações da sociedade civil e representantes do governo. Esses órgãos têm a responsabilidade de elaborar diretrizes setoriais específicas, adaptadas às peculiaridades de cada segmento, promovendo uma compreensão mais clara das obrigações legais e dos melhores métodos de conformidade.

Além disso, tanto na esfera pública quanto na privada, identificam-se, dentre as boas práticas adotadas, (i) a promoção de ações de educação e capacitação, por meio de treinamentos e *workshops* para os agentes de diversos setores, com o objetivo de propiciar a efetiva adequação às normas de proteção de dados pessoais e disseminar uma cultura que observe as boas práticas; (ii) a edição de guias/manuais orientativos aos setores econômicos, entre outras.

5 Considerações à relevância das normas setoriais sobre proteção de dados pessoais

5.1 Setor de telecomunicações

O setor de telecomunicações opera sob um conjunto legal e normativo com o objetivo de assegurar a proteção dos dados pessoais e preservar a privacidade dos usuários de serviços de telecomunicações, enquanto titulares desses dados.

Nesse contexto, destacam-se a Lei Geral de Telecomunicações (Lei nº 9.472 de 1997, também conhecida como "LGT") e o Marco Civil da Internet (Lei nº 12.965 de 2014, ou "MCI"), os quais estabelecem princípios e diretrizes para o tratamento de informações pessoais pelos agentes desse setor.

A LGT desempenha um papel crucial na proteção de dados pessoais no setor de telecomunicações, ao definir: (i) os direitos dos usuários, incluindo o direito à privacidade de seus dados e ao sigilo das comunicações; (ii) os deveres e direitos dos provedores de serviços; e (iii) as diretrizes para o tratamento adequado desses dados pelos agentes.

O Marco Civil da Internet, por sua vez, estabelece princípios e direitos para o uso da Internet no país, incluindo a garantia da privacidade e proteção de dados

pessoais,[7] exceto em casos de solicitação de divulgação por autoridade competente ou por ordem judicial que assim o determine.[8]

Além das normas mencionadas, o setor é regulado por resoluções específicas, como o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações ("RGC"), aprovado pela Resolução nº 765/2023 da Agência Nacional de Telecomunicações ("ANATEL").[9] Este regulamento aborda vários aspectos dos direitos dos consumidores, incluindo a proteção de dados e privacidade, além de estabelecer regras para a coleta, armazenamento e tratamento de dados pessoais, exigindo práticas transparentes e seguras por parte das empresas.

O Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 738/2020 da ANATEL,[10] é outra peça importante no quadro regulatório setorial. Em consonância com a LGPD, ele impõe às empresas de telecomunicações o dever de reter a menor quantidade possível de dados de usuários, mantendo-os sob sigilo em ambiente controlado e seguro,[11] desde que assegurados recursos tecnológicos para a quebra do sigilo.[12]

---

7 "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; (...)."

8 "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. §1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º;

§3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição; §4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais."

9 Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2023/1900-resolucao-765#art85Anexo

10 Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738.

11 Cf. "Art. 65-H. As prestadoras devem zelar pelo sigilo das comunicações e pela confidencialidade dos dados dos usuários de seus serviços, inclusive registros de conexão, nos termos da legislação e regulamentação".

12 *Vide* "Art. 65-K. As prestadoras devem tornar disponíveis os recursos tecnológicos, facilidades e dados necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados".

Outrossim, este Regulamento também aborda de maneira abrangente a guarda de dados pessoais para o cumprimento de obrigações legais e regulatórias,[13] conferindo maior segurança jurídica ao tratamento realizado pelos agentes.

Nos últimos anos, diante da substituição crescente do serviço fixo pelo móvel e dos diferentes regimes conferidos a eles, em decorrência das mudanças comportamentais dos usuários e dos avanços tecnológicos, a relevância dos dados e os impactos do seu tratamento têm aumentado.

Percebe-se, portanto, que as normas regulamentadoras atuam em conjunto na salvaguarda da inovação e dos direitos dos indivíduos, enquanto titulares de dados pessoais, promovendo a transparência, a segurança e a confiança no ambiente digital.

Em consonância com o exposto, em uma auditoria recente realizada pelo Tribunal de Contas da União, conforme Acórdão 1384/2022-TCU-Plenário, que aprovou a auditoria em 382 organizações públicas federais para avaliar a aderência de suas ações às diretrizes estabelecidas pela LGPD, a ANATEL obteve 0,76 no indicador de adequação à norma, indicando estar em um nível "intermediário" de conformidade.[14]

5.2 Setor de saúde suplementar

O setor de saúde suplementar é considerado altamente sensível quando se trata da proteção de dados pessoais, devido ao potencial impacto na privacidade e intimidade dos indivíduos/titulares de dados. Isso se deve, em grande parte, ao volume de informações e dados sensíveis, como informações médicas, históricos de tratamentos, exames clínicos e condições de saúde, que são coletados, tratados e retidos por instituições de saúde, como clínicas, hospitais e empresas farmacêuticas e seus respectivos profissionais.

Outrossim, o tratamento de dados pessoais no setor de saúde está intrinsecamente relacionado ao benefício conferido pelos serviços e produtos ofertados. É dizer, no contexto da oferta de serviços e produtos na área de saúde, a coleta e

[13] Cf. "Art. 65-I. As prestadoras devem reter a menor quantidade possível de dados de usuários, mantendo-os sob sigilo, em ambiente controlado e de segurança, excluindo-os: I - tão logo atingida a finalidade de seu tratamento; ou, II - quando encerrado o prazo de guarda determinado por obrigação legal ou regulatória".

[14] Relatório TCU de Feedback – ANATEL, disponível em: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/c814b44fe4acc37bbc389abe4c01cc3c.

o tratamento adequados desses dados são medidas cruciais para personalização de tratamentos, prevenção e combate a doenças, e eficácia dos cuidados médicos. Além disso, o tratamento destes dados vem sendo essencial ao processo de desenvolvimento de novos medicamentos e terapias.

A LGPD estabelece importantes diretrizes para a coleta, uso e tratamento de dados pessoais sensíveis, incluindo dados genéticos e relacionados à saúde e vida sexual. Neste sentido, a norma reconhece a relevância dessas informações e a necessidade de protegê-las de maneira rigorosa, dado que os dados pessoais sensíveis, se mal utilizados ou expostos, podem causar danos significativos à privacidade e à dignidade dos titulares.

Ainda sobre o tema, o Conselho Federal de Medicina (CFM) publicou a Resolução nº 2.314/2022,[15] que define e regulamenta a telemedicina para assistência, educação, pesquisa, prevenção de doenças, gestão e promoção de saúde. A norma estabelece que a prestação de serviços de telemedicina deve seguir os padrões normativos e éticos do atendimento presencial[16] e a obrigação de se obter o consentimento explícito do paciente ou de seu representante sobre a possibilidade de seus dados pessoais serem compartilhados, bem como sobre seu direito de revogar o consentimento, salvo em caso de emergência médica.[17]

Outrossim, nos serviços prestados por telemedicina, os dados e imagens dos pacientes constantes no registro do prontuário devem ser preservados, obedecendo as normas legais e aquelas editadas pelo CFM pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade, à irrefutabilidade e à garantia do sigilo profissional das informações.[18]

Além da LGPD, cumpre destacar a Resolução nº 2.227/18 do CFM, que trata do sigilo das informações médicas e reforça a necessidade de consentimento informado e a segurança no tratamento desses dados. Outro aspecto relevante é a interoperabilidade dos sistemas de saúde, que permite a troca de informações entre diferentes entidades de saúde, mas exige um cuidado especial com a proteção dos dados durante esse processo.

Diante da sensibilidade do tema, percebe-se a necessidade de uma abordagem cuidadosa e ética nos processos de coleta, armazenamento e compartilhamento de informações médicas a fim de preservar a dignidade e os direitos dos

[15] Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852.
[16] Cf. art. 16 da Resolução nº 2.314/2022.
[17] Cf. parágrafo único do art. 15 da Resolução nº 2.314/2022.
[18] Cf. art. 3º da Resolução nº 2.314/2022.

indivíduos, ao mesmo tempo em que permite avanços significativos na prestação de serviços de saúde.

Nesse contexto, a iniciativa privada tem coordenado ações de autorregulação, a exemplo do Código de Boas Práticas – CNSAúde (Confederação Nacional de Saúde), que fornece orientações para agentes de saúde. O código aborda aspectos como transparência na coleta de dados, obtenção de consentimento adequado dos titulares de dados pessoais, adoção de medidas de segurança para prevenir incidentes de segurança (*e.g.*, vazamentos e ataques cibernéticos), além de diretrizes voltadas ao compartilhamento seguro de dados pessoais sensíveis e informações médicas entre profissionais de saúde.

Na mesma toada, a Cartilha elaborada pelo Instituto Brasileiro de Defesa do Consumidor (IDEC)[19] traz um panorama geral sobre a proteção de dados pessoais no contexto do setor de saúde, ao abordar temas como o direito à saúde, a transformação digital, o uso de dados pessoais no acesso a medicamentos e serviços de saúde e desafios apresentados pela Inteligência Artificial. Ainda de acordo com o Instituto, as políticas de uso de dados em saúde encontram-se em fase de construção no Brasil e no mundo, mas já existem preocupações quanto ao uso equilibrado e consciente de dados pessoais no setor da saúde.[20]

Por sua vez, a Agência Nacional de Saúde Suplementar (ANS) vem desempenhando um papel crucial na regulamentação e supervisão das atividades dos agentes regulados.

Dentre as suas iniciativas, destaca-se a Cartilha de Proteção de Dados Pessoais,[21] que orienta agentes de saúde, profissionais do setor e pacientes sobre as melhores práticas para proteção de dados pessoais e dados pessoais sensíveis. A Cartilha aborda temas como transparência na coleta e no tratamento dos dados, os direitos dos titulares, a importância da segurança da informação e da adoção de medidas técnicas e organizacionais adequadas para evitar o acesso não autorizado, vazamentos e outros incidentes de segurança, dentre outros.

[19] Disponível em: https://idec.org.br/sites/default/files/direito-a-saude-protecao-dados-pessoais-pt.pdf.

[20] Cf. consta da fl. 70 do documento "Direito à Saúde e Proteção de Dados Pessoais: desafios e potencialidades contemporâneas", disponível em: https://idec.org.br/sites/default/files/direito-a-saude-protecao-dados-pessoais-pt.pdf.

[21] Disponível em: https://www.gov.br/ans/pt-br/arquivos/acesso-a-informacao/tratamento-de-dados-pessoais/cartilha_lgpd_r2_semgov.pdf.

Por fim, desde 2022, a atuação da Agência vem sendo orientada, dentre outras, pela Resolução nº 80, de 28 de junho de 2022,[22] que dispõe sobre a Política de Proteção de Dados Pessoais no âmbito da Agência.

5.3 Setor de transportes aquaviários

A coleta e análise de dados pessoais, incluindo informações de passageiros e tripulantes, possibilitam às autoridades marítimas e às empresas de transporte monitorar e assegurar a conformidade com regulamentações de segurança, como verificações de antecedentes e controle de acesso a áreas sensíveis em embarcações. Essa prática é fundamental para prevenir ameaças à segurança, como pirataria e atividades ilícitas.

Além disso, a utilização de dados pessoais desempenha um papel essencial na melhoria da experiência dos passageiros, enquanto titulares desses dados, ao possibilitar que as empresas de transporte aquaviário se valham de informações sobre preferências, histórico de viagens e *feedback* dos passageiros para personalizar serviços, como cardápios, entretenimento a bordo e acomodações, ajustar, de forma mais eficaz, horários e rotas em atenção às demandas, atraindo mais clientes e aumentando sua competitividade no mercado.

No âmbito da Agência Nacional de Transportes Aquaviários (ANTAQ), foi aprovada a Política de Proteção de Dados Pessoais (PPDP) por meio da Portaria DG ANTAQ nº 425/2022.[23] A PPDP aplica-se a todos que, de forma direta ou indireta, realizem atividades que envolvam o tratamento de dados pessoais custodiados pela Agência, estabelece diretrizes claras e abrangentes para a gestão e proteção de dados pessoais no contexto das atividades da ANTAQ, ao abordar aspectos como coleta, armazenamento, tratamento e compartilhamento de dados pessoais em conformidade com as disposições da LGPD.

Além disso, a ANTAQ vem buscando alinhar-se às normas e diretrizes setoriais, conforme evidenciado pelo Relatório de Feedback do TCU.[24] Isso porque, ao

[22] Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2022/res0080_30_06_2022.html#:~:text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20de,Ag%C3%AAncia%20Nacional%20de%20Sa%C3%BAde%20Suplementar.

[23] Disponível em: https://sophia.antaq.gov.br/Terminal/acervo/detalhe/31347?guid=1657065600600&returnUrl=%2FTerminal%2Fresultado%2Flistar%3Fguid%3D1657065600600%26quantidadePaginas%3D1%26codigoRegistro%3D31347%2331347&i=7.

[24] Disponível em: https://www.gov.br/antaq/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais-1/RelatorioFeedbackANTAQ.pdf.

analisar o esforço da Agência em adaptar suas práticas operacionais e estratégicas para garantir a segurança e a privacidade dos dados pessoais tratados, o Tribunal conferiu 0,60 no indicador de adequação à LGPD, valor este correspondente ao nível intermediário de adequação às normas de proteção de dados pessoais.

5.4 Setor de aviação civil

O tratamento de dados pessoais desempenha um papel fundamental no avanço e na modernização do setor de aviação civil. A coleta e análise de informações pessoais de passageiros, tripulantes e outros intervenientes são cruciais para atender às normativas vigentes e garantir elevados padrões de segurança, eficiência e comodidade nas operações aéreas. Por conseguinte, tanto as empresas aéreas quanto as autoridades de aviação utilizam dados pessoais para realizar verificações de histórico, identificar passageiros e tripulantes, e garantir a conformidade com regulamentos de segurança e imigração.

Ademais, a coleta e tratamento de dados pessoais possibilita às companhias aéreas e autoridades de aviação compreenderem melhor as necessidades dos passageiros com deficiência, permitindo a adaptação de serviços e instalações para atender a demandas específicas, em conformidade com as normas de acessibilidade.

Além disso, o uso de dados pessoais é fundamental para melhorar a experiência do passageiro, na medida em que possibilita que as companhias aéreas os utilizem para personalizar serviços, desenvolver ofertas especiais com base nas preferências dos passageiros e melhorar a eficiência das operações, como o embarque e desembarque, preferências de assentos e refeições especiais. Isso contribui para uma experiência mais agradável e conveniente para os viajantes e auxilia as companhias aéreas a otimizarem suas operações e alocar recursos de forma mais eficaz.

Contudo, a relevância do uso de dados pessoais no setor de aviação civil suscita debates relevantes sobre privacidade e proteção de dados, especialmente se considerado o volume elevado e o fluxo constante de informações e dados pessoais e sensíveis.

No âmbito da Agência Nacional de Aviação Civil ("ANAC"), em 2015, foi publicado o Manual de Tratamento de Informações com Restrição de Acesso,[25] que aborda em seu item 3.2 as informações consideradas pessoais e/ou sensíveis, bem como o respeito à intimidade e à vida privada dos titulares de dados. Após a entrada em vigor da LGPD, a ANAC aprovou, por meio da Instrução Normativa nº 172, de agosto de 2021,[26] a Política de Proteção de Dados Pessoais da ANAC, garantindo a conformidade do tratamento com a legislação de proteção de dados.[27] Igualmente, foram publicados o Aviso de Privacidade da ANAC[28] e a Portaria nº 2.235, de agosto de 2020,[29] que define o Encarregado pelo Tratamento de Dados Pessoais, um agente essencial à garantia da conformidade com a legislação de proteção de dados.

Recentemente, em auditoria realizada pelo Tribunal de Contas da União[30] para avaliar os controles implementados pelas organizações públicas federais em adequação à LGPD revelou que a ANAC obteve o valor de 0,48 no indicador de adequação, o que corresponde ao nível "inicial".[31]

Sob a perspectiva de boas práticas, é relevante observar que a ANAC conta com uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), estabelecida pela Portaria nº 9.367/STI,[32] a quem compete a atribuição de receber, analisar e responder as notificações relacionadas a incidentes de segurança em redes de computadores, bem como agir preventivamente para minimizar o risco e o impacto de possíveis incidentes de segurança da informação.

25 Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/boletim-de-pessoal/2016/14/anexoiv.pdf.

26 Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/instrucoes-normativas/2021/instrucao-normativa-no-172-02-08-2021.

27 "Art. 3º São objetivos da PoPD: I – estabelecer as regras gerais aplicáveis à ANAC; II – dotar a ANAC de instrumentos normativos e organizacionais que a capacitem administrativamente a assegurar a proteção de dados pessoais; e III – estabelecer diretrizes para a elaboração de normas complementares e procedimentos internos necessários à implementação da proteção de dados pessoais."

28 Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/aviso-de-privacidade-agencia-nacional-de-aviacao-civil-anac.

29 Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/PA20202235.PDF.

30 Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/RelatriodeFeedbackTCU.pdf.

31 Cf. fls. 4 do Relatório, disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/RelatriodeFeedbackTCU.pdf.

32 Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/boletim-de-pessoal/2022/bps-v-17-no-40-03-a-07-10-2022/portaria-9367/visualizar_ato_normativo.

5.5 Setor de transportes terrestres

Notadamente, no âmbito do setor de transportes terrestres, o tratamento de dados pessoais, conduzido tanto pelo Poder Público, incluindo a ANTT, quanto pelos agentes regulados, tem como objetivo primordial garantir aos usuários uma infraestrutura adequada e apropriada prestação de serviços de transporte terrestre, com transparência e regulação efetiva, promovendo a melhoria contínua dos serviços oferecidos. Para alcançar esse propósito, são tratados dados pessoais relacionados: (i) aos passageiros de transporte rodoviário e, quando aplicável, ferroviário; (ii) aos transportadores pessoas físicas, a exemplo dos constantes no Cadastro Nacional dos Transportadores Rodoviários de Mercadorias; e (iii) prestadores de serviços ou fornecedores.

Diante desse contexto, a CNT/SESTSENAT/ITL, em colaboração com representantes dos diversos modais, publicou o "Guia de Boas Práticas de Proteção de Dados no Setor de Transporte",[33] que tem por objetivo estabelecer padrões e protocolos para o tratamento de dados pessoais, facilitando e otimizando a conformidade e a aplicação da normativa de proteção de dados e outras regulamentações relacionadas ao tema pelas empresas do setor.

No âmbito da ANTT, embora as iniciativas relacionadas ao tema sejam incipientes, a Deliberação nº 448 de 2020[34] instituiu a Comissão de Apoio à Proteção de Dados Pessoais pelo Conselho Diretor. A Comissão tem por finalidade formular diretrizes relacionadas à LGPD e oferecer suporte na elaboração de procedimentos e protocolos internos para ações relacionadas ao tratamento de dados pessoais e proteção à privacidade.[35]

Cumpre ainda observar que, conforme o Aviso de Privacidade da Agência,[36] a autarquia está em processo de adequação aos normativos legais sobre proteção de dados, o que inclui a publicação de manuais e guias, bem como a formação de comitês dedicados ao tema.

---

33 Disponível em: https://publicador.sestsenat.org.br/arquivos/b37861f6-e632-45d7-89ca-e8cdbca3d267.pdf.

34 Disponível em: https://tinyurl.com/3uj4hkzp.

35 "Art. 1º Instituir a Comissão de Apoio à Proteção de Dados Pessoais destinada a:

I – formular diretrizes, propor ações e monitorar medidas destinadas à adequação da ANTT à Lei Geral de Proteção de Dados Pessoais – LGPD e à implementação de boas práticas relacionadas à proteção de dados pessoais; e

II – dar o suporte à realização das atividades do encarregado pelo tratamento de dados pessoais decorrentes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) e demais atribuições definidas pela LGPD."

36 Disponível em: https://www.gov.br/antt/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-1/aviso-de-privacidade.

5.6 Setor financeiro e de meios de pagamento

Antes mesmo da vigência da Lei Geral de Proteção de Dados (LGPD), normativas específicas já se preocupavam com o sigilo e a confidencialidade no tratamento e armazenamento de dados pessoais por parte das instituições financeiras e outras entidades autorizadas pelo Banco Central. Um exemplo notável é a Lei Complementar nº 105/2001, conhecida como "Lei do Sigilo Bancário",[37] que assegura a confidencialidade dos dados financeiros, exceto por ordem judicial para fins de investigação de atos ilegais.[38]

O referido normativo cumpre relevante papel, visto que tem como objetivo preservar a privacidade relacionada às atividades bancárias, bem como contempla regras que objetivam evitar práticas ilícitas. Outro exemplo é a Lei nº 4.658/2018,[39] que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de tratamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Em um setor caracterizado por operações complexas envolvendo procedimentos, pessoas, programas, equipamentos, normas internas e normas legais, a arquitetura desse sistema deve considerar diversos aspectos da proteção de dados pessoais e privacidade, incluindo controle de acesso, rastreabilidade, conhecimento das finalidades declaradas e executadas, anonimização de dados, entre outros.

Por conseguinte, a proteção de dados pessoais tornou-se um elemento intrínseco ao desempenho adequado no setor, pois o tratamento adequado desses dados, a segurança e a gestão da informação desempenham papel crucial nas operações financeiras. Com a digitalização dos serviços nesse setor, a implementação de uma cultura voltada à proteção de dados pessoais tornou-se uma medida cada vez mais urgente para todos os agentes envolvidos.

---

37 Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

38 Conforme Art. 1, §4º, c/c Art. 3º da Lei do Sigilo Bancário: "Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.(...) §4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes: (...)"; e "Art. 3º Serão prestadas pelo Banco Central do Brasil, pela Comissão de Valores Mobiliários e pelas instituições financeiras as informações ordenadas pelo Poder Judiciário, preservado o seu caráter sigiloso mediante acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide".

39 Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf.

Com a entrada em vigor da LGPD, novas diretrizes e obrigações foram introduzidas, visando à proteção ao crédito por meio de uma abordagem regulatória com traços de inovação.[40]

Embora o dado financeiro ou bancário não integre o rol taxativo dos dados pessoais sensíveis previstos na LGPD,[41] tal como se verifica no GDPR,[42] os riscos resultantes de eventual incidente de segurança que os atinja vêm sendo reconhecidos no âmbito sancionatório e, por conseguinte, inaugurando novas preocupações quanto a sua proteção, na medida em que a correlação entre sigilo de dados financeiros com a proteção à intimidade e à privacidade tem o condão de justificar a adoção de cuidados técnicos robustos.

Nos últimos anos, o setor tem experimentado uma evolução tecnológica e mercadológica significativa, em grande parte proporcionada por uma regulamentação pró-competitiva.

A título exemplificativo, cita-se a regulamentação do Open Finance, que busca facilitar o compartilhamento de dados e serviços por meio de um sistema aberto e interoperável mediante o empoderamento do titular dos dados. Trata-se de um ótimo exemplo das inovações que vêm sendo introduzidas neste segmento. O tema foi objeto de ampla discussão social e posteriormente regulamentado por meio da Resolução Conjunta nº 01/2020,[43] cujo texto já foi alterado por outras medidas.[44] Nessa linha, a Resolução Conjunta nº 05/2022,[45] que introduziu importantes alterações na regulamentação em questão, definiu a interoperabilidade como sendo "o compartilhamento padronizado de dados, mediante consentimento de cliente, de forma segura, ágil e precisa, entre os participantes dos sistemas disciplinados (...)", com o fito de (i) estimular a inovação; (ii) promover a

40 *Vide* artigos 7º e 20 da LGPD, que assim dispõem: "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente" c/c "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

41 Cf. inciso II do artigo 5º da LGPD, que assim prevê: "Art. 5º Para os fins desta Lei, considera-se: (...) II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

42 Conforme artigo 9º do GDPR, disponível em: https://gdpr-info.eu/art-9-gdpr/.

43 Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51028/Res_Conj_0001_v4_P.pdf.

44 Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=5.

45 Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=5.

concorrência; (iii) aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiros; e (iv) promover a cidadania financeira.[46]

No entanto, a segurança dos dados tem sido uma preocupação na implementação do Open Finance, ao exigir a adoção de medidas efetivas de proteção dos dados pessoais dos titulares, especialmente considerando o aumento potencial no volume de compartilhamentos devido à interoperabilidade dos sistemas – em que a confiança do usuário na segurança das informações é fundamental para o sucesso da iniciativa.

Cabe mencionar a Resolução Conjunta nº 6 de 23 de maio de 2023,[47] que estabelece requisitos para o compartilhamento de dados e informações sobre indícios de fraudes, a serem observados por instituições financeiras, instituições de pagamento e outras instituições autorizadas pelo Banco Central. Destaca-se, nesse sentido, a obrigação de obtenção de consentimento prévio dos titulares para o registro de dados e informações em seus sistemas, ressalvados dados sigilosos nos termos de legislação especial, relacionados a indícios da prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores e de financiamento do terrorismo.

Em tempo, após a entrada em vigor da LGPD, nota-se que o BACEN publicou sua Política de Privacidade[48] e aprovou, por meio da Resolução BCB nº 249 de 2022,[49] sua Política de Governança da Informação, aplicável ao tratamento de qualquer informação em meio digital, físico ou oriunda de comunicações que sejam recebidas, coletadas e tratadas pelo Banco Central, e que visa a proteção das informações tratadas no Banco Central, garantir a disponibilidade e a qualidade adequada das informações básicas para o cumprimento das missões institucionais, garantir a devida prestação de informações à sociedade, em especial as de interesse público, o compartilhamento de informações com outros órgãos públicos, entre outros objetivos.

46 *Vide* art. 3º da Resolução Conjunta nº 01/2020, que assim prevê: "Art. 3º Constituem objetivos do Open Finance: (...); IV – promover a cidadania financeira".

47 Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=6.

48 Disponível em: https://www.bcb.gov.br/acessoinformacao/politicaprivacidade.

49 Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249.

6 Desafios atuais e seus impactos na economia digital

A edição de normas específicas de proteção de dados para cada setor econômico, embora seja em parte necessária devido às particularidades de cada área, vem resultando em um mosaico de regras e diretrizes com desafios significativos de harmonização e interpretação sistemática, com notórios impactos à economia digital.

Isso porque os desafios de harmonização e coordenação entre os diferentes setores residem, principalmente nas especificidades regulatórias de cada setor, visto que cada um possui características únicas (*e.g.*, diversidade de interesses, tecnologias e práticas) em relação à importância e ao volume de dados pessoais que são, dentre de suas dinâmicas particulares, coletados e tratados.

Além disso, em uma sociedade que experimenta uma economia digital, na qual a evolução tecnológica ocorre de maneira rápida e os dados, sobretudo em mercados digitais, podem revelar como os indivíduos pensam, decidem e consomem, configurando verdadeiros ativos, desponta a necessidade de um acompanhamento periódico dos agentes reguladores, responsáveis por instituir novas tecnologias e rever as normas vigentes, o que acrescenta um nível adicional à complexidade de harmonização de normas sobre proteção de dados pessoais.

Soma-se a isso a existência de iniciativas legislativas que visam aprimorar, direta ou indiretamente, a proteção de dados pessoais, bem como regular o uso de inteligência artificial no país, evidenciando a importância de uma atuação colaborativa e conjunta entre o poder legislativo, os órgãos reguladores e os agentes regulados.

Apesar dos desafios mencionados, é crucial que os reguladores busquem um equilíbrio entre a especificidade necessária para cada setor e a necessidade de consistência e clareza nas regras de proteção de dados, visando o desenvolvimento econômico do país. Para empresas que atuam em múltiplos setores, a conformidade com um mosaico de regulamentações complexas pode se tornar uma tarefa desafiadora e onerosa, dificultando a implementação de práticas de forma coesa e eficiente.

Por outro lado, a convergência entre essas normas traz diversos benefícios. Em primeiro lugar, ela não apenas reduz a carga administrativa e minimiza contradições e lacunas normativas, mas também permite que os agentes regulados atuem em maior conformidade com o arcabouço legal e normativo de proteção de dados pessoais. Com isso, os agentes econômicos são capazes de desenvolver sistemas e processos internos que se alinham de maneira mais direta com as

regulamentações, garantindo uma abordagem mais sólida e abrangente para lidar com dados pessoais e minimizando impactos operacionais.

Em segundo lugar, a segurança jurídica oriunda da harmonização entre normas setoriais tende a acarretar maior confiança entre os agentes que integram as cadeias de serviços. Isso porque ao perceberem que suas informações e dados pessoais estão sendo tratados de maneira adequada, independentemente do setor de atividade, estes ficam mais propensos a compartilhar seus dados pessoais, o que é particularmente relevante em um ambiente econômico orientado.

Ademais, ao respeitar as regulamentações de proteção de dados em todos os setores em que operam, os agentes regulados demonstram seu compromisso com a privacidade e a integridade dos dados pessoais, fortalecendo a confiança entre estes e terceiros e promovendo uma cultura de respeito à privacidade capaz de conferir vantagens competitivas.

Em terceiro lugar, a afinidade entre as normas setoriais também promove maior clareza e transparência no tratamento de dados pessoais, possibilitando que os agentes regulados partilhem práticas de tratamento e compartilhamento destes dados, propiciando políticas de privacidade coordenadas e mais aderentes, capazes de mitigar preocupações com a segurança da informação.

É dizer, a eficácia das normas de proteção de dados pessoais também é amplificada quando os atores conseguem identificar padrões comuns de risco e adotar medidas preventivas abrangentes.

Em quarto lugar, a harmonização das normas setoriais é benéfica para a cooperação interdisciplinar. Frequentemente, para o desenvolvimento e a implementação de modelos de negócio, agentes econômicos de distintos setores precisam compartilhar dados pessoais. Nesse cenário, o emprego de normas que possibilitem uma interpretação sistemática facilitaria o adequado tratamento e compartilhamento destes dados, garantindo que estes agentes colaborem entre si de maneira eficaz enquanto protegem os dados pessoais envolvidos.

Finalmente, diante de uma maior coesão entre as normas regulamentadoras, o poder público, assim como a iniciativa privada, encontra maior facilidade em desenvolver abordagens de segurança mais robustas e holísticas, mitigando vulnerabilidades potenciais em todos os âmbitos.

Em suma, nada obstante o avanço normativo no tema, a atuação coordenada entre os órgãos reguladores, o Poder Legislativo e a iniciativa privada, por exemplo, por meio de mecanismos colaborativos de participação social (*e.g.*, audiências públicas, AIR, consulta públicas, entre outros), é medida essencial para assegurar

o desenvolvimento da economia digital, ao minimizar lacunas e divergências interpretativas, garantir uma maior conformação legal e normativa, reduzir assimetrias e promover uma abordagem mais coesa ao tema de proteção de dados pessoais no país.

Abstract: This article is intended to analyze the regulation of personal data protection in Brazil in regulated sectors, addressing the particularities related to each sector and the challenges that remain.

Keywords: Personal Data Protection. Regulation. Regulated economic sectors. Digital Economy.

Referências

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

BRASIL. *Decreto nº 7.724, de 16 de maio de 2011*. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm.

BRASIL. *Lei Complementar nº 105, de 10 de janeiro de 2001*. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. *Portaria nº 1, de 8 de março de 2021*. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados – ANPD. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618.

BRASIL. *Portaria nº 16, de 8 de julho de 2021*. Aprova o processo de regulamentação no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em: https://in.gov.br/en/web/dou/-/portaria-n-16-de-8-de-julho-de-2021-330970241.

BRASIL. *Resolução CD/ANPD nº 1, de 28 de outubro de 2021*. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021#:~:text=RESOLU%C3%87%C3%83O%20CD%2FANPD%20N%C2%BA%201,Nacional%20de%20Prote%C3%A7%C3%A3o%20de%20Dados.

BRASIL. *Resolução CD/ANPD nº 2, de 27 de janeiro de 2022*. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper.

BRASIL. *Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023*. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

BRASIL. *Enunciado CD/ANPD nº 1, de 22 de maio de 2023*. Disponível em: https://www.in.gov.br/en/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934.

BRASIL. *Resolução nº 738, de 21 de dezembro de 2020*. Altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública, e dá outras providências. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738.

BRASIL. *Resolução CFM nº 2.314, de 20 de abril de 2022*. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852.

BRASIL. Tribunal de Contas da União. *Acórdão 1.384/2022*. Plenário. Relator: Ministro Augusto Nardes. Disponível em: https://sistemas.anatel.gov.br/anexar api/publico/anexos/download/c814b44fe4acc37bbc389abe4c01cc3c.

BRASIL. *PORTARIA-DG ANTAQ Nº 425/2022*. Aprovar a Política de Proteção Dados Pessoais PPDP no âmbito da Agência Nacional de Transportes Aquaviários. Disponível em: https://sophia.antaq.gov.br/Terminal/acervo/detalhe/31347?guid=1657065600600&returnUrl=%2FTerminal%2Fresultado%2Flistar%3Fguid%3D1657065600600%26quantidadePaginas%3D1%26codigoRegistro%3D31347%2331347&i=7.

BRASIL. *Decreto nº 8.771, de 11 de maio de 2016*. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm.

BRASIL. *Guia de Boas Práticas da Lei Geral de Proteção de Dados* (LGPD). Governo Federal. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

BRASIL. *Nota Técnica nº 2/2023/CGN/ANPD*. Autoridade Nacional de Proteção de Dados. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/auditorias-acoes-de-supervisao-e-correicao/balanco-agenda-regulatoria-2021_2022-2_2022_.pdf.

BRASIL. *Resolução ANATEL nº 765, de 06 de novembro de 2023*. Aprova o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqY_JQkkacYY1Io0H4P4T-fNweaeY3IbkkfrOpDNox9cDYKMgKFw-zrmvKIdumZ4bQyG-_FIsaDHp8N82IcP5sIz.

BRASIL. *Portaria ANPD Nº 35, de 4 de novembro de 2022*. Torna Pública a Agenda Regulatória para o biênio 2023-2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024/AgendaRegulatria20232024.pdf/view.

BRASIL. *Resolução CFM Nº 2.314, de 20 de abril de 2022*. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cfm-n-2.314-de-20-de-abril-de-2022-397602852.

BRASIL. *Direito à Saúde e Proteção de Dados Pessoais*: desafios e potencialidades contemporâneas. Instituto Brasileiro de Defesa do Consumidor. Disponível em: https://idec.org.br/sites/default/files/direito-a-saude-protecao-dados-pessoais-pt.pdf.

BRASIL. *Informações básicas para entender a Lei Geral de Proteção de Dados Pessoais*. Agência Nacional de Saúde Suplementar. Disponível em: https://www.gov.br/ans/pt-br/arquivos/acesso-a-informacao/tratamento-de-dados-pessoais/cartilha_lgpd_r2_semgov.pdf.

BRASIL. *Resolução ANS nº 80, de 28 de junho de 2022*. Dispõe sobre a Política de Proteção de Dados Pessoais no âmbito da Agência Nacional de Saúde Suplementar. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2022/res0080_30_06_2022.html#:~:text=Disp%C3%B5e%20sobre%20a%20Pol%C3%ADtica%20de,Ag%C3%AAncia%20Nacional%20de%20Sa%C3%BAde%20Suplementar.

BRASIL. *Manual de Tratamento de Informações com Restrição de Acesso*. Agência Nacional de Aviação Civil. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/boletim-de-pessoal/2016/14/anexoiv.pdf.

BRASIL. Instrução Normativa nº 172, de 2 de agosto de 2021. Aprova a Política de Proteção de Dados Pessoais – PoPD no âmbito da Agência Nacional de Aviação Civil – ANAC. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/instrucoes-normativas/2021/instrucao-normativa-no-172-02-08-2021.

BRASIL. *Portaria nº 9.367/STI, de 30 de setembro de 2022*. Institui o Documento de Constituição da ETIR ANAC. Disponível em: https://www.anac.gov.br/assuntos/legislacao/legislacao-1/boletim-de-pessoal/2022/bps-v-17-no-40-03-a-07-10-2022/portaria-9367/visualizar_ato_normativo.

BRASIL. *Guia de Boas Práticas de Proteção de Dados no Setor de Transporte*. CNT – SEST SENAT – ITL. Disponível em: https://publicador.sestsenat.org.br/arquivos/b37861f6-e632-45d7-89ca-e8cdbca3d267.pdf.

BRASIL. *Deliberação nº 448/2020*. Institui a Comissão de Apoio à Proteção de Dados Pessoais. Disponível em: https://tinyurl.com/3uj4hkzp.

BRASIL. *Portaria nº 2.235, de 31 de agosto de 2020*. Designa o titular da Gerência Técnica de Gestão da Informação - GTGI/GSIN/SAF como Encarregado pelo Tratamento de Dados Pessoais no âmbito da Agência Nacional de Aviação Civil e dá outras providências. Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/PA20202235.PDF.

BRASIL. *Lei Complementar nº 105, de 10 de janeiro de 2001*. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

BRASIL. *Resolução nº 4.658, de 26 de abril de 2018*. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf.

BRASIL. *Resolução Conjunta nº 5 de 20 de maio de 2022*. Dispõe sobre a interoperabilidade no Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=5.

BRASIL. *Resolução Conjunta nº 6, de 23 de maio de 2023*. Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=6.

BRASIL. *Resolução BCB nº 249, de 5 de outubro de 2022*. Divulga a Política de Governança da Informação do Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249.

BRASIL. *Relatório de Feedback TCU*. Acórdão 1.384/2022 - ANATEL. Auditoria para Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. Disponível em: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/c814b44fe4acc37bbc389abe4c01cc3c.

BRASIL. *Relatório de Feedback TCU*. Acórdão 1.384/2022 - ANTAQ. Auditoria para Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. Disponível em: https://www.gov.br/antaq/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais-1/RelatorioFeedbackANTAQ.pdf.

BRASIL. *Relatório de Feedback TCU*. Acórdão 1.384/2022 - ANAC. Auditoria para Auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. Disponível em: https://www.gov.br/anac/pt-br/acesso-a-informacao/seguranca-da-informacao/tratamento-de-dados-pessoais/RelatriodeFeedbackTCU.pdf.

BRASIL. *Aviso de Privacidade da ANTT*. Agência Nacional de Transportes Terrestres Disponível em: https://www.gov.br/antt/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-1/aviso-de-privacidade.

BRASIL. *Política de Privacidade e Termos de Uso do site, dos aplicativos e dos serviços digitais do Banco Central*. Banco Central do Brasil. Disponível em: https://www.bcb.gov.br/acessoinformacao/politicaprivacidade.

UNIÃO EUROPEIA. *General Data Protection Regulation*. Regulamento Europeu de Proteção de Dados aplicável a todos os Estados-Membros da União Europeia, 2018. Disponível em: https://dsgvo-gesetz.de/art-9-dsgvo/.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

OLIVEIRA, Gabriela Andrade Guimarães de. Proteção de dados pessoais no Brasil em setores regulados. *Revista Fórum de Direito na Economia Digital – RFDED*, Belo Horizonte, ano 7, n. 10, p. 89-111, jan./dez. 2023.