Cadernos Jurídicos
FADI

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709, DE 2018) NA PROTEÇÃO E REGULAMENTAÇÃO DO COMPARTILHAMENTO DE DADOS SENSÍVEIS ENTRE ENTES DA ADMINISTRAÇÃO PÚBLICA CONFORME O PRINCÍPIO DA FINALIDADE

Caroline Isabelle Vieira Barros Gretzitz
Laura Pereira de Bernardi
Orientadora: Prof. Dr. Bernardina Ferreira Furtado Abrão

Resumo: Este trabalho analisa a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018) inserida na Administração Pública, quanto à proteção e à regulamentação do compartilhamento de dados pessoais sensíveis entre os entes públicos, conforme o princípio da finalidade. A pesquisa ressalta a importância da proteção dos dados considerando sua relevância na contemporaneidade e delineia a evolução dessa proteção, de um direito atrelado à privacidade para um direito fundamental autônomo, em virtude da Emenda Constitucional nº 115, de 2022. O estudo aborda a definição e **a** aplicação do princípio da finalidade administrativa para fins de tratamento de dados e seu compartilhamento pela Administração Pública. A metodologia empregada foi de natureza teórica, com pesquisa bibliográfica, documental, legislativa, doutrinária e análise da jurisprudência relevante, incluindo a ADI 6649, a ADPF 695 e a Ação Civil Pública nº 5028572-20.2022.4.03.6100, além da análise crítica da aplicação da LGPD e do compartilhamento de dados no âmbito da colaboração entre a saúde pública e a saúde suplementar (privada). Conclui-se que a finalidade no tratamento e compartilhamento de dados pelo poder público é crucial para salvaguardar os direitos fundamentais, garantindo que a utilização de dados pessoais pela Administração Pública sirva ao interesse público.
Palavras-chave: Administração Pública, Poder Público, Setor Público, Direito Administrativo, Direito Digital, Princípio da Finalidade.

Abstract: This work analyzes the application of the General Personal Data Protection Law (Law No. 13,709, of 2018) within the Public Administration, regarding the protection and regulation of sensitive personal data sharing among public entities, according to the principle of purpose. The research highlights the importance of data protection considering its relevance in contemporary times and outlines the evolution of this protection, from a right linked to privacy to an autonomous fundamental right, by virtue of Constitutional Amendment No. 115, of 2022. The study addresses the definition and application of the principle of administrative purpose for data processing and sharing by the Public

Administration. The methodology employed was theoretical in nature, with bibliographic, documentary, legislative, and doctrinal research, as well as the analysis of relevant jurisprudence, including ADI 6649, ADPF 695, and Civil Public Action No. 5028572-20.2022.4.03.6100, in addition to a critical analysis of the application of the LGPD and data sharing within the scope of collaboration between public health and supplementary (private) health. It concludes that the purpose in the processing and sharing of data by the public authorities is crucial to safeguard fundamental rights, ensuring that the use of personal data by the Public Administration serves the public interest.
Keywords: Public Administration, Public Authority, Public Sector, Administrative Law, Digital Law, and Principle of Purpose.

Introdução

Num contexto social configurado pela onipresença de tecnologia — e no qual, crescentemente, o exercício das prerrogativas que os cidadãos possuem erige-se sobre a utilização de da internet, a World Wide Web e meios informatizados, a Administração Pública utiliza-se destes para maior eficiência na prestação de serviços públicos relevantes e essenciais à população e para otimização de políticas públicas, assim detendo, tratando e compartilhando quantia vultosa de dados pessoais dos administrados nesse processo. A vulnerabilidade dessas informações, contidas de aspectos intrínsecos à vida e à personalidade dos indivíduos, leva à necessidade de uma resposta jurídica robusta, a qual assegure que a eficiência estatal não comprometa os direitos fundamentais.

Sob esse contexto, a regulamentação do compartilhamento desses dados entre os entes públicos e a sua proteção emerge como um tema de relevância ímpar, o qual será extensivamente abordado no presente trabalho, o qual se propõe a examinar a aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018), com ênfase ao compartilhamento de dados sensíveis entre os entes da Administração Pública, pautando-se pelo princípio da finalidade como norteador para a legitimidade desse tratamento, e também como um limite essencial a essa prática.

Por fim, o trabalho perpassa a análise da evolução da proteção de dados pessoais no Brasil — outrora mera extensão do direito à privacidade, consolidado como direito fundamental autônomo em virtude da Emenda Constitucional nº 115, de 2022 — com destaque ao princípio da finalidade como balizador para a ação estatal, inclusive abordando a responsabilidade do Estado e de seus agentes de tratamento. Por fim, explora-se a matéria por meio de casos concretos paradigmáticos, tais como o julgamento das Arguição de Descumprimento de Preceito Fundamental 695 e Ação Direta de Inconstitucionalidade 6649 pelo Supremo Tribunal Federal e da Ação Civil Pública nº 5028572-20.2022.4.03.6100), além da análise crítica da aplicação da LGPD e do compartilhamento de dados especificamente na área da saúde, com ênfase na colaboração entre a saúde pública e a saúde suplementar (privada).

Para tanto, utilizou-se de pesquisa teórica, baseada principalmente na legislação relevante, além de bibliografia especializada (doutrina), periódicos, artigos científicos, documentos institucionais (tais como o guia de aplicação da Lei Geral de Proteção de Dados Pessoais à Administração Pública elaborado pela Autoridade Nacional de Proteção de Dados e o relatório de auditoria do Tribunal de Contas da União acerca da adesão da Administração Pública federal às regras estabelecidas pela LGPD), e julgados relevantes, oferecendo uma perspectiva ponderada acerca do compartilhamento de dados no setor público, enfatizando que o avanço tecnológico e eficiência na Administração Pública devem ser compatibilizados com os direitos fundamentais dos cidadãos, assegurando que o compartilhamento de dados pessoais adeque-se às finalidades legais e sirva ao interesse público, evitando que a coleta em massa de informações possibilitada pelo progresso tecnológico conduza à violação de direitos fundamentais.

I. A imprescindibilidade da proteção de dados na era da informação e o interesse público

Em virtude dos avanços tecnológicos e da informática, a proteção dos dados pessoais adquiriu relevância imprescindível — visto que, apesar de não se limitar "aos dados armazenados, processados e transmitidos na esfera da informática" (pois abarca a proteção de todo e qualquer dado pessoal, sem distinção do banco de dados e modo de armazenamento), os dados disponíveis compõem bancos de dados informatizados. Soma-se a isso a simultânea facilidade e velocidade de acesso, transmissão e cruzamento desses dados, a qual exacerba as hipóteses de interferência na seara dos direitos fundamentais das pessoas, no que é afeto ao "conhecimento e o controle de informações sobre a sua vida pessoal, privada e social" (Sarlet, Marinoni, Mitidiero, 2025, p. 722). Quanto à essa possibilidade de cruzamento de dados, Rodotà adverte que esse potencial de interconexão entre bancos de dados é indicativo do crescimento de "uma sociedade do controle, da vigilância e da classificação" (2008, p. 146), assim tornando a privacidade fundamental à "cidadania eletrônica" contemporânea (Rodotà, 2008, p. 145).

Nessa perspectiva, Doneda (2021, p. 26-27) escreve que o direito à proteção de dados pessoais, outrora intensamente próximo ao direito da privacidade, mas atualmente assume feições próprias — pois a proteção de dados não só implica uma tutela da privacidade, mas também a tutela do indivíduo face a diversas formas de controle e contra tratamento discriminatório, visando assegurar a "integridade de aspectos fundamentais de sua própria liberdade pessoal". Além disso, não é só a pessoa que é afetada individualmente, e sim classes e grupos sociais inteiros — a questão da proteção de dados não é individual, e têm desdobramentos sociais significativos (Doneda, 2021, p. 26-27).

Essa nova conjuntura da era da informação — a "era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas" — exige uma adequação do Direito, e a maneira como é

exercido e pensado cotidianamente (Pinheiro, 2021, p. 31). Afinal, "Toda mudança tecnológica é uma mudança social, comportamental, portanto jurídica." (Pinheiro, 2021, p. 32).

Sob esse prisma, o Direito deve ser simples e consciente das relações sociais em toda a sua complexidade, evoluindo conforme a sociedade muda — uma vez que o propósito do ordenamento jurídico é organizar centralizadamente o poder de sorte que possuiria o benefício da adaptabilidade frente às mudanças, assegurando assim o seu patamar de certeza e eficácia social (Pinheiro, 2021, p. 36). É essa capacidade adaptativa do Direito que informa a segurança do ordenamento em si, no que tange a sua estabilidade moldada pela "atuação legítima do poder capaz de produzir normas válidas e eficazes" (Pinheiro, 2021, p. 37).

Outrora, a tutela da privacidade direcionava-se à proteção oposta à intromissões indesejadas na esfera privada, porém, o progresso tecnológico e acentuação do processamento de informações modificaram o conceito de tais ingerências, posto que aumentou vertiginosamente a quantia de informações detidas por entes públicos e privados e esses dados constituem bem jurídico de valor ímpar, porquanto viabilizam que sejam delineados "perfis" contendo "hábitos de consumo, saúde, características genéticas e comportamentais de grande parte da população." (Tepedino, 2021, p. 13).

Neste enquadramento, Rodotà (2008, p. 157) cunha a ideia de que além de uma "sociedade da vigilância", cimenta-se a "sociedade da classificação", caracterizada justamente pela produção massiva de perfis de indivíduos, familiares e grupos. E é essa criação de perfis que faz com que a pessoa seja alvo constante de determinadas publicidades, destinatária de certa propaganda política ou excluída de oportunidades — essa viabilidade de obtenção detalhada de opiniões, gostos e predileções facilita ofertas cada vez mais personalizadas e individualizadas, contribuindo para uma "sociedade individual de massa" moldada pela uso geral de tecnologia da informação e da comunicação (Rodotà, 2008, p. 157).

Ainda, os indivíduos atualmente são identificados a partir de seus dados pessoais (fornecidos a empresas e a entidades públicas ou coletados de outras maneiras), e, sendo indicativos de características de suas personalidades, torna-se imprescindível a sua proteção, sob a concepção de que a privacidade constitui uma liberdade negativa, reconhecendo-se e tutelando-se a pessoa "contra abusos na obtenção e tratamento destes dados" (Doneda, 2021, p. 25).

No mesmo sentido, é mister destacar que atualmente, os indivíduos são frequentemente representados e avaliados a partir desses dados, de tal modo que a problemática da proteção de dados incide sobre outros aspectos afetos à personalidade. Isto porque seu tratamento pode ser feito de tal maneira que implique numa perda de autonomia, liberdade e individualidade (Doneda, 2021, p. 25-26).

Nessa conjuntura, ocorre a prática do "profiling", aplicável a indivíduos e a grupos de pessoas, a qual consiste na "elaboração de perfis de comportamento de uma pessoa a partir de informações

que ela disponibiliza ou que são colhidas", por meio do qual os dados pessoais são tratados "com o auxílio de métodos estatísticos e de técnicas de inteligência artificial" visando a obtenção de uma "metainformação" consistente na síntese dos hábitos, preferências e demais registros pessoais de uma pessoa (Doneda, 2021, p. 148).

Similarmente, também ocorre o *data mining* (mineração de dados), forma de coleta dos dados pessoais consistente na "busca de correlações, recorrências, formas, tendências e padrões significativos" com base em quantia grande de dados, mediante "auxílio de instrumentos estatísticos e matemáticos". Dessa maneira, partindo-se de uma quantia significativa de informação bruta e não categorizada, identificam-se informações potencialmente interessantes. Conforme cresce a quantia de informações disponíveis em "estado bruto", também cresce o potencial de extração de sua utilidade mediante *data mining* (Doneda, 2021, p. 150).

Nessa concepção mais primitiva do "dado" como recurso bruto, compreende-se como uma "informação em estado potencial", anterior à sua transmissão e interpretação, enquanto a informação "alude a algo além da representação contida no dado, chegando ao limiar da cognição" (Doneda, 2021, p. 139).

As duas técnicas supracitadas constituem exemplos do potencial útil obtido por meio de dados pessoais, ilustrando a possibilidade de "distanciamento entre a informação conscientemente fornecida pela pessoa e a utilidade na qual ela é transformada" no âmbito da coleta e tratamento dos dados pessoais (Doneda, 2021, p. 153-154).

Ademais, é relevante pontuar que a atual "sociedade da informação" proporciona à Administração Pública a oportunidade de coletar qualquer informação sobre os cidadãos, sob a premissa de eventual utilidade pública — tutela da saúde, segurança, etc — porém, quanto a isso Rodotà (2008, p. 162) observa que "a democracia é também sobriedade, até mesmo renúncia, quando pode existir um risco para a liberdade dos cidadãos" (Rodotà, 2008, p. 162).

Por fim, para os propósitos deste trabalho, conforme a definição de Pinheiro (2023, p. 19), "dados pessoais" são:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva (Pinheiro, 2023, p. 19).

Ainda, mais especificamente, a autora descreve os "dados pessoais sensíveis" são aqueles referentes a "características da personalidade do indivíduo e suas escolhas pessoais" (Pinheiro, 2023, p. 19), incluindo:

> (...) origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Pinheiro, 2023, p. 19-20).

Estes dados constituem uma categoria de informação sob maior potencial de servir a uma utilização discriminatória ou lesiva, caso conhecida e submetida a tratamento (Doneda, 2021, p. 144).

Porém, é evidente que mesmo os dados não classificados como sensíveis podem revelar aspectos definidos como sensíveis sobre a personalidade de um indivíduo ao serem tratados, podendo levar à discriminação — pois não é o dado em si mesmo que é discriminatório ou perigoso, mas seu potencial uso (Doneda, 2021, p. 144).

Já "tratamento dos dados" descreve toda e qualquer operação de manuseio de dados pessoais:

> (...) coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Pinheiro, 2023, p. 19).

Por fim, "titular" trata-se da pessoa a quem os dados pessoais tratados referem-se (Pinheiro, 2023, p. 19), enquanto "agentes de tratamento" são:

> O controlador que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção, e o operador que realiza algum tratamento de dados pessoais motivado por contrato ou obrigação legal (Pinheiro, 2023, p. 20).

1.1. A influência internacional, a Emenda Constitucional nº 115, e a consagração da proteção de dados como direito fundamental no ordenamento brasileiro

Anteriormente, na carência de menção expressa ao direito à proteção de dados pessoais no texto constitucional, este atrelava-se ao direito à privacidade (na concepção de uma "intimidade informática"), e ao direito ao livre desenvolvimento da personalidade, o qual abarca o direito à livre disposição sobre os dados pessoais — portanto, cuida-se não só de uma proteção dos dados em relação ao seu conhecimento e utilização por terceiros, cabendo falar em direito à autodeterminação informativa, a exemplo da normativa alemã e espanhola (Sarlet, Marinoni, Mitidiero, 2025, p. 723).

Sobre o tema, vale destacar que o Tribunal Constitucional Federal da Alemanha decidiu de maneira paradigmática sobre a constitucionalidade de características atreladas ao censo populacional, asseverando a incompatibilidade da dignidade humana e o direito ao livre desenvolvimento da personalidade com a não proteção individual à ilimitada coleta, armazenamento, aproveitamento, transferência e divulgação de dados pessoais (Sarlet, Marinoni, Mitidiero, 2025, p. 723).

Assim, segundo a Corte Constitucional alemã (Bundesverfassungsgericht, 15 de dezembro de 1983), a privacidade expande a sua definição além do mero "direito a ser deixado só", tornando-se imprescindível à "liberdade existencial", na forma de "tutela das escolhas de vida contra toda forma de controle público e de estigmatização social" — não é tão só o direito do indivíduo à exclusão de terceiros de potencialmente conhecerem ou divulgarem informações relativas à sua pessoa, mas também é o direito ao controle da utilização dessas informações em todo momento e lugar. Assim,

molda-se num poder social de "controlar diretamente os sujeitos públicos e privados que tratam os dados pessoais".

De tal forma, numa conjuntura social na qual informação é a mais valorosa riqueza, a tutela da privacidade assegura o equilíbrio dos poderes — isto pois a ausência de privacidade representa risco à integridade da democracia, não apenas às liberdades individuais (Rodotà, 2008, p. 144).

Portanto, neste cenário, no meio da União Européia, o modelo de direito à proteção de dados baseia-se no direito à autodeterminação informativa, o qual amplia o conceito do direito a ser deixado só (poder do indivíduo de impedir certos usos de informações referentes a si mesmo), para incluir o poder de controlar, a qualquer momento, o uso alheio de suas informações — com ênfase no consentimento do titular e seu direito de acessar todo conjunto de informações coletadas sobre a sua pessoa, cuidando-se de poder difuso (que não requer intermédio burocrático), haja vista que é exercido de maneira direta pelo interessado em face de todos os sujeitos (públicos e privados) que coletam dados pessoais (Rodotà, 2008, p. 148-149).

Em adição, no modelo europeu, devido à coleta de informações atrelar-se a princípios fundamentais (principalmente o da finalidade, que será explorado mais à frente), há previsão de hipóteses de "indisponibilidade", nas quais nem sequer o interessado pode consentir a certos usos de seus dados — tal como previsto na legislação italiana (Código em matéria de proteção de dados pessoais) no que concerne os dados pessoais sensíveis (destacadamente aqueles referentes à saúde e às opiniões). Essa vedação à concessão desses dados dá-se para evitar que o indivíduo venha a consentir ao uso de dados que possam levar à discriminação ou violação da dignidade da pessoa em razão de contrapartida econômica, dessa maneira efetivamente protegendo os dados íntimos de tornarem-se mera mercadoria (Rodotà, 2008, p. 149).

Como delineado por Rodotà (2008, p. 154-156), essa tutela da proteção de dados que determina "indisponibilidade" ou "inalienabilidade" de categorias específicas de dados justifica-se pela matéria estar incluída na seara dos direitos fundamentais — logo, os dados pessoais não podem ser transformados em objetos de propriedade ou submetidos à pressão da lógica do mercado, visto que a relação entre o indivíduo e suas próprias informações faz parte dos direitos da personalidade. Dado isso, a concorrência não deve ser o imperativo social preponderante, precisando ser compatível com "com os direitos fundamentais, com a liberdade de escolha e o respeito da dignidade" (Rodotà, 2008, p. 163). Portanto, não se perde o direito de controle sobre os próprios dados pessoais mesmo quando em poder de terceiros — independentemente de tratarem-se de entes públicos ou privados (Rodotà, 2008, p. 154-156).

Nesse contexto, influenciada pelos ordenamentos jurídicos estrangeiros, a doutrina brasileira já defendia a essencialidade do reconhecimento de um "direito fundamental autônomo implicitamente

positivado à proteção de dados pessoais", considerada uma "leitura harmônica e sistemática do texto constitucional de 1988" (Sarlet, Marinoni, Mitidiero, 2025, p. 723).

Tal direito eventualmente foi confirmado pelo STF em abril e maio de 2020, no julgamento histórico da ADI 6.387-DF (Relatora Ministra Rosa Weber), na qual se discutiu a constitucionalidade da Medida Provisória n. 954, de 17.04.2020, da Presidência da República. A Medida Provisória exigia às empresas de telecomunicações (fixas e móveis) a disponibilização dos nomes completos, endereços e números de telefone dos usuários PN e PJ para o IBGE durante a pandemia do COVID 19 para fins de uso exclusivo e direto de elaboração de estatísticas oficiais por meio de entrevistas domiciliares (Sarlet, Marinoni, Mitidiero, 2025, p. 724). O STF julgou a medida impugnada como inconstitucional em razão de sua desproporcionalidade, reconhecendo violação à proteção de dados pessoais, direito fundamental autônomo implicitamente positivado à época, segundo a doutrina prevalente supracitada (Sarlet, Marinoni, Mitidiero, 2025, p. 724).

Em contraponto à percepção do STF de que tal medida seria desproporcional e configuraria uma violação de proteção de dados pessoais, escreveu Han (2020a) no período de pandemia do COVID 19 acerca de como Estados asiáticos (tais como Japão, Coreia, China, Hong Kong, Taiwan e Singapura) com uma tradição cultural confucionista — e consequentemente mais autoritária — e na qual impera o coletivismo, despido de individualismo proeminente, valeram-se de maneira intensa da vigilância digital, crendo no potencial do *big data* para defender-se da pandemia. Na Ásia, especialistas em informática e macrodados contribuem para o combate à epidemias, e não só virologistas e epidemiologistas (Han, 2020a).

Isso deu-se porque na Ásia a consciência crítica em face da vigilância digital e do *big data* é quase nula — não se fala em proteção de dados mesmo em Estados liberais como o Japão e a Coreia, não há *backlash* da população diante da recopilação frenética de dados pelas autoridades: "a digitalização os embriaga diretamente" (Han, 2020a).

Especialmente, na China há uma vigilância social exacerbada propiciada pela troca irrestrita de dados entre os fornecedores da Internet e de telefonia celular e as autoridades — de fato, não há proteção de dados, visto que inexiste a "esfera privada" à sociedade chinesa (Han, 2020a). Sobre essa troca abundante de dados, escreve Han (2020a):

> Enquanto isso a China introduziu um sistema de crédito social inimaginável aos europeus, que permitem uma valorização e avaliação exaustiva das pessoas. Cada um deve ser avaliado em consequência de sua conduta social. Na China não há nenhum momento da vida cotidiana que não esteja submetido à observação. Cada clique, cada compra, cada contato, cada atividade nas redes sociais são controlados. Quem atravessa no sinal vermelho, quem tem contato com críticos do regime e quem coloca comentários críticos nas redes sociais perde pontos. A vida, então, pode chegar a se tornar muito perigosa. Pelo contrário, quem compra pela Internet alimentos saudáveis e lê jornais que apoiam o regime ganha pontos. Quem tem pontuação suficiente obtém um visto de viagem e créditos baratos. Pelo contrário,

> quem cai abaixo de um determinado número de pontos pode perder seu trabalho (Han, 2020a).

Ainda, na China — a qual submete o indivíduo a uma vigilância rigorosa inconcebível no Ocidente, podendo falar-se num denominado "totalitarismo digital" segundo Han (2020b) — há 200 milhões de câmeras de vigilância, dotadas de inteligência artificial e grande eficiência técnica para reconhecimento facial, inescapáveis em quaisquer espaços públicos. Toda essa infraestrutura demonstrou-se extremamente eficaz para conter a epidemia, sem resistência, diferentemente dos fechamentos de fronteira realizados na Europa (Han, 2020a).

Entretanto, uma abordagem de combate digital ao vírus comparável à chinesa seria inviável na Europa, em razão da proteção de dados (regida pela GDPR, a *General Data Protection Regulation*, ou Regulamento Geral sobre a Proteção de Dados, em português) — enquanto na China os dados sensíveis dos clientes de fornecedores de telefonia celular e de Internet são compartilhados com os serviços de segurança e com os ministérios de saúde (Han, 2020a).

Sobre a digitalização crescente impulsionada pela pandemia, Han (2020a) sugere que pela epidemia devêssemos até mesmo redefinir a soberania, e que a Europa aferrar-se a modelos ultrapassados de soberania ao fechar as fronteiras e proclamar estado de alarme — "É soberano quem dispõe de dados".

Todavia, Han (2020b) ressalta que não apenas a China solicita dados de seus cidadãos visando seu controle e disciplina — o procedimento de *scoring* (qualificação de crédito social) chinês baseia-se nos mesmos algoritmos adotados pelos sistemas ocidentais de avaliação de crédito (tal como o FICO, nos Estados Unidos, e o Schufa, na Alemanha). A vigilância digital é um fenômeno que já ocorre em todos os lugares, à sua maneira (Han, 2020b).

Não apenas na China, mas em outros países asiáticos a vigilância digital foi empregada para conter a epidemia, ausentes demasiadas considerações à proteção de dados e à esfera privada: em Taiwan o Estado valeu-se do envio simultâneo a todos de SMS para localizar aqueles que estiveram em contato com infectados e para informar acerca dos lugares e edifícios em que houve pessoas contaminadas, e, inclusive, numa fase inicial usou a conexão de diversos dados para a localização de possíveis infectados em razão das viagens que fizeram (Han, 2020a).

Já na Coreia, realizou-se um "monitoramento digital implacável dos contatos", de competência da polícia, mediante rastreamento feito com métodos tecnológicos próprios da criminalística (Han, 2020b). Dessa maneira, aqueles que se aproximavam de edifícios em que esteve um infectado recebiam um sinal de alarme através do "Corona-app", visto que todos os lugares em que infectados estiveram estavam registrados no aplicativo, além de terem sido instaladas câmeras de vigilância em todos os edifícios do país — com os dados de telefonia celular e do material filmado em vídeo, possibilitou-se a criação de um perfil completo do movimento de um infectado, os quais eram publicados, e nos escritórios do Ministério da Saúde coreano funcionários denominados *tracker*

analisavam o material filmado para completar o perfil de movimento dos infectados e localizar aqueles que estiveram em contato com eles (Han, 2020a).

Ademais, o autor alerta da possibilidade da China promover o seu "Estado policial digital" como um modelo de sucesso contra a pandemia, e exibir a "superioridade" de seu sistema orgulhosamente, sendo possível que o Estado policial à maneira chinesa alcance o Ocidente — assim tornando "o estado de exceção" na situação normal (Han, 2020a).

Sob essa conjuntura, e considerada a imprescindibilidade da salvaguarda da privacidade, conforme Moraes (2025, p. 190) a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, adicionou ao rol dos direitos e garantias individuais o direito à proteção de dados pessoais ("Art. 5º., LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."). Além disso, asseverou que compete à União a organização e fiscalização da proteção e tratamento dos dados pessoais ("Art. 21. Compete à União, XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei."), e, adicionalmente, legislar de maneira privativa acerca da proteção e tratamento de dados pessoais ("Art. 22. Compete privativamente à União legislar sobre: XXX - proteção e tratamento de dados pessoais.").

Logo, constata-se que a decisão do STF não só foi chancelada mas foi reforçada pela legitimação democrática conferida pela emenda constitucional (Sarlet, Marinoni, Mitidiero, 2025, p. 725). Sendo assim, a EC/115 alçou a proteção de dados pessoais ao status de direito fundamental autônomo com âmbito de proteção próprio (independentemente de sua intersecção com outros direitos), conferindo-o incontrovertivelmente o caráter normativo de superioridade sobre o ordenamento jurídico nacional remanescente e a característica de restrição material à reforma constitucional (observados os limites de circunstância, tempo e formalidade, vide o art. 60, § 1.º a 4.º, da CF). Ainda, conforme o art. 5.º, § 1.º, CF, as normas pertinentes à proteção de dados são providas de aplicabilidade imediata (direta) e vinculam de maneira direta todos os agentes públicos e privados (Sarlet, Marinoni, Mitidiero, 2025, p. 726).

Sob esse contexto, o escopo da salvaguarda multifacetada dos dados pessoais (no que se refere à coleta, armazenamento, tratamento, utilização e transmissão de dados pessoais) compreende:

> (a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos ou privados;
> (b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais;
> (c) o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados;
> (d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados;
> (e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados (Sarlet, Marinoni, Mitidiero, 2025, p. 727).

Adicionalmente, de modo complementar à dimensão negativa da proteção de dados, é incumbência estatal a responsabilidade de protegê-los valendo-se de prestações positivas de norma e fato — note-se, mediante regulação infraconstitucional efetiva (Sarlet, Marinoni, Mitidiero, 2025, p. 727). Na mesma linha, redigiu Doneda:

> A atuação de uma disciplina de proteção de dados pessoais compreende uma ação positiva do Estado que, para atingir o patamar de isenção e autoridade necessárias a um direito fundamental, deve ser confiada a uma autoridade de garantia caracterizada pela autonomia e independência (Doneda, 2021, p. 318).

No Brasil, esta garantia advém da Autoridade Nacional de Proteção de Dados (ANPD), conforme a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD):

> Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (Redação dada pela Lei nº 14.460, de 2022)
> Art. 5º, XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019)

II. O Princípio da finalidade do Direito Administrativo como limite ao tratamento e compartilhamento de dados pessoais

Precipuamente, para adentrar-se no âmbito da aplicação do princípio da finalidade aplicado ao tratamento de dados pela Administração Pública e o compartilhamento de dados entre órgãos públicos, faz-se necessário explicar do que se trata o princípio da finalidade na seara administrativa.

Inicialmente, destaca-se que a principiologia do Direito Administrativo aplica-se ao regime jurídico administrativo — disciplina jurídica peculiar caracterizada por visar "equilíbrio entre a satisfação dos interesses coletivos e a proteção das liberdades individuais", da qual é proveniente a bipolaridade "autoridade da Administração" em contraposição à "liberdade do indivíduo" (Nohara, 2025, p. 6).

Para explicar-se o princípio da finalidade, primeiramente é necessário destacar os princípios da legalidade e da supremacia do interesse público, sobre os quais se constrói o restante da principiologia administrativa, conforme Di Pietro (2025, p. 200):

> Os dois princípios fundamentais e que decorrem da assinalada bipolaridade do Direito Administrativo – liberdade do indivíduo e autoridade da Administração – são os princípios da legalidade e da supremacia do interesse público sobre o particular, que não são específicos do Direito Administrativo porque informam todos os ramos do direito público; no entanto, são essenciais, porque, a partir deles, constroem-se todos os demais (Di Pietro, 2025, p. 200).

Primeiramente, conforme o princípio da legalidade, em toda a sua atividade funcional sujeita-se o administrador público aos "mandamentos da lei e às exigências do bem comum", dos quais não pode afastar-se ou desviar-se, "sob pena de praticar ato inválido e expor-se a responsabilidade

disciplinar, civil e criminal" (Meirelles, 2020, p. 79). Isto é, a eficácia da atividade administrativa é condicionada ao atendimento da Lei e do Direito, e, além disso, implica não só a atuação conforme a lei, mas também a observância dos princípios administrativos (Meirelles, 2020, p. 79). Nesse sentido, detalha Meirelles sobre a distinção entre o conceito de legalidade na esfera pública e administrativa em comparação à sua denotação para o particular:

> Na Administração Pública não há liberdade nem vontade pessoal. Enquanto na administração particular é lícito fazer tudo que a lei não proíbe, na Administração Pública só é permitido fazer o que a lei autoriza. A lei para o particular significa "pode fazer assim"; para o administrador público significa "deve fazer assim" (Meirelles, 2020, p. 79).

Sob essa perspectiva, destaca-se a relação entre a finalidade da conduta administrativa e a lei — "Uma atividade e um fim supõem uma norma que lhes estabeleça, entre ambos, o nexo necessário" (Lima, s. d., p. 21 *apud* Carvalho, 2025, p. 96).

Tal relação dá-se porque, em regra, as leis administrativas são de ordem pública - seus preceitos não podem ser descumpridos, nem mesmo na hipótese de acordo ou vontade conjunta de seus aplicadores e destinatários, pois contêm "poderes-deveres, irrelegáveis pelos agentes públicos" (Meirelles, 2020, p. 79). Em outros termos, "a natureza da função pública e a finalidade do Estado impedem que seus agentes deixem de exercitar os poderes e de cumprir os deveres que a lei lhes impõem", dado que esses poderes são conferidos à Administração Pública com o propósito de utilização em benefício da coletividade, e por isso não são passíveis de renúncia ou descumprimento pelo administrador sem ofensa ao bem comum — "o supremo e único objetivo de toda ação administrativa" (Meirelles, 2020, p. 79).

Nesse contexto, depreende-se que os poderes concedidos pela lei à Administração Pública e a sua atuação vinculam-se à finalidade pública (interesse público) legalmente prevista:

> Em consequência, se, ao usar de tais poderes, a autoridade administrativa objetiva prejudicar um inimigo político, beneficiar um amigo, conseguir vantagens pessoais para si ou para terceiros, estará fazendo prevalecer o interesse individual sobre o interesse público e, em consequência, estará se desviando da finalidade pública prevista na lei. Daí o vício do desvio de poder ou desvio de finalidade, que torna o ato ilegal (Di Pietro, 2025, p. 204-205).

Isto posto, o princípio da finalidade é atrelado ao princípio da supremacia do interesse público — expressamente previsto no artigo 2º, caput, da Lei nº 9.784 de 1999 (Lei do Processo Administrativo Federal), e desenvolvido no seu parágrafo único, inciso II, como a exigência de "atendimento a fins de interesse geral, vedada a renúncia total ou parcial de poderes ou competências, salvo autorização em lei" (Di Pietro, 2025, p. 205-206). No mesmo sentido, Carvalho (2025, p. 96) escreve que segundo o princípio da finalidade o objetivo almejado pela Administração Pública é tão somente o interesse público — nunca o particular, do contrário haveria uma atuação discriminatória.

Sobre a supremacia do interesse público, detalha Nohara (2025, p. 7) sobre sua relação íntima com o alcance da finalidade (ou interesse) pública:

> Estes pressupostos fundamentam-se na supremacia do interesse público sobre o particular, tendo em vista que a finalidade-última do Estado, que alicerça sua formação como ente dotado de soberania e apto a dirigir e controlar as ações de todos mediante a imposição da obediência, repousa na satisfação de interesses coletivos. Se a interpretação do direito público for outra, o Direito como um todo perde sua potencialidade de mecanismo de regulação direcionado para a realização de uma sociedade mais justa, e dele emerge sua faceta mais obscura de instrumento de pacificação para a manutenção dos interesses de poucos (Nohara, 2025, p. 7).

Ainda, a finalidade também trata-se do resultado que a Administração visa alcançar com seus atos, que sempre prima pelo interesse público, conforme Di Pietro (2025, p. 494):

> Pode-se falar em fim ou finalidade em dois sentidos diferentes: 1. em sentido amplo, a finalidade corresponde à consecução de um resultado de interesse público; nesse sentido, se diz que o ato administrativo tem que ter finalidade pública; 2. em sentido restrito, finalidade é o resultado específico que cada ato deve produzir, conforme definido na lei; nesse sentido, se diz que a finalidade do ato administrativo é sempre a que decorre explícita ou implicitamente da lei (Di Pietro, 2025, p. 494).

Isto posto, em caso de infrigimento da finalidade legal do ato (em sentido estrito) ou de desatendimento de seu fim de interesse público (sentido amplo), o ato será ilegal e configurará desvio de poder (Di Pietro, 2025, p. 495).

Embora a Constituição de 1988 não elenque expressamente o princípio da finalidade entre os princípios administrativos em seu art. 37, caput (o qual se limita aos princípios da legalidade, da impessoalidade, da moralidade administrativa, da publicidade e eficiência), este é citado dentre aqueles definidos pela Constituição do Estado de São Paulo (art. 111), a qual acrescentou aos princípios constitucionais já estabelecidos também os princípios da razoabilidade, finalidade, motivação e interesse público. Nesse mesmo sentido, a Lei nº 9.784/99, refere-se ao princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência no seu art. 2º (Di Pietro, 2025, p. 200).

Ainda, são relacionados ao princípio da finalidade os princípios da razoabilidade e proporcionalidade — o segundo é um dos aspectos do primeiro, visto que o princípio da razoabilidade refere-se à proporcionalidade entre meios e fins. Esta concepção está contida no art. 2º, parágrafo único, inciso VI da Lei nº 9.784/99: "VI - adequação entre meios e fins, vedada a imposição de obrigações, restrições e sanções em medida superior àquelas estritamente necessárias ao atendimento do interesse público" (Di Pietro, 2025, p. 227).

Nesse sentido, o regime jurídico administrativo prima pelo simultâneo alcance das finalidades públicas e o respeito à liberdade individual, considerados os direitos fundamentais constitucionalmente previstos. Para estes fins, o juízo de razoabilidade e proporcionalidade anteriormente mencionado é o critério utilizado para mensurar o patamar de restrição da liberdade individual em nome do interesse público necessário para que não haja prejuízo ao núcleo essencial de garantias ou direitos fundamentais (Nohara, 2025, p. 7).

2.1. O princípio da finalidade no âmbito do tratamento de dados pessoais pela administração pública, conforme a LGPD

Sob contornos mais gerais, Doneda (2021, p. 171) destaca entre a principiologia para a proteção de dados pessoais utilizada na legislação mundo afora, o princípio da finalidade. Este determina que "toda utilização dos dados pessoais deve obedecer à finalidade conhecida pelo interessado antes da coleta de seus dados", sendo dotado de notável significância prática, já que a restrição da transferência de dados pessoais a terceiros nele baseia-se, e sobre ele pode construir-se um critério para avaliar a "razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade)".

Sobre esse conceito de finalidade, em "Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)", Pinheiro escreve acerca do tratamento de dados pessoais conforme a sua finalidade, de acordo com os ditames da LGPD — "A linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas." (2023, p. 25).

Nessa mesma linha, o Guia Orientativo para o Tratamento de dados pessoais pelo Poder Público da Autoridade Nacional de Proteção de Dados (2023, p. 22), explica com base no princípio da finalidade (art. 6º, I, da LGPD) que o tratamento de dados pessoais pela Administração Pública deve visar a "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.", e, especificamente no que tange o setor público, esse tratamento deve atender a uma "finalidade pública", na "persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (vide o art. 23 da LGPD).

Esclarece-se que a expressão "setor público" é referente a tudo aquilo que não é setor privado" — isto é, "todas as infraestruturas, instituições, serviços e políticas que, em tese, pertencem ao conjunto da população brasileira", que, por pertencerem a esse conjunto, não são passíveis de apropriação por um grupo específico e nem podem alienar um determinado grupo de pessoas (Gaetani, 2022, p. 24), enquanto Administração Pública, no entendimento de Di Pietro (2025, p. 177), no seu sentido material ou objetivo, compreende "a atividade concreta e imediata que o Estado desenvolve, sob regime jurídico total ou parcialmente público, para a consecução dos interesses coletivos."

Portanto, igualmente às instituições privadas (que devem apresentar uma "finalidade clara e transparente" para o tratamento de dados), as pessoas jurídicas de direito público devem considerar a "finalidade pública e o interesse público" ao tratarem dados (Pinheiro, 2023, p. 65).

Dessa maneira, ambas as instituições públicas e privadas devem cientificar o usuário da captura de seus dados pessoais, qual a finalidade e a quantia de tempo pela qual serão utilizados, de

forma simples e acessível. O objetivo é favorecer a compreensão do cidadão, para que não haja dificuldade caso queira saber "quais informações são coletadas, para quais finalidades são utilizadas e quais os meios para exercer seus direitos previstos nos arts. 18 e 19 da lei", viabilizando que o usuário compreenda "quais dados a organização detém, como os utiliza e age para protegê-los." (Pinheiro, 2021, p. 288).

Ainda, o Guia (2023, p. 23) explica que a "finalidade pública" supracitada deve ser legítima (lícita, amparada numa autorização legal do tratamento), específica (escopo do tratamento e estabelecimento das garantias imprescindíveis à proteção dos dados pessoais deve ser delimitável com base na sua finalidade), explícita (exprimida precisa e claramente) e informada (proporcionada em linguagem descomplicada, de compreensão e acesso simples ao titular dos dados).

Outro corolário do princípio da finalidade no que tange o tratamento de dados pessoais é a limitação ao seu tratamento posterior — isto é, uma possível utilização secundária dos dados pessoais só pode ser feita se objetivar uma finalidade que seja compatível com a finalidade originária do tratamento desses dados (ANPD, 2023, p. 23). Semelhantemente, o princípio da adequação (art. 6º, II, da LGPD) exige "compatibilidade entre o tratamento dos dados pessoais e as finalidades que são informadas ao titular", com observância ao contexto em que esse tratamento é realizado — significando que o tratamento deve ser "compatível com o propósito informado ao titular" (ANPD, 2023, p. 23).

A relevância prática desse ditame demonstra-se principalmente nas hipóteses de "tratamento posterior de dados publicamente disponíveis e de uso compartilhado de dados pessoais pelo Poder Público" (ANPD, 2023, p. 23).

Sob esse prisma, quanto ao uso compartilhado de dados entre os entes da Administração Pública, prevê o art. 25 da LGPD que:

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Em outros termos, no caso do Poder Público, o manejo dos dados tratados é particularizado, de modo que "a sua estruturação e organização devem visar à execução das políticas públicas e à prestação de serviços" (Pinheiro, 2023, p. 66).

Nessa linha, detalha o art. 26 do mesmo diploma:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

Isto significa que incumbe à Administração Pública assegurar que o "uso compartilhado de dados segue os propósitos especiais que concernem à execução das políticas públicas" (Pinheiro, 2023, p. 66), e, simultaneamente, que "a ponderação entre a necessidade da publicidade das

informações disponíveis ao acesso garante que os direitos dos titulares sejam respeitados" (Pinheiro, 2023, p. 66).

Já no que tange dados publicamente disponíveis, conforme o art. 7º, § 3º da LGPD, seu tratamento é permitido desde que consideradas a finalidade, a boa-fé e o interesse público que fundamentaram a sua disponibilização (ANPD, 2023, p. 23).

Ademais, o posterior tratamento para finalidades diversas apenas poderá ser concretizado se "observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei" (art. 7º, § 7º da LGPD).

Outrossim, no que toca o compartilhamento de dados pessoais entre os entes da do Poder Público, estabelece o art. 26 da LGPD que devem ser atendidas "finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei" (ANPD, 2023, p. 23-24).

Sob esse contexto, a aferição da compatibilidade entre a finalidade originária e a secundária do tratamento de dados pessoais pela Administração Pública deve considerar:

> (i) o contexto e as circunstâncias relevantes do caso concreto;
> (ii) a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior;
> (iii) a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis;
> (iv) as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos; e
> (v) o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos, nos termos do art. 23 da lgpd (ANPD, 2023, p. 24).

2.2. A conformidade da Administração Pública ao princípio da finalidade no tratamento de dados

Em 2022, o Tribunal de Contas da União realizou uma auditoria (avisada com três meses de antecedência, no primeiro trimestre de 2021) acerca de *compliance* da Administração Pública à proteção e segurança de dados (conforme a LGPD), no qual 60 perguntas foram respondidas por 382 organizações públicas federais, resultando num relatório (Marques, 2022, p. 30).

A questão 6.1 do questionário do relatório do TCU visou aferir se as organizações realizaram a identificação e a documentação da finalidade das operações de tratamento de dados pessoais, de maneira compatível ao art. 6º, inciso I, da LGPD e conforme ao item 7.2.1 da ABNT NBR ISO/IEC 27701:2019, que recomenda às organizações que identifiquem e documentem os "propósitos específicos para o tratamento dos dados pessoais", além de assegurarem que os titulares entendam tais propósitos (Brasil, 2022, p. 29-30).

No entanto, as respostas à questão ilustraram que apenas 11% das organizações identificaram e documentaram a totalidade das finalidades das atividades de tratamento de dados pessoais (Brasil, 2022, p. 30).

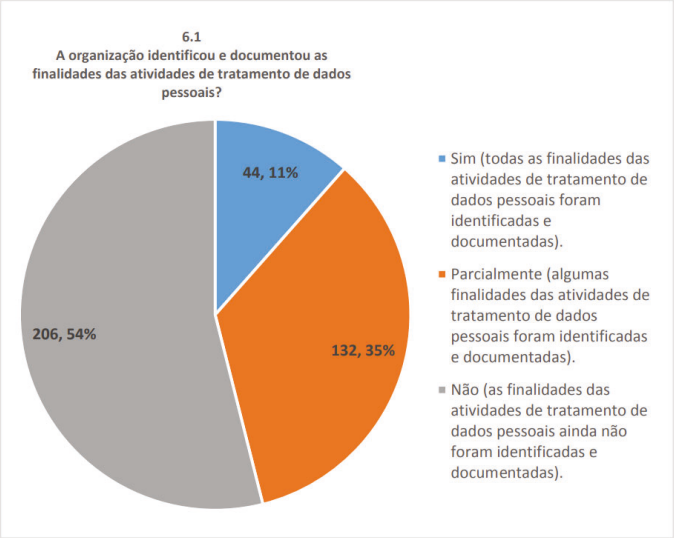

Figura 1 - Identificação e documentação das atividades de tratamento de dados pessoais (Fonte: Brasil, 2022, p. 30)

Ainda, quanto às organizações que informaram que realizaram a identificação de parcela ou totalidade das finalidades das atividades de tratamento de dados pessoais, adicionalmente responderam às subquestões 6.1.1 — para verificar se procedem à coleta somente dos dados estritamente necessários ao cumprimento das finalidades de tratamento de dados pessoais, vide a LGPD, art. 6º, incisos II e III; e item 7.4.1 da ABNT NBR ISO/IEC 27701:2019 — e 6.1.2 — para avaliar se procederam à análise da retenção (armazenamento) dos dados pessoais durante o tempo estritamente necessário ao cumprimento das mesmas finalidades, vide o item 7.4.7 da ABNT NBR ISO/IEC 27701:2019 (Brasil, 2022, p. 30).

Contudo, a maioria (51%) das organizações que respondeu à questão 6.1.1 não aferiu se coleta só os dados estritamente necessários para cumprir com as finalidades, vide a Figura 2. Quanto à questão 6.1.2, constatou-se que 61% destas organizações não avaliaram se os dados pessoais são retidos (armazenados) durante o tempo estritamente necessário para cumprimento das finalidades elencadas, conforme a Figura 3 (Brasil, 2022, p. 30).

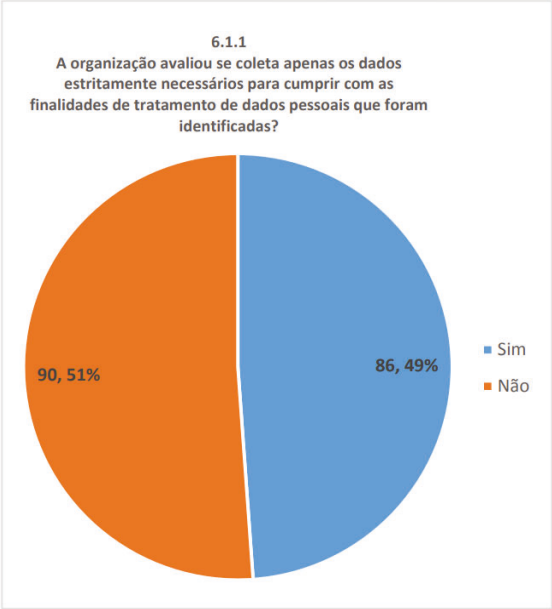

Figura 2 - Avaliação quanto à coleta de dados estritamente necessários às finalidades de tratamento (Fonte: Brasil, 2022, p. 31)

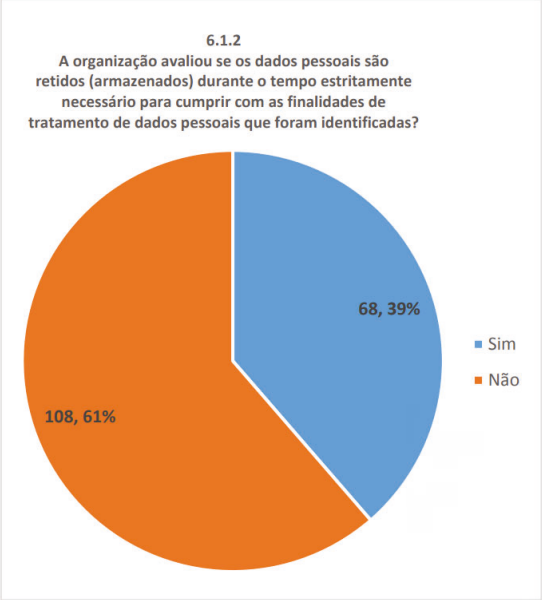

Figura 3 - Avaliação quanto ao tempo em que os dados pessoais são retidos (Fonte: Brasil, 2022, p. 31)

As respostas dessas questões denotam a indispensabilidade da avaliação e definição das finalidades dos procedimentos de tratamento de dados pessoais pelas organizações. A coleta de dados pessoais estritamente necessários ao cumprimento das finalidades exige preocupação especial, visto que a coleta de dados desnecessários pelas organizações é comum. Já no que tange o tempo de guarda de registros, a ANPD pode dispor sobre o tema, conforme o art. 40 da LGPD (Brasil, 2022, p. 31).

Perante o exposto, e considerado que ações já foram adotadas pela SGD/ME para orientação dos órgãos sob sua alçada em relação ao tópico, a equipe de auditoria propôs recomendação ao CNJ e ao CNMP de que, em razão do controle realizado sobre a atuação administrativa das organizações sujeitas às suas jurisdições, expeçam orientação acerca da imprescindibilidade de avaliar se coletam tão somente os dados estritamente necessários para as finalidades de tratamento de dados pessoais, e estes são retidos apenas durante o tempo estritamente necessário a esses objetivos, visto o art. 6º, incisos II e III, da LGPD e as diretrizes estabelecidas nos itens 7.4.1 e 7.4.7 da ABNT NBR ISO/IEC 27701:2019 (Brasil, 2022, p. 32).

III. A segurança de informações na Lei Geral De Proteção de Dados Pessoais

As iniciativas do governo digital ampliaram o foco das políticas de governos eletrônicos com o objetivo de instituir serviços públicos digitais mais simplificados, céleres e eficientes (Borges de Carvalho, 2020, p. 30). Deste modo, o Direito Administrativo assume um papel decisivo como autoridade capaz de fornecer segurança jurídica aos arranjos institucionais das políticas públicas de compartilhamento de informações pessoais. Ao passo que, deve ser responsabilizado civilmente quando os preceitos da LGPD são descumpridas, ou seja, na hipótese de vazamento ou compartilhamento ilegal de dados. Logo, a necessidade de proteção destas informações vulneráveis e sensíveis no meio digital é de exclusiva responsabilidade do órgão que o maneja na rede digital (Figueiredo, 2024, p. 37).

Quanto à proteção de dados pessoais no Brasil, uma das legislações mais influentes no seu processamento é a LGPD. Com a sua promulgação, ficou ainda mais claro que a proteção de dados pessoais é um direito essencial de todo indivíduo, de modo que deve ser respeitado para que preserve sua imagem, dignidade e privacidade. Evidenciando, os riscos que todos os cidadãos correm de terem os seus dados expostos de forma indevida (Carvalho, 2022, p. 10).

Naturalmente os dados pessoais são importantes para os usuários, uma vez que ao depositarem essas informações sob tutela do Estado, acreditam que estão resguardados pelo armazenamento seguro e legal do Órgão (Carvalho, 2020, p. 20). Tal fato, mostra-se ainda mais essencial devido à rápida capacidade de disseminação e o grande impacto que essas informações podem causar quando expostos de forma indevida (Pinheiro; Lotufo, 2020, p. 31). Isso se dá pois não há limites materiais ou fronteiriços na rede virtual, permitindo que uma informação pessoal — muitas vezes confidencial e privada — possa ser transferida de um lugar a outro rapidamente (Pinheiro; Lotufo, 2020, p. 31). Logo, visando impedir a exposição destes é necessária a adoção de medidas preventivas que assegurem a sua seguridade no âmbito digital (Carvalho, 2020, p. 20).

A LGPD em seu artigo 5º, incisos I, II, III e IV, traz diversos conceitos relacionados à tal normatividade, dentre eles, o conceito de dados pessoais, dados pessoais sensíveis e uso

compartilhado de dados. Considera-se dado pessoal as informações relacionadas à pessoa natural identificada ou identificável, por sua vez, os dados pessoais sensíveis são as informações relacionadas à origem étnica ou racial, convicção religiosa, opinião política, dados referentes à saúde, dados genéticos quando vinculados a pessoa natural, e por fim, uso compartilhado de dados trata-se da comunicação, difusão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais (Silva; Ferreira, 2025, p. 3).

> Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; 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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Nesse aspecto, a Administração Pública ao tratar dados, também é subordinada às determinações da LGPD — a qual foi inspirada na GDPR (General Data Protection Regulation – Regulamento Geral de Proteção de Dados) europeu, totalmente implantada na União Europeia em maio de 2018 (Nohara, 2025, p. 915). A Lei brasileira tem como finalidade resguardar a privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade e o exercício da cidadania pelas pessoas naturai, conforme especificado por Nohara (2025, p. 916).

É a ideia de que a segurança está aliada à privacidade durante todo o uso de dados, esteja ele em vulnerabilidade ou não (Carvalho, 2022, p. 15). Nesse contexto, a LGPD estabelece regulamentações rígidas, que vinculam a administração pública o cumprimento de uma série de requisitos e procedimentos ao longo do ciclo de tratamento de dados, todos inseridos em um quadro de governança bem estruturado. Consequentemente, o processamento de dados deve seguir as bases legais e princípios protegidos, garantindo os direitos dos titulares e adotando boas práticas e a estrutura de governança adequada (Figueiredo, 2024, p. 27). Sob esse viés, Pinheiro (2023, p. 38) justifica a necessidade de regulamentação vinculada à privacidade no trecho:

> Essa metodologia foi uma forma mais objetiva encontrada pelo regulador de se tratar uma regra que, apesar de se referir a direitos fundamentais, como a proteção da privacidade, necessita de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais. Portanto, a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico (Pinheiro, 2023, p. 38).

Dessa forma, a relação entre a regulamentação e a necessidade de proteção à privacidade dos usuários depositários dos bancos de dados, representa a necessidade de que as informações sejam tratadas de forma ética e responsável. Diante disso, ao exigir que as empresas e órgãos públicos sejam transparentes sobre as suas práticas, a LGPD dá capacidade aos titulares e contribui para a construção de uma sociedade mais justa, ética, transparente e segura (Figueiredo, 2024, p. 32).

Assim, uma vez que a proteção de dados é um direito de cada indivíduo, a LGPD, visa legislar sobre a privacidade dos usuários, principalmente no que diz respeito à coleta e tratamento de seus dados, disciplinando ainda, sobre o compartilhamento de dados pessoais pelo poder público entre seus Entes (Figueiredo, 2024, p. 13). Logo, é nítido que a proteção de dados na Administração Pública é um tópico de extrema importância, uma vez que as entidades governamentais lidam com uma quantidade significativa de informações pessoais, de forma que sua administração envolve o tratamento adequado, a coleta, o armazenamento e o uso de informações pessoais, garantindo a privacidade e a segurança destas bases (Figueiredo, 2024, p. 14).

Nesse sentido, o artigo 23, inciso I da LGPD, prevê um conjunto de requisitos que são necessários para o tratamento de dados pelo Poder Público vez que, deverá ser realizado em atendimento de sua finalidade pública, na persecução do interesse público, de forma que execute as atribuições legais do serviço público, bem como um encarregado a administrar estes dados (Figueiredo, 2024, p. 14).

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua **finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público** [grifo nosso], desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Portanto, ao passo que a utilização dos dados deve ser padronizada entre si, as informações passam a ser viáveis ao uso dos Entes, permitindo o compartilhamento destes entre os diferentes Órgãos e estabelecendo a relação jurídica entre o Poder Público e o indivíduo titular dos dados (Figueiredo, 2024, p. 15). No entanto, esse vínculo nasce em desequilíbrio entre seus partícipes, uma vez que o Estado possui amplas prerrogativas para a coleta e armazenamento de dados e em contrapartida o usuário apenas cede as suas informações, confiando plenamente que suas informações depositadas estão seguras e serão usadas sob o pretexto de boa-fé do Estado. Então, visando mitigar esta disparidade de posicionamento entre os integrantes da relação jurídica, o Poder Público possui uma série de previsões legais que limitam a execução de sua atividade com os dados que lhe são cedidos (Figueiredo, 2024, p. 16). Nesse sentido, o tratamento de dados pela Administração Pública,

conforme a LGPD, deve garantir uma série de fatores, de modo a reafirmar a adequação do tratamento e a garantia de resguardo das informações, quais sejam:

> (i) para o cumprimento de obrigação legal ou regulatória pelo controlador; **(ii)pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres** [grifo nosso]; (iii)para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iv)quando necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (v)para o exercício regular de direitos em processo judicial, administrativo ou arbitral; (vi)para a proteção da vida do titular ou de terceiro; (vii)para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (viii)quando necessário para atender aos interesses legítimos do controlador ou de terceiro; (ix)para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Pinheiro, 2023, p. 39).

Dessa forma, é possível compreender que ao tratar os dados pessoais, deve-se conciliar tanto as exigências da LGPD como as normas que regem a sua atuação. Logo, a proteção de dados não pode ser um obstáculo à transparência e ao controle social, especialmente, no que condiz às informações de interesse público (Figueiredo, 2024, p. 16). A partir desta análise, é crucial compreender as disposições da referida Lei à luz da Constituição Federal, vez que seus princípios normatizam a Administração Pública e relacionam-se diretamente com o direito à privacidade dos cidadãos (Figueiredo, 2024, p. 19).

Na redação do artigo 37 da Constituição Federal, estabelece-se os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Esses princípios são fundamentais para garantir a transparência da Administração Pública, promovendo confiança dos cidadãos nas instituições públicas. Adequando ainda, com os fundamentos da LGPD, no sentido de que incluem a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Desse modo, ao adotar esta abordagem, garante-se que as informações dos cidadãos sejam tratadas de forma ética e segura e em conformidade com a legislação vigente e aos direitos constitucionais (Figueiredo, 2024, p. 20).

A segurança de informação desempenha um papel crucial na proteção dos dados pessoais dos cidadãos, de modo a implementar medidas rígidas e exigentes de segurança digital, visando mitigar o risco de violação de dados e garantir a integridade, confidencialidade e disponibilidade de informações. Ainda, vale ressaltar que o direito à privacidade representa um dos princípios basilares dos direitos individuais e encontra-se tanto na Constituição Federal quanto na LGPD. Cabendo então, ao Poder Público o compromisso de preservar esse direito, assegurando que as informações pessoais dos cidadãos sejam tratadas de forma lícita, ética e segura, adotando medidas de segurança em conformidade com as suas obrigações legais, o Poder Público não apenas cumpre com os princípios democráticos e os direitos constitucionais dos cidadãos (Figueiredo, 2024, p. 20).

Portanto, a proteção de dados e a privacidade devem ser consideradas como elementos essenciais da governança digital, promovendo a confiança e legitimação das instituições públicas. De forma que, a segurança de informação não se trata apenas uma conformidade legal, mas de uma responsabilidade ética da Administração Pública que, exige uma análise baseada tanto no Direito Administrativo quanto no Direito Constitucional, permitindo que as entidades públicas forneçam a proteção de dados e promovam a confiança de seus depositários (Figueiredo, 2024, p. 21).

3.1. Responsabilidade civil objetiva e a teoria do risco administrativo

A LGPD garante à Administração Pública uma série de requisitos e etapas obrigatórias ao tratamento de dados, com o objetivo de manter uma estrutura adequada de governo aos administradores responsáveis por aquelas informações (Figueiredo, 2024, p. 20). Dessa forma, o tratamento deve atrelar-se a base legal e principiológica regente, de modo que a partir da sua garantia, o manejo de dados terão o direito como vínculo basilar de modo que a partir da adoção de boas práticas e adequada estrutura de governança estarão seguros nos bancos de dados governamentais. Assim, os princípios civis buscam estruturar um equilíbrio patrimonial e moral violado, garantindo que o Estado tenha amplos meios de alcance para que estas informações estejam seguras, permitindo que quando esses meios de segurança são desrespeitados e consequentemente estes dados sejam divulgados indevidamente, debata-se sobre a responsabilidade civil do Poder Público no tratamento destes (Figueiredo, 2024, p. 30).

Adota-se como Poder Público, todos os entes previstos na Lei de Informação, sendo eles os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; as autarquias, as fundações públicas e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (Figueiredo, 2024, p. 30). Logo, o tratamento de dados pessoais por pessoas jurídicas de direito público é fundamental para garantir que os órgãos públicos tratem os dados pessoais dos cidadãos de forma ética, transparente e responsável (Figueiredo, 2024, p. 31).

Desta forma, é válido ressaltar que tanto a Constituição Federal, em seu artigo 37, §6º, quanto o Código Civil, tratam da responsabilidade civil do Estado em regime objetivo, observando que:

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
> § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Isso se dá pois o Estado possui prerrogativas que o administrado não possui, sendo ele o sujeito jurídico, político e economicamente mais poderoso. De forma que, o indivíduo, tem posição

de subordinação, mesmo que protegido pelas normas do ordenamento jurídico (Figueiredo, 2024, p. 34). Diante disso, passa a considerar que o Estado deveria arcar com o risco natural de suas numerosas atividades. Quanto ao fato, determina Nohara (2025, p. 919):

> Ademais, quanto às responsabilidades, foi estabelecido que o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei nº 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo (Nohara, 2025, p. 919).

Nesse contexto, é relevante citar a teoria do risco administrativo como fundamento da responsabilidade objetiva do Estado (Figueiredo, 2024, p. 34). A teoria do risco administrativo determina responsabilidade do Estado quando verificado danos causados a terceiros no exercício de suas atividades, independentemente da existência de culpa por parte da administração pública. Mostrando-se vinculante nas hipóteses de vazamento de dados no momento de compartilhamento de dados. Logo, assumindo o risco de eventuais danos decorrentes das atividades. Ainda, quando confirmada, deve-se indenizar as vítimas mesmo que, quando não há culpa, devendo arcar com os prejuízos causados a terceiros em decorrência das ações ou omissões da Administração Pública, inclusive arcando com os danos causados por agentes públicos (Figueiredo, 2024, p. 35).

Dessa forma, a responsabilização objetiva do Estado garante que, sempre que a Administração Pública causa um dano, haja obrigação de indenizar os prejudicados, respondendo assim o Estado independente do ato que gerou prejuízo. Na mesma linha, expõe Coelho (2012, p. 741):

> Não é relevante a questão da licitude ou ilicitude do ato causador do dano; a indenização será devida em qualquer hipótese pelo Estado. Note-se que, se houver ato ilícito (dolo ou culpa) por parte de seu agente, terá o Estado direito de regresso contra ele. Paga, então, ao prejudicado e recupera com o agente culpado o valor da indenização. [...] **Para que o Estado se responsabilize objetivamente pelo dano, não se exige que o causador seja funcionário público efetivo ou comissionado [**grifo nosso**]**. O preceito normativo menciona a responsabilidade das pessoas jurídicas de direito público pelos danos causados por seus agentes, conceito amplo que alcança toda e qualquer pessoa a serviço do Estado. Por outro lado, se o dano é provocado por quem não cumpre essa condição, o Estado não é responsabilizável (Coelho, 2012, p. 741).

Assim, a violação de direitos individuais decorrente do tratamento de dados gera responsabilidade pelos danos causados, impondo-se a obrigação de indenizar os prejudicados independente de culpa (Figueiredo, 2024, p. 37). Embora esses dados possam ser tratados e compartilhados pela Administração Pública, para a execução de políticas públicas, sem a necessidade de consentimento, é imprescindível que sua dispensa seja tornada pública, garantindo os titulares dos dados sejam informados sobre a utilização de suas informações, como visto no artigo 11, incisos I, II, alíneas a, b e §2º da LGPD, conforme segue:

> Art. 11 - O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

Ainda, quanto às hipóteses de dispensa do consentimento do uso de dados pessoais, o artigo 7º incisos I, II, III e seguintes da LGPD vem elucidá-lo, como segue:

> Art. 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019). Vigência.
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Dessa forma, a dispensa do consentimento é uma exceção a regra de aplicabilidade ao compartilhamento de dados entre os Entes da Administração Pública, de modo que para que a anuência não seja uma obrigação, é necessário a ciência ao titular de dados sobre quais dados serão coletados, como será o armazenamento, quais os tratamentos realizados, finalidades delimitadas e por fim se esses dados serão repassados à outra pessoa (Figueiredo, 2024, p. 33). Logo, é possível observar um vínculo entre a relação da responsabilidade civil com o Princípio da Finalidade, uma vez que se interligam na funcionalidade e objetivação da captação de informações. Isso, sendo evidenciado justamente pela necessidade do Estado detalhar todas as etapas de tratamento e circulação dos dados até sua disponibilização aos Órgãos da Administração Pública. Este fato é de suma importância, que se mostra evidente no princípio da finalidade na qual os entes devem tratar dados pessoais de forma lícita, leal e transparente, respeitando os direitos fundamentais de liberdade e privacidade (Figueiredo, 2024, p. 36)

Nesse sentido, a responsabilidade civil da Administração Pública manifesta-se no quando os princípios e outros preceitos da LGPD são descumpridos pelos agentes da administração. O

descumprimento dessas normas pode ocasionar dano aos titulares, ou seja, àqueles que depositam suas informações e dados sob a tutela do Estado gerando a responsabilidade civil pública objetiva do Estado (Figueiredo, 2024, p. 37).

3.2. Agentes de tratamento da LGPD (autoridades)

A LGPD determina três figuras como agentes responsáveis pelo tratamento de dados, sendo ele o Controlador que pode ser pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais; o Operador, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e o Encarregado, que é a pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Figueiredo, 2024, p. 38).

Quanto ao fato, escreve Nohara (2025, p. 916):

> A LGPD traz toda uma gama de novos protagonistas no tratamento da informação:
> (1) os agentes de tratamento, quais sejam: o controlador e o operador, sendo o controlador a pessoa pública ou privada a quem compete decisões referentes ao tratamento de dados, e operador a pessoa natural ou jurídica que realiza o tratamento dos dados em nome do controlador;
> (2) o encarregado, sendo esta a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (Nohara, 2025, p. 916).

Conforme o trecho, vale ressaltar que ambos possuem responsabilidades legais diferentes quanto aos titulares dos dados e à Autoridade Nacional de Proteção de Dados. Logo, apesar de agente diferentes, seus comprometimentos são similares, vez que tanto o controlador quanto o operador são obrigados a manter os registros das atividades de tratamento de dados pessoais, sob a premissa de proteger as informações e reforçar as garantias que lhe são devidas, conforme previsto no artigo 36 da LGPD (Figueiredo, 2024, p. 38), observando que:

> Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.

Portanto, através da atuação de todos os agentes de tratamento, a LGPD assegura a transparência nas operações em si, uma vez que a própria ANPD exige que o Controlador elabore um relatório de impacto à proteção de dados pessoais, incluindo dados sensíveis para o seu tratamento (Figueiredo, 2024, p. 38), conforme o artigo 37 da LGPD:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Ainda, as atividades do Operador e do Controlador diferenciam-se nas responsabilidades em relação a eventuais danos causados. O Operador poderá ser responsabilizado solidariamente nos casos de deixar de observar as obrigações legais ou desobedecer às instruções do Controlador. As violações

cometidas pelo Controlador serão motivo para sua responsabilização direta, pois a LGPD estabelece obrigações específicas ao controlador, fazendo com que seja inviável a sua figura não estar envolvida no tratamento (Figueiredo, 2024, p. 39).

Tal fato pode ser elucidada pelo artigo 42, §1, incisos I e II da LGPD:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Desta forma, pode-se concluir que a LGPD determina três agentes responsáveis pelo tratamento de dados: o Controlador, que toma as decisões; o Operador que executa o tratamento em nome do Controlador; e o Encarregado, que atua como intermediário aos agentes e a Agência Nacional de Proteção de Dados (Figueiredo, 2024, p. 40).

Em resumo, a lei obriga esses agentes a responsabilidade de manter registros das operações de tratamento e prevê a responsabilidade civil pelos danos causados, de modo que o Controlador é sempre responsável, enquanto o Operador responde solidariamente se descumprir suas obrigações legais (Figueiredo, 2024, p. 41).

IV. Compartilhamento de dados entre os entes da Administração Pública

O tratamento de dados pela Administração Pública deve ser subordinado e vinculado diretamente à base legal e principiológica aos direitos dos seus portadores (Figueiredo, 2024, p. 21). Isso inclui a necessidade de anonimização e pseudoanonimização dos dados, respeitando a identidade e a intimidade dos indivíduos e consequentemente, estabelecendo regras claras sobre o uso de dados, considerando a finalidade pelo qual ela foi coletada (Silva; Ferreira, 2025, p.4). Assim, a transparência sobre as práticas de compartilhamento, bem como a prestação de contas são essenciais para garantir a confiança da sociedade no uso dessas informações pelo poder (Silva; Ferreira, 2025, p. 4).

Conforme observado, a LGPD normatiza o controle de informações pessoais no Brasil, determinando obrigações e responsabilidades para as empresas que obtêm e manuseiam dados das pessoas. Os artigos 26 e 27 da LGPD, estabelecem as condições necessárias para o compartilhamento de informações pessoais pelos entes da Administração Pública, priorizando a proteção da privacidade e segurança dos cidadãos. Logo, é imprescindível que os Órgãos e Entes adotem procedimentos necessários para o manejo de informações pessoais (Silva; Ferreira, 2025, p. 5).

O gráfico abaixo representa quais os documentos que atualmente são exigidos pelo Poder Público, de modo que os cidadãos precisam dispor destas informações para os Entes, para que tenham acesso a um grande número de serviços público por eles proporcionados:

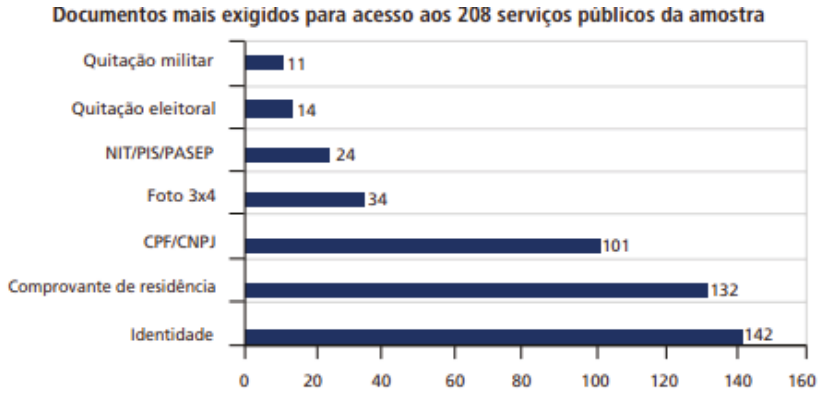

Figura 4 - Documentos mais exigidos para acesso a 208 serviços públicos brasileiros (Brasil, p. 24, 2018)

Diante destas informações, é imprescindível que os dados pessoais que estão em conhecimento do governo devem ser usados de forma racional e justificada, sendo utilizada unicamente para as suas funções legais. Ressaltando que o compartilhamento deve ser justificado pontualmente sob qual o objetivo da divulgação destas informações para os outros Entes da Administração Pública, de modo que o titular dos seus dados deve ser comunicado prontamente (Silva; Ferreira, 2025, p. 6).

Nesse aspecto, o Artigo 26, §1º, incisos I. III. IV, V, §2º da LGPD determina as regras e as restrições para a troca de informações pessoais entre os órgãos e entidades governamentais, com o objetivo de proteger a privacidade e segurança dos dados dos cidadãos, garantindo o processamento de informações pessoais seja feito de forma clara e responsável, conforme segue:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
> I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; (Incluído pela Medida Provisória nº 869, de 2018)
> V - na hipótese de a transferência dos dados objetivar a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados; ou (Incluído pela Medida Provisória nº 869, de 2018)

> § 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

Logo, é essencial que as autoridades sigam as diretrizes da LGPD e implementem medidas de segurança e transparência ao compartilhar informações pessoais. De modo que, é essencial que os usuários tenham conhecimento de seus direitos e possam manejar suas informações, assegurando a transparência e a prestação de contas no tratamento destas (Silva; Ferreira, 2025, p.6).

Ainda, no que condiz a autorização do Poder Público para o compartilhamento destes dados, o Artigo 27, incisos I, II, III e Parágrafo Único da LGPD, determina a necessidade de autorização do titular dos dados para que seja feita a difusão destes elementos para outras entidades públicas ou privadas legalmente, conforme segue:

> Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto:
> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
> III - nas exceções constantes do § 1º do art. 26 desta Lei.
> Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

Assim, para os órgãos públicos, a partilha de dados é uma estratégia para o aprimoramento das políticas governamentais, permitindo a integração dos setores como saúde, educação, segurança, entre outros. Essa prática potencializa novas metodologias de intervenção Estatal, visando o desenvolvimento econômico e a democratização de informações e comunicações (Silva; Ferreira, 2025, p. 7). Dessa forma, o compartilhamento de dados públicos gera inúmeras oportunidades para a sociedade, governos e para o setor privado. Consequentemente, essa gestão impulsiona a inovação, promovendo a transparência e aumentando a eficiência dos serviços públicos, estimulando também a economia, com a geração de empregos e o desenvolvimento de novos mercados. Ademais, o compartilhamento de dados configura-se como uma ferramenta fundamental que dinamiza o desenvolvimento sustentável e a melhoria da qualidade de vida da população, favorecendo a criação de novos setores (Silva; Ferreira, 2025, p. 13).

O incentivo ao compartilhamento de dados entre órgãos e entidades públicas traz diversos benefícios, permitindo a entrega de serviços com foco no cidadão, com a quebra de barreiras institucionais entre os próprios órgãos da própria administração pública. Os benefícios do uso compartilhado de dados entre os Entes são vários, entre eles, a simplificação do atendimento aos indivíduos, a redução de solicitações de emissão de documentos e requisição de outros serviços, o aumento do controle e diminuição de erros durante o processamento dos pedidos (Brasil, p. 20, 2018). Logo, é possível compreender que o compartilhamento de dados é uma forma de aprimoramento dos processos de gestão e qualidade dos dados, garantindo a eficiência do serviço público, bem como o resguardo da confiabilidade das informações (Araújo, 2021, p. 18).

No que concerne à execução de políticas públicas, é relevante discorrer que o conceito de políticas públicas não está sendo definido na LGPD. A ANPD, no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público, conceitua as políticas públicas como instrumentos para resolução de problemas sociais, como segue:

> Exemplo 7. Política de controle do tabagismo - Secretaria de Saúde realiza tratamento de dados pessoais de pessoas fumantes, atendidas em hospitais públicos, **para fins de planejamento e execução de política pública de controle do tabagismo e prevenção e tratamento do câncer de pulmão** [grifo nosso]. A política foi estabelecida em norma infralegal, da qual constam, entre outros elementos, objetivos, competências e meios de financiamento. Os dados pessoais são tratados pela própria Secretaria de Saúde e, eventualmente, compartilhados com a autarquia responsável por executar programa de orientação e auxílio a pessoas que desejam parar de fumar. **Por envolver dados sensíveis, o tratamento dos dados pessoais é realizado com base no art. 11, II, b, da LGPD. A finalidade é específica de execução de política públic**a [grifo nosso], estabelecida em regulamento, em conformidade com a LGPD (Brasil, 2023, p. 21).

Portanto, as políticas públicas são conceitos abstratos que se materializam através de instrumentos, como meio de enfrentamento de problemas públicos. Ainda, é relevante destacar que o programa encontra-se formalizado como ato normativo, permitindo o compartilhamento de dados para a execução de políticas públicas. Neste caso, engloba-se as duas hipóteses de dados, tanto sensíveis quanto pessoais, sendo materializadas a partir do artigo 7º da LGPD, que dispõe viável o compartilhamento de dados pessoais pela administração pública para fins de execução de políticas públicas (Vuori, 2024, p. 38).

Nessa linha, no que tange a conceituação de política pública, escreve Bucci (2006, p. 39):

> Política pública é o programa de ação governamental que resulta de um processo ou conjunto de processos juridicamente regulados — processo eleitoral, processo de planejamento, processo de governo, processo orçamentário, processo legislativo, processo administrativo, processo judicial — visando coordenar os meios à disposição do Estado e as atividades privadas, para a realização de objetivos socialmente relevantes e politicamente determinados. Como tipo ideal, a política pública deve visar a realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento dos resultados (Bucci, 2006, p. 39).

Ainda, as políticas públicas são complementares — preenchem lacunas normativas e concretizam princípios e regras, visando objetivo determinado, e, diferentemente das leis, não são gerais e abstratas, e sim elaboradas para a realização de objetivos determinados (Bucci, 2001, p. 11). Portanto, sucintamente, políticas públicas podem ser definidas, provisoriamente, como "programas de ação governamental voltados à concretização de direitos", os quais "funcionam como instrumentos de aglutinação de interesses em torno de objetivos comuns, que passam a estruturar uma coletividade de interesses", sendo que "toda política pública é um instrumento de planejamento, racionalização e participação popular" — dos quais os elementos são "o fim da ação governamental, as metas nas quais se desdobra esse fim, os meios alocados para a realização das metas e, finalmente, os processos de sua realização" (Bucci, 2001, p. 13).

A título de exemplo, cita-se o estudo sobre a política pública Programa Bolsa Família no documento "Proteção de dados pessoais em Políticas de Proteção Social: Contribuições a partir do Programa Bolsa Família, Diagnósticos e Recomendações nº 6". Nesta, é utilizado os dados do Cadastro Único para programas sociais — CadÚnico, havendo dados compartilhados com outras instituições da Administração, sendo divulgados para a Caixa Econômica Federal, os Municípios, a Secretaria Nacional de Renda de Cidadania, a Secretaria Nacional do Cadastro Único. Os dados, entre estes Entes são utilizados para a identificação, seleção e exclusão de beneficiários, pagamento do benefício, acompanhamento de condicionalidades, fiscalização, e também a formação de diagnósticos e desenvolvimento de novas políticas (Vuori, 2024, p. 41).

Nesse sentido, o princípio expresso no artigo 26 da LGPD proíbe a divulgação de dados pela administração pública a entidades privadas, exceto quando o compartilhamento for necessário para um fim específico de implementação descentralizada das atividades públicas.

De acordo com Di Pietro (2025, p. 573), a descentralização administrativa acontece quando há uma "divisão de poderes entre uma pessoa física ou jurídica", que ocorre quando o Estado atribui a empresa pública, autarquia, sociedade de economia mista, fundação pública ou consórcio público a prestação de serviços públicos ou autorizações quando uma entidade privada executa um serviço público em nome do Estado. Dito isso, a cooperação e compartilhamento dos dados torna a administração pública ainda mais produtiva, ágil e cada vez mais prática e segura (Araújo, 2021, p. 20).

Assim, a oportunidade de colaboração entre o setor público e privado no compartilhamento de dados públicos é essencial para garantir a eficiência e a segurança na troca de informações, uma vez que ambos os setores podem contribuir com as suas respectivas responsabilidades, conhecimentos e recursos visando viabilizar o compartilhamento de dados de forma responsável e benéfico para a sociedade. Vale destacar que ao estabelecer diretrizes claras e mecanismos de governança, o Estado promove a transparência, a proteção de dados e reforça o compromisso e adesão aos princípios éticos, garantindo que a colaboração seja pautada pelo interesse público e pelo respeito aos direitos individuais dos cidadãos (Silva, Ferreira, 2025, p. 14).

4.1. Compartilhamento de Dados Pessoais e a Transformação Digital na Saúde

A cooperação entre o setor público e privado tende a impulsionar a inovação e o desenvolvimento de soluções tecnológicas avançadas, uma vez que tem capacidade de potencializar o aproveitamento dos dados e o desenvolvimento de políticas públicas. Com este propósito, firmam-se estratégias para o compartilhamento de dados públicos entre os referidos Órgãos, reafirmando a necessidade de uso daquela informação para fins específicos (Silva, Ferreira, 2025, p. 14). Inclusive, esse apontamento mostra-se relevante na área da saúde, uma vez que a saúde suplementar, área que

abrange a operação de planos e seguros privados de assistência médica à saúde — Planos ou Seguros de Saúde —, utilizam-se de dados e informações dos seus beneficiários (Fragoso, 2020, p. 04).

No Brasil, o sistema de saúde é caracterizado pelo seu hibridismo, de modo que há a interação entre os serviços públicos e a oferta privada na prestação de serviços relativos à saúde. Em um dos polos, situa-se a rede pública conveniada com o Departamento de Informática do SUS (Data-SUS); de outro, o sistema privado, composto pela atuação direta de profissionais e estabelecimentos de saúde, além da cobertura prestada pelas operadoras de planos de saúde (Gregori, 2020, p. 11).

Regulada pela Agência Nacional de Saúde Suplementar (ANS), os serviços privados são compostos de seguradoras especializadas em saúde, medicina de grupo, cooperativas, instituições filantrópicas e autogestões. Os quais têm como objetivo a organização de um fundo conjunto que realizará a avaliação do risco, a definição do preço do plano, a cobrança, gestão financeira dos recursos, a organização da rede de assistência à saúde, o pagamento aos prestadores e a gestão de saúde dos seus beneficiários (Fragoso, 2020, p. 05).

Logo, considerando que mais de 9 (nove) milhões de brasileiros são conveniados a planos individuais ou familiares de seguradoras, é possível observar que nesta rede há um contínuo tratamento das informações que, ao serem cedidas por estes indivíduos produzem um extenso banco de dados que amplia-se a cada nova contratação (Fragoso, 2020, p. 05).

Assim, no mercado de consumo da saúde suplementar, o tratamento e a integração destes dados pessoais e dados sensíveis do consumidor, devem ser administrados conjuntamente pela ANS como pelas empresas que atuam no setor, sendo eles imprescindíveis, para a elaboração de políticas públicas eficazes para que a prestação de serviço ser adequada e de qualidade. Sendo essas, realizadas com observância das normas inseridas no Código de Defesa do Consumidor inclusive seus princípios, relevando-se ilegal, ofensivos à ordem jurídica, sempre que esses limites discrepam-se, sujeitando ao controle judicial nestas hipóteses (Gregori, 2020, p. 12).

Nesse sentido, a LGPD define que as informações relativas à saúde dos indivíduos são consideradas dados pessoais sensíveis — conforme o artigo 5º, inciso II, LGPD. Este fato, reflete a necessidade de consentimento expresso do titular para que estes dados cedidos sejam tratados de forma específica pelas seguradoras — conforme o artigo 11, inciso I, da LGPD. Vale ressaltar que, a única hipótese de que estas informações sejam utilizadas sem a necessidade de permissão do agente, é quando sua finalidade advém da tutela da saúde para fins públicos, sendo este um rol mais estrito de indivíduos que podem administrá-la, devendo ser realizada por profissionais da saúde, responsáveis pelos serviços de saúde ou outras autoridades sanitárias — conforme o artigo 11, inciso II, alínea "f", LGPD (Fragoso, 2020, p. 05).

Contudo, apesar de ser um meio inovador de administração e manejo tecnológico de informações, a principal preocupação decorre da possibilidade de seu uso inadequado, especialmente,

quanto tem-se à apropriação de registros de saúde dos usuários desses planos visando à obtenção de vantagens econômicas pelas seguradoras, por meio da monetização desses conteúdos em favor da Indústria (Fragoso, 2020, p. 06). Nessa lógica, o tratamento de informações no setor da saúde suscita questionamentos acerca da privacidade e da segurança dos depositários, uma vez que, se tais práticas forem acessíveis apenas àqueles que dispõem de recursos financeiros e tecnológicos, elas podem agravar as desigualdades já existentes no sistema de saúde (Hora, 2023, p. 73).

O chamado *health score* (pontuação da saúde) representa uma estratégia de gerenciamento de clientes utilizada por seguradoras. Baseada na análise dos dados coletados através de aplicativos de saúde, redes sociais e elementos de gamificação, funciona como uma base de dados "propositalmente" cedida pelo usuário, permitindo realizar o seu rastreio e consequentemente sua capitalização. Através do monitoramento das condições de saúde dos usuários, as seguradoras colhem, armazenam e rastreiam esses dados, atribuindo pontuações que acumulam-se e demonstram o grau de risco destes usuários. Isto ocorre pois, ao instalar os aplicativos são aceitos os termos de privacidade sem a ciência de que seu conteúdo e consequentemente informações como corrida, medição arterial, alerta para ingestão de água são fornecidas com auxílio dos próprios aparelhos celulares (Fragoso, 2020, p. 06).

Ocorre que esta prática é proibida, uma vez que expõe grupos vulneráveis à discriminação, impondo comportamento à vida privada do consumidor. Uma vez que coleta as informações relativas à doenças com a coleta dos dados sensíveis, de modo que, para estes consumidores os planos tendem a ficar mais caros. Nesse sentido, uma série de dispositivos legais são violados, inclusive a Constituição Federal, o Código de Defesa do Consumidor, a Lei 9.656/98 e a LGPD (Fragoso, 2020, p. 07).

Assim, a Lei estabelece uma preocupação ética quanto ao tratamento de informações e da própria condição do consumidor que as fornece, assegurando a salvaguarda da privacidade e a proteção dos dados pessoais. Tal fato, mostra-se relevante diante das estratégias de mitigação de riscos implementadas pela Lei, uma vez que para que as operadoras de plano de saúde operem o *health score,* utilizam-se de algoritmos preditivos que estimam o risco da saúde dos consumidores através de uma base de dados pessoais, utilizando-o para discriminar preços que são discrepantes e abusivos para quem contrata os serviços (Fragoso, 2020, p. 07). Assim, desprende-se que as operadoras de planos de saúde não podem tratar dados sobre a saúde com o objetivo de seleção de riscos na contratação de qualquer modalidade e na contratação ou exclusão de consumidores (Gregori, 2020, p. 14).

Nesse aspecto, é possível verificar que a coleta de dados sensíveis para o desenvolvimento de perfis sociais e individuais são capazes de ocasionar práticas discriminatórias, conforme discorre Rodotà (2008, p.12):

> Porém, é fácil objetar que mesmo as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados, agregados, que digam respeito a uma minoria racial ou linguística; ou às consequências de uma decisão política ou econômica tomada justamente com base na análise dos dados anônimos (Rodotà, 2008, p.12).

Desta forma, é evidente a existência de protocolos específicos que padronizam e vinculam estas informações, laudos, exames, doenças, e imagens, visando o seus processamento e categorização, permitindo assim empresas vinculadas à Indústria da Saúde adquiram a selecionem os quesitos de contratação de planos de Saúde abusivos adaptados ao perfil de contratação do usuário. De modo que estes sistemas dialogam com o compartilhamento destas informações sensíveis, uma vez que são facilmente exploradas no sistema de saúde. Assim, ao passo que os consumidores aderem aos sistemas das operadoras de saúde, acabam por fornecer informações sem plena consciência das consequências decorrentes desta exposição. Tornando-se possível vislumbrar a manipulação e o aproveitamento destes dados pelas operadoras (Prux; Piai, 2020, p. 11).

V. Julgamento da ADI 6649 e da ADPF 695 pelo Supremo Tribunal Federal

Ajuizada pelo Partido Socialista Brasileiro (PSB) em 16 de junho de 2020, a Arguição de Descumprimento de Preceito Fundamental nº 695, submeteu ao Supremo Tribunal Federal a análise da constitucionalidade do compartilhamento indiscriminado e massivo de dados pessoais advindo dos registros de carteira de habilitação (CNH). A controvérsia centra-se na compatibilidade dessa prática com os direitos fundamentais à privacidade e à proteção de dados, evidenciando os limites do poder estatal no tratamento de dados sensíveis (Leite; Fonseca, 2024, p. 53). Entre os dados compartilhados estavam informações personalíssimas, como nome, filiação, endereços, telefones, dados dos veículos e fotos dos portadores de Carteira Nacional de Habilitação (CNH) sendo compartilhados pelo Serviço federal de Processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN) com fulcro no Decreto nº 10.046/2019 (Leite; Fonseca, 2024, p. 53).

De acordo com a exordial, o tratamento da ABIN, responsável por planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do país, representava perigo para a intimidade, privacidade, autodeterminação informativa e proteção de dados, vez que não atuava subjugando-se aos princípios da publicidade, finalidade, razoabilidade. Ainda questiona-se o compartilhamento de dados sensíveis e pessoais de milhares de brasileiros entre o SERPRO à ABIN, realizado para fins de inteligência estatal sem respaldo legal (Leite; Fonseca, 2024, p. 53).

Em outra perspectiva, protocolada em 23 de dezembro de 2020 e ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) a Ação Direta de Inconstitucionalidade 6.649 foi proposta em face de determinados dispositivos do Decreto 10.046/2019. Argumentando que tais dispositivos são inconstitucionais, extrapolando os poderes conferidos ao Presidente da República e

violando os direitos fundamentais à dignidade da pessoa humana, intimidade, privacidade, sigilo dos dados, proteção de dados pessoais e autodeterminação informativa (Leite; Fonseca, 2024, p. 54). O maior questionamento da ADI, refere-se ao advento de uma vigilância estatal pois, além da inclusão de dados pessoais que são considerados como básicos, o decreto inclui o compartilhamento de atributos biométricos, definidos como características biológicas, sendo elas: digitais; íris dos olhos; formato de face; voz etc (Leite; Fonseca, 2024, p. 55).

Apesar de temas diferentes, ambas as ações convergem em uma matéria: o Tratamento de Dados Pessoais pela Administração Pública. Nesse aspecto, o relator, Min. Gilmar Mendes, proferiu o voto conjunto à ADI 6.649 e a ADPF. 695, interpretando de forma intermediária os dispositivos, de modo que visando afastar conclusões equivocadas do decreto, confere ao seu art. 3, I, onde discorre sobre a "informações do Estado", concluindo que a admissão de informações está restrita às informações gerais do Estado, excluindo assim os atributos da personalidade ou aqueles inerentes ao cidadão (Leite; Fonseca, 2024, p. 55). Ainda, no mesmo, refere-se que a expressão "compartilhada da forma mais ampla possível, deverá compreender tão somente as informações relativas ao funcionamento do aparelho estatal" (Brasil, 2020), de modo que as informações de cunho pessoal deverão submeter-se ao crivo da LGPD.

O relator ainda reforça que não é justo e, sequer razoável a operação das repartições públicas com aparelhos e instrumentos antigos e desatualizados quando há uma intensa evolução da sociedade moderna. De forma que a renúncia à tecnologia acarreta um aparato estatal obsoleto e arcaico, contribuindo para a ineficiência administrativa (Leite; Fonseca, 2024, p. 57). Assim, o Min. Gilmar Mendes assegura que a necessidade de garantir que essas entidades possuam uma composição plural, democrática e aberta em constante diálogo com a sociedade civil (Leite; Fonseca, 2024, p. 57).

No que condiz a seus desfechos, a Suprema Corte acolheu parcialmente os pedidos da ADI e ADPF, declarando inconstitucional o artigo 22 do Decreto nº 10.046/2019. Além disso, atribuiu interpretação a determinados pontos do regulamento, definindo que o compartilhamento de dados pessoais entre os Entes da Administração Pública deve estar em consonância com o princípio da finalidade (vide art. 6º, inciso I, da LGPD). Estes que devem ser compatíveis com as finalidades apresentadas ao titular, de modo que expressa que a proteção do tratamento de dados não pode ser relativizada, assegurando que o tratamento seja conduzido por meios legítimos e transparentes. Essa orientação revela que o compartilhamento no setor público deve-se vincular ao que determina o artigo 23 da LGPD, publicizando os atos e as práticas utilizadas para a execução das operações de tratamento conforme a Autoridade Nacional de Proteção de Dados (Leite; Fonseca, 2024, p. 58).

Ademais, quanto às atividades de inteligência, essas devem observar a legislação específica que aborda sobre o compartilhamento de informações de cunho pessoal e os requisitos dispostos pelo julgamento da ADI 6.529, sendo eles: adoção de medidas proporcionais e necessárias ao atendimento

do interesse público, a propositura de um procedimento administrativo formal, a utilização de sistemas eletrônicos responsável por registrar todo e qualquer acesso às bases e a observância aos pressupostos da LGPD no que condiz ao meio público (Leite; Fonseca, 2024, p. 59).

Nesse sentido, as conclusões da professora Nohara (2025, p. 916) quanto ao tema:

> O julgamento, ocorrido em setembro de 2022, foi no sentido da possibilidade de compartilhamento, conferindo interpretação conforme o Decreto nº 10.046/2019, desde que observados parâmetros de:
> 1. compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública com: (a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, I, da Lei nº 13.709/2018); (b) compatibilidade do tratamento com as finalidades informadas (art. 6º, II); (c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público;
> 1. rigorosa observância do art. 23, I, da Lei nº 13.709/2018, que determina que seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos"; e
> 2. o acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes supra-arroladas (Nohara, 2025, p. 916).

Ainda, de acordo com o Min. Relator, na evidência de abuso e vazamento de informações pessoais, a responsabilidade civil do Estado é objetiva, visando sanar os danos sofridos pelos titulares, com fulcro nos artigos 42 e seguintes da LGPD, bem como o direito de regresso em face dos servidores e agentes públicos que praticaram o ilícito culposo ou doloso. No sentido de que, sendo uma prática dolosa ao dever de publicidade, a responsabilização ocorrerá mediante ato de improbidade administrativa, conforme artigo 11, inciso IV, da Lei nº 8.429/92 (Leite; Fonseca, 2024, p. 59).

VI. Análise da Ação Civil Pública Nº 5028572-20.2022.4.03.6100

A Ação Civil Pública nº 5028572-20.2022.4.03.6100 trata-se de uma ação movida pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança da Informação em face da União, Caixa Econômica Federal, Dataprev e a Autoridade Nacional de Proteção de Dados (ANPD) visando realizar uma investigação devido a um suposto vazamento massivo de dados de beneficiários do Auxílio Brasil (Figueiredo, 2024, p. 54).

Conforme o Instituto:

> A associação sem fins lucrativos, que trabalha em defesa da proteção de dados pessoais dos titulares de dados, foi informado que em 24/10/2022, houve o vazamento de dados em massa de mais de 4.000.000 (quatro milhões) de titulares de dados, através de correspondentes bancários que foram contratados pelos Réus, os quais tiveram acesso aos dados compartilhados dos Beneficiários do auxílio, tratando-se de

> um programa governamental de renda mínima para pessoas mais pobres (Brasil, 2022).

Considerando a natureza do vazamento, é evidente que os dados foram provenientes das empresas e órgãos públicos aos quais os brasileiros confiam a proteção de seus dados, tornando o caso ainda mais grave. Conforme segue:

> Esses dados violados pairam no registro e no banco de dados de incontáveis instituições, assim como em poder de terceiros que, facilmente, poderão fazer uso maléfico e fraudulento dessas informações, em franco prejuízo material, moral e social desses cidadãos", destacou a procuradora da República Karen Louise Jeanette Kahn (Brasil, 2022).

Desse modo, o Juiz Federal Marco Aurélio de Mello Castrianni, legitimou o ajuizamento da ação, considerando a necessidade de salvaguarda dos dados pessoais desses indivíduos a partir dos seus direitos originários no contexto da LGPD, como se observa:

> O requisito essencial para a legitimidade da associação é o cumprimento do tempo mínimo de criação a pertinência temática entre os objetivos da associação e o bem jurídico tutelado na ACP (AgInt nos EDcl no REsp n. 1.788.290/MS). Ao presente caso, resta evidenciado que os requisitos essenciais da associação autora estão preenchidos. Neste contexto, entendo que restou comprovada a legitimidade da associação autora, mesmo sem a autorização por assembleia, conforme entendimento jurisprudencial pátrio (Brasil, 2022).

O Juiz Federal, julgou parcialmente procedente o pedido, enfatizando os artigos 2º e 42º da referida da LGPD, que referem-se aos deveres de manter a privacidade e a inviolabilidade da intimidade, da honra e da imagem dos indivíduos, os quais são basilares na proteção de dados e resultam na responsabilidade civil do Controlador ou o Operador dos dados pessoais (Figueiredo, 2024, p. 55). Ainda, utilizando os artigos 3º e 22 da lei nº 12.965/14 (Marco Civil da Internet), destacou a necessidade do zelo à privacidade e a proteção de dados pessoais, os quais são princípios intrínsecos do uso da internet no Brasil (Brasil, 2022).

Destarte, com a devida base legal, o magistrado considerou comprovado o vazamento de dados pessoais dos beneficiários do Auxílio Brasil, o que configura violação à LGPD. De modo que, os réus foram considerados responsáveis pelo vazamento, ao passo que é necessário tomar as medidas para reparar os danos causados. Medidas estas, baseadas no fornecimento de registro de conexão e acesso aos dados vazados, disponibilização aos titulares de informação sobre seus dados e como eles foram utilizados, implementação de medidas de segurança para evitar novos vazamentos, comunicação aos titulares sobre o incidente e as medidas adotadas, elaboração de relatórios de impacto à proteção de dados e por fim o pagamento de indenização por danos morais individuais e coletivos no valor de R$ 15.000,00 para cada uma das 4 milhões de vítimas que tiveram os seus dados vazados (Figueiredo, 2024, p. 55).

Vale reforçar que o Juiz Federal Marco Aurélio de Mello Castrianni pontuou a importância da proteção dos dados pessoais e a necessidade de responsabilizar os agentes que violem essa proteção. De modo que, a decisão veio proteger os direitos dos titulares dos dados, garantindo que

sejam informados sobre o vazamento e que tenham seus dados protegidos, além de servir como precedente para casos semelhantes, reforçando a importância da proteção de dados pessoais (Figueiredo, 2024, p. 55).

Desta forma, é evidente que a ação civil fundamenta-se em diversas teorias já abordadas no trabalho. Logo, a responsabilidade civil objetiva mostra-se manifestamente expressa na comprovação do dano e do nexo causal entre a conduta ilícita e o dano, dispensando a culpa, de forma que a responsabilidade civil recai sobre o Controlador ou Operador de dados, tornando-se suficiente para corroborar com a responsabilização direta da União, Caixa Econômica Federal, Dataprev e a Autoridade Nacional de Proteção de Dados, com o vazamento massivo de informações pessoais (Brasil, 2022). Ainda, considerando a Teoria do Risco Administrativo, cabe à Administração Pública o dever de indenizar os danos causados pelos seus serviços, independente de culpa, em razão do risco inerente às suas atividades.

Neste contexto, a Ação Civil Pública supracitada, representa um passo importante para a proteção de dados pessoais no Brasil, uma vez que a decisão demonstra que a LGPD está sendo aplicada e que as empresas que não cumprirem a lei serão responsabilizadas (Figueiredo, 2024, p. 56).

Considerações Finais

Diante de todo o exposto, é possível afirmar que a proteção de dados dos usuários adquiriu relevância fundamental a contar da consolidação de um modelo administrativo marcado pela eficiência tecnológica. Este fato justifica a necessidade de responsabilização das pessoas físicas e jurídicas pela guarda e uso das informações dos usuários. Desta forma, a LGPD institui novas responsabilidades, direitos e deveres de forma que desenvolva-se políticas e normas alinhadas às boas práticas do uso de dados, fundamentada principalmente no princípio da finalidade — de modo que essas informações disponibilizadas não podem ser capitalizadas, fazendo parte de direitos específicos e relativos à personalidade de cada indivíduo.

Nesse sentido, a base conceitual de proteção do usuário no compartilhamento de suas informações pelos Entes da Administração Pública, reside justamente na vinculação do princípio da finalidade com o tratamento de dados pessoais, uma vez que o manejo e proteção destes fundamenta-se na necessidade de consentimento do titular e a partir de sua aprovação que seus dados sejam usados com responsabilidade pelo setor público e privado.

Logo, a consolidação do direito fundamental à proteção de dados pessoais reafirma a necessidade de compatibilizar o uso de tecnologias e a eficiência administrativa com os direitos fundamentais. A comparação entre o modelo asiático de vigilância e a estrutura ocidental de proteção de dados demonstra que a efetividade estatal não pode justificar práticas desproporcionais ou

invasivas. Neste contexto, o princípio da finalidade — art. 6º, I, da Lei nº 13.709/2018, e a proteção constitucional assegurada pela emenda nº 115/2022, constituem guias essenciais para garantir o tratamento e o compartilhamento de dados pela Administração Pública sirvam ao interesse público legítimo, sem comprometer a dignidade e a liberdade dos indivíduos, cabendo ao Estado administrar os dados de forma ética e transparente, que utilize o todo seu potencial tecnológico como instrumento de promoção aos direitos — e não de controle social.

Em vista disso, ao vincular todas as esferas aos princípios administrativos, ou seja, a finalidade específica e clara, estabelece-se uma diretriz que garante a aplicação dos conceitos trazidos pela legislação supracitada. Assim, com o manejo ideal e consciente destas informações, consequentemente a Administração Pública tem capacidade de utilizar estes dados e executar as políticas públicas voltadas à prestação de serviços, ponderando as necessidades dos seus titulares.

Dessa forma, a proteção de dados e a privacidade devem ser consideradas elementos principais da governança digital, legitimando propriamente as instituições públicas. Assim, a partir desta responsabilidade e com o surgimento de prerrogativas de vinculatividade à LGPD, o Estado compromete-se a eventuais riscos das falhas de segurança — como o vazamento de dados ou o descumprimento dos preceitos da lei, devendo indenizar as vítimas independente de culpa, conforme a Teoria do Risco Administrativo. Reforçando a responsabilidade civil da Administração Pública como mantenedora destes dados sensíveis e pessoais. Determinando três agentes responsáveis pelo tratamento de dados: o Controlador, o Operador e por fim o Encarregado.

A pesquisa demonstrou que, embora o avanço tecnológico amplie a capacidade estatal de gestão e formulação de políticas públicas, ele também potencializa os riscos à privacidade e a dignidade dos indivíduos, exigindo um aparato jurídico que garanta a proteção destes dados e a manipulação deles no compartilhamento. Este fato fica muito claro quando analisado no contexto da utilização de informações sensíveis no campo da saúde com o objetivo de manter um *health score* (pontuação da saúde) dos seus usuários. Esta prática segue na contramão de todos os preceitos da lei e ainda pode ser visualizada em grandes companhias de seguradoras como forma de monetização destas informações para ganho próprio.

Nesse sentido, a ADI 6649 e a ADPF 695 reforçam a necessidade de contínua vigilância e aprimoramento das práticas administrativas, explicitando a necessidade de um amparo legal que tenha como fundamento basilar a responsabilização dos entes e o princípio corolário da administração pública -o princípio da finalidade, para que haja o manejo responsável de dados dos sujeitos. Exemplificando a responsabilização que a Administração Pública tem pelos seus atos, a Ação Civil Pública nº 5028572-20.2022.4.03.6100 expressa como vazamento de informações que são de tutela pública devem ser indenizados, sendo esta a consequência da proteção de Dados no Brasil, uma vez

que demonstra que a LGPD está sendo aplicada e que as empresas que não cumprirem a lei serão responsabilizadas a medida da necessidade e do prejuízo que este causa.

Conclui-se, portanto, que o equilíbrio entre a eficiência administrativa e a tutela dos direitos fundamentais depende da consolidação de uma governança de dados responsável, que reconheça o cidadão não como mero objeto de tratamento informacional, mas como sujeito de direitos. Assim, o compartilhamento de dados atuará como uma forma de aprimoramento dos processos de gestão e qualidade de dados, garantindo a eficiência do serviço público, bem como o resguardo da confiabilidade dos indivíduos.

Referências bibliográficas

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo: Tratamento de dados pessoais pelo Poder Público**. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-depublicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 24 ago. 2025.

ARAUJO, João Victor Clemente de. **Compartilhamento de dados no âmbito da Administração Pública**: as consequências jurídicas e benefícios para o cidadão. Goiânia, Pontifícia Universidade Católica (PUC) de Goiás, Escola de Direito e Relações Internacionais - Núcleo de Prática Jurídica. Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1559. Acesso em: 26 ago. 2025.

BORGES DE CARVALHO, L. Governo digital e direito administrativo: entre a burocracia, a confiança e a inovação. **Revista de Direito Administrativo**, *[S. l.]*, v. 279, n. 3, p. 115–148, 2020. DOI: 10.12660/rda.v279.2020.82959. Disponível em: https://periodicos.fgv.br/rda/article/view/82959. Acesso em: 26 ago. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6649**. Direito constitucional. Direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade. Tratamento de dados pessoais pelo Estado brasileiro. Compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal. ADI e ADPF conhecidas e, no mérito, julgadas parcialmente procedentes. interpretação conforme à constituição. Declaração de inconstitucionalidade com efeitos futuros. Relator: Ministro Gilmar Mendes. Julgado em 15 de setembro de 2022. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206649%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 10 abr. 2025.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695**. Direito Constitucional. Direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade. Tratamento de dados pessoais pelo Estado brasileiro. Compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal. ADI e ADPF conhecidas e, no mérito, julgadas parcialmente procedentes. Interpretação conforme à constituição. Declaração de inconstitucionalidade com efeitos futuros. Relator: Ministro Gilmar Mendes. Julgado em 15 de setembro de 2022. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADPF%20695%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 10 abr. 2025.

BRASIL, Tribunal de Contas da União. **Auditoria**. Diagnóstico do grau de implementação da Lei Geral de Proteção de Dados na Administração Pública federal. TCU, Brasil, 2022. Disponível em: https://capitaldigital.com.br/wp-content/uploads/2022/06/038.172-2019-4-AN-auditoria_Lei-Geral-de-Protecao-de-Dados.pdf. Acesso em : 02 out. 2025.

BUCCI, Maria Paula Dallari et alli. Direitos humanos e políticas públicas. São Paulo, Pólis, 2001. 60p. (Cadernos Pólis, 2). Disponível em: <https://www.polis.org.br/uploads/831/831.pdf>. Acesso em: 12 fev. 2020.
BUCCI, Maria Paula Dallari. O conceito de política pública em direito. In: BUCCI, Maria Paula Dallari (org.). Políticas públicas: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006.
CARVALHO, Igor de Castro. **LGPD e Poder Público: a necessidade de profissionais DPO na Administração Pública**. 2023. 28 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2023. Disponível em: https://repositorio.ufu.br/bitstream/123456789/37798/1/LGPDPoderP%C3%BAblico.pdf. Acesso em: 26 ago. 2025.
CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 39. ed. Rio de Janeiro: Atlas, 2025.
COELHO, Fábio Ulhôa. **Curso de direito civil**: obrigações/responsabilidade civil. 5ª ed., São Paulo: Saraiva, 2012
HORA, Nina da. Privacidade, ética e transparência de dados na saúde. In: SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedroza (org.). **Lei Geral de Proteção de Dados e o controle social da saúde.** Porto Alegre: Editora Rede Unida, 2023. p. 69–76.
DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.
FIGUEIREDO, Davi Quaresma Vale Pinheiro. **Proteção de dados pessoais no contexto da administração pública**: a responsabilidade civil da administração pública no tratamento de dados. 2024. 66 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário UNDB, São Luís. Disponível em: http://repositorio.undb.edu.br/jspui/handle/areas/1301. Acesso em: 26 ago. 2025.
FRAGOSO, Fernanda Rocha. **Lei Geral de Proteção de Dados e o Health Score**. Revista Governança e Compliance, [s.l.], mar. 2020. Disponível em: https://www.academia.edu/42867608/LGPD_E_HEALTH_SCORE. Acesso em: 5 out. 2025.
GAETANI, Francisco; LAGO, Miguel. **A construção de um estado para o século XXI**. 1. ed. Rio de Janeiro: Cobogó, 2022.
GREGORI, Maria Stella. **Os impactos da Lei Geral de Proteção de Dados Pessoais na saúde suplementar.** *Revista de Direito do Consumidor*, São Paulo, v. 127, p. 171–196, jan./fev. 2020. Disponível em: https://dtr.stj.jus.br/DTR/handler.ashx?dtr=2019\42758. Acesso em: 5 out. 2025.
HAN, Byung-Chul. **O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han**. El País Brasil, São Paulo, 22 mar. 2020a. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html. Acesso em: 3 out. 2025.
HAN, Byung-Chul. **Por que a Ásia está melhor que a Europa na pandemia? O segredo está no civismo**. El País Brasil, São Paulo, 30 out. 2020b. Disponível em: https://brasil.elpais.com/internacional/2020-10-30/por-que-a-asia-esta-melhor-que-a-europa-na-pandemia-o-segredo-esta-no-civismo.html. Acesso em: 3 out. 2025.
LEITE, Carolina Quarantini; FONSECA, Alexandre Barreiros de Carvalho. Compartilhamento de dados pessoais sensíveis entre os órgãos da administração pública: uma análise do Decreto nº 10.046/2019 à luz da relatoria da ADPF 695 e ADI 6649/DF. **Revista Conversas Civilísticas**, v. 4, n. 1, p. 39-67. DOI: 10.9771/rcc.v4i0.60763. Salvador, 2024. Disponível em: https://revbaianaenferm.ufba.br/index.php/conversascivilisticas/article/view/60763. Acesso em: 26 ago. 2025.
MARQUES, Jhony Wesley. **Análise do nível de aderência à LGPD no setor público**. 2022. Trabalho de Conclusão de Curso (Tecnologia em Sistemas para Internet) - Universidade Tecnológica Federal do Paraná, Toledo, 2022.
MEIRELLES, Hely Lopes. **Direito Administrativo brasileiro**. 44. ed. São Paulo: Malheiros, 2020.
MORAES, Alexandre de. **Direito Constitucional**. 41. ed. Rio de Janeiro: Atlas, 2025.
NOHARA, Irene Patrícia D. **Direito administrativo**. 14. ed. Rio de Janeiro: Atlas, 2025.

PIETRO, Maria Sylvia Zanella D. **Direito Administrativo**. 38. ed. Rio de Janeiro: Forense, 2025.
PINHEIRO, Patricia P. **Direito Digital**. 7. ed. Rio de Janeiro: Saraiva Jur, 2021.
_____, **Proteção de Dados Pessoais**: Comentários à Lei nº 13.709/2018 LGPD). 4. ed. Rio de Janeiro: Saraiva Jur, 2023.
PINHEIRO, Patricia P.; LOTUFO, Larissa. Proteção de dados pessoais. In: PINHEIRO, Patrícia P. (coord.). **Segurança digital**: proteção de dados nas empresas. São Paulo: Atlas, 2021. p. 31-38.
PRUX, Oscar Ivan; PIAI, Kevin de Sousa. **Discriminação algorítmica e a tutela aos dados pessoais no ambiente corporativo: uma análise da saúde ao emprego.** Maringá, Centro Universitário de Maringá (UniCesumar), Revista Argumentum, v. 21, n. 3, set./dez. 2020. Disponível em: https://ojs.unimar.br/index.php/revistaargumentum/article/view/1331. Acesso em: 4 out. 2025.
RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Maria Celina Bodin de (org.). Rio de Janeiro: Renovar, 2008.
SACCARO JUNIOR, Nilo Luiz; ROCHA, Wilsimara Maciel; MATION, Lucas Ferreira (org.). **CMAP 2016 a 2018**: estudos e propostas do Comitê de Monitoramento e Avaliação de Políticas Públicas Federais. Brasília, DF: Ipea. 2018. Disponível em: http://repositorio.ipea.gov.br/handle/11058/8796. Acesso em: 26 ago. 2025.
SARLET, Ingo W.; MARINONI, Luiz G.; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 14. ed. Rio de Janeiro: Saraiva Jur, 2025.
SILVA, Maycon Neves da; FERREIRA, Mauro Monteiro. Compartilhamento de dados pelo poder público: um caminho para a transparência e melhoria dos serviços. **Revista DCS**, *[S. l.]*, v. 22, n. 79, 2025. DOI: 10.54899/dcs.v22i79.105. Disponível em: https://ojs.revistadcs.com/index.php/revista/article/view/105. Acesso em: 26 ago. 2025.
TEPEDINO, Gustavo. Prefácio à 1ª edição. In: DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 13-14.
VUORI, Natália Brezolin. **Compartilhamento de dados pessoais no poder público**. Dissertação (Mestrado – Programa de Mestrado Profissional em Governança e Desenvolvimento). Brasília: Enap (Escola Nacional de Administração Pública), 2024. Disponível em: http://repositorio.enap.gov.br/handle/1/8341. Acesso em: 26 ago. 2025.