CENTRO UNIVERSITÁRIO
UNIDADE DE ENSINO SUPERIOR DOM BOSCO – UNDB
CURSO DE DIREITO

CATARINE ROBERTA MUNIZ DE ARAÚJO

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: um estudo do caso do metrô de São Paulo

São Luís
2024

CATARINE ROBERTA MUNIZ DE ARAÚJO

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: um estudo do caso do metrô de São Paulo

Monografia apresentada ao Curso de Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profa. Ma. Manuela Ithamar Lima.

São Luís

2024

Dados Internacionais de Catalogação na Publicação (CIP)
Centro Universitário – UNDB / Biblioteca

Araújo, Catarine Roberta Muniz de

A proteção de dados pessoais na administração pública: um estudo do caso do metrô de São Paulo. / Catarine Roberta Muniz de Araújo. ___São Luís, 2024.
54 f.

Orientador: Profa. Manuela Ithamar Lima.
Monografia (Graduação em Direito) - Curso de Direito – Centro Universitário Unidade de Ensino Superior Dom Bosco – UNDB, 2024.
1. Proteção de dados pessoais. 2. Tratamento de dados. 3. Direito administrativo. 4. Administração pública. 5. Lei Geral de Proteção de Dados Pessoais (LGPD). I. Título

CDU 342.9:004

CATARINE ROBERTA MUNIZ DE ARAÚJO

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: um estudo de caso do metrô de São Paulo

Monografia apresentada ao Curso de Direito do Centro Universitário Unidade de Ensino Superior Dom Bosco como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovada em:19/06/2024.

BANCA EXAMINADORA:

Profa. Ma. Manuela Ithamar Lima (Orientadora)

Centro Universitário

Unidade de Ensino Superior Dom Bosco – UNDB

Profa. Ma. Gláucia Maria Maranhão Pinto Lima

Centro Universitário

Unidade de Ensino Superior Dom Bosco – UNDB

Prof. Me. Igor Martins Coelho Almeida

Centro Universitário

Unidade de Ensino Superior Dom Bosco – UNDB

AGRADECIMENTOS

Agradeço à minha mãe, Ana Cristina e ao meu pai José Augusto, que muito me apoiaram ao longo da vida; aos meus irmãos, Roberto e Paulo Sérgio, pelo eterno vínculo fraternal; à minha avó, Conceição, de alma cândida e bondosa; com quem compartilho momentos incríveis.

Agradeço também à passagem de tempo até aqui; aos que comigo caminharam ou caminham em matéria ou em ideia; ao que já fui, ao que sou, ao que serei.

Obrigada.

“Só tem convicções aquele que nada aprofundou”.

Emil Cioran

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, Lei nº 13.709/2018, estabelece normas rigorosas para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando proteger os direitos fundamentais de liberdade e privacidade dos indivíduos. A administração pública, ao fornecer serviços à população, deve garantir que o tratamento dos dados pessoais dos cidadãos seja realizado em conformidade com as diretrizes estabelecidas pela LGPD. A implementação da LGPD na administração pública exige a adoção de medidas técnicas e administrativas adequadas para assegurar a proteção dos dados pessoais. Isso inclui a necessidade de nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto à proteção de dados, a criação de políticas de privacidade transparentes e a implementação de mecanismos de segurança da informação. Além disso, é imperativo que os dados pessoais sejam tratados apenas para finalidades legítimas, específicas, explícitas e informadas aos titulares, minimizando ao máximo a coleta e o processamento excessivo de informações. A LGPD também enfatiza a importância do consentimento do titular dos dados, exceto em situações onde o tratamento é necessário para cumprir obrigações legais, executar políticas públicas ou proteger a vida e a integridade física dos cidadãos. Deste modo, a administração pública deve equilibrar a necessidade de eficiência na prestação dos serviços públicos com a obrigação de proteger a privacidade dos indivíduos, adotando práticas de governança de dados que promovam a transparência e a confiança da sociedade. Portanto, o desafio que se coloca é: de que modo é concedido o tratamento de dados pessoais pela administração pública quando do fornecimento de um serviço público à luz da LGPD?

Palavras-chave: Proteção de dados pessoais. Tratamento de dados. Direito Administrativo. Administração Pública. LGPD.

ABSTRACT

Brazil's General Personal Data Protection Law (LGPD), Law No. 13,709/2018, establishes strict standards for the collection, storage, processing and sharing of personal data, aiming to protect individuals' fundamental rights to freedom and privacy. The public administration, when providing services to the population, must ensure that the processing of citizens' personal data is carried out in accordance with the guidelines established by the LGPD. The implementation of the LGPD in public administration requires the adoption of appropriate technical and administrative measures to ensure the protection of personal data. This includes the need to appoint a data protection officer, carry out data protection impact assessments, create transparent privacy policies and implement information security mechanisms. Furthermore, it is imperative that personal data is only processed for legitimate, specific, explicit and informed purposes to the holders, minimizing the collection and excessive processing of information as much as possible. The LGPD also emphasizes the importance of the data subject's consent, except in situations where processing is necessary to comply with legal obligations, execute public policies or protect the lives and physical integrity of citizens. Therefore, public administration must balance the need for efficiency in the provision of public services with the obligation to protect the privacy of individuals, adopting data governance practices that promote transparency and trust in society. Therefore, the challenge that arises is: how is the processing of personal data granted by the public administration when providing a public service in light of the LGPD?

Keywords: Protection of personal data. Data processing. Administrative law. Public administration. GDPR.

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CCPA	California Consumer Privacy Act
CDC	Código de Defesa do Consumidor
CGI.br	Comitê Gestor da Internet no Brasil
CJF	Conselho da Justiça Federal
CRFB	Constituição da República Federativa do Brasil de 1988
DPA	Data Protection Authority
DPO	Data Protection Officer
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EUA	Estados Unidos da América
IBGE	Instituto Brasileiro de Geografia e Estatística
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LINDB	Lei de Introdução às Normas do Direito Brasileiro
MCI	Marco Civil da Internet
MPV	Medida Provisória
NSA	National Security Agency
PEC	Proposta de Emenda à Constituição
PL	Projeto de Lei
PLC	Projeto de Lei da Câmara
PLS	Projeto de Lei do Senado
RGPD	Regulamento Geral sobre a Proteção de Dados
STF	Supremo Tribunal Federal
TICs	Tecnologias da Informação e Comunicação
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A era da informação trouxe uma revolução na maneira como a administração pública coleta, processa e utiliza dados pessoais. Com a digitalização crescente e a implementação de tecnologias avançadas para o tratamento de dados, a gestão pública tornou-se profundamente dependente dessas informações para a prestação eficiente de serviços públicos. No entanto, essa transformação também levantou preocupações significativas sobre a privacidade e a proteção dos dados dos cidadãos.

No Brasil, a Constituição Federal de 1988 já assegurava direitos fundamentais como liberdade, intimidade, vida privada e acesso à informação (Brasil, 1988). Contudo, o reconhecimento explícito do direito à proteção de dados pessoais apenas foi consolidado com a Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018. A LGPD veio preencher uma lacuna crucial no ordenamento jurídico brasileiro, estabelecendo normas claras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando proteger os direitos dos indivíduos em um ambiente cada vez mais digitalizado (Brasil, 2018).

A implementação da LGPD na administração pública exige uma série de medidas técnicas e administrativas para assegurar a proteção dos dados pessoais. Essas medidas incluem a nomeação de um encarregado de proteção de dados, a realização de avaliações de impacto à proteção de dados, a criação de políticas de privacidade transparentes e a adoção de mecanismos robustos de segurança da informação. Além disso, a administração pública deve garantir que os dados pessoais sejam tratados exclusivamente para finalidades legítimas, específicas e explícitas, informadas previamente aos titulares dos dados.

Um aspecto central da LGPD é o consentimento dos titulares dos dados, que deve ser obtido, exceto em situações onde o tratamento dos dados é necessário para cumprir obrigações legais, executar políticas públicas ou proteger a vida e a integridade física dos indivíduos. Assim, a administração pública enfrenta o desafio de equilibrar a eficiência na prestação de serviços com a obrigação de proteger a privacidade dos cidadãos.

Diante deste cenário, o presente estudo busca responder à seguinte questão: de que modo deve ser concedido o tratamento de dados pessoais pela administração pública quando do fornecimento de um serviço público à luz da LGPD? A resposta a essa pergunta é fundamental para garantir que a administração pública atue de maneira transparente, ética e em conformidade com a legislação vigente, promovendo a confiança dos cidadãos nas instituições públicas enquanto protege seus direitos fundamentais.

O estudo, de natureza qualitativa, bibliográfica e documental, utiliza a metodologia dedutiva para explorar a aplicação da LGPD na Administração Pública, com foco no equilíbrio

entre transparência e proteção de dados. Em conclusão, a pesquisa analisa como a LGPD se aplica à Administração Pública, destacando a necessidade de balancear o dever de transparência com o direito à proteção de dados, especialmente em contratações públicas e decisões automatizadas.

2 DIREITO À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

No Brasil, embora a Constituição Federal de 1988 garantisse direitos fundamentais como a liberdade, a intimidade, a privacidade, a honra e a imagem, a transparência da Administração e o acesso à informação, e a confidencialidade nas comunicações de dados, não havia uma garantia explícita de proteção de dados pessoais, especialmente na era digital (Brasil, 1988).

A Constituição, ao tratar da inviolabilidade da correspondência e das comunicações, não considerava especificamente os riscos do tratamento informatizado de dados pessoais. Doneda (2011) critica essa lacuna, apontando que o sistema não contemplava adequadamente as ameaças do processamento de informações pessoais. Essa ambiguidade levou a interpretações limitadas sobre a proteção de dados, como visto no julgamento do MS n.º 21.729/DF e do RE n.º 418.416-8/SC pelo STF, que entendia a proteção apenas para dados em transmissão, e não para dados armazenados. No MS n.º 21.729/DF, o Ministro Sepúlveda Pertence afirmou que a proteção no inciso XII do artigo 5º da Constituição se aplica apenas à comunicação de dados, e não aos dados em si (Brasil, 1995).

Reconhecendo a necessidade de uma legislação mais alinhada com a realidade da sociedade da informação do século XXI, surgiu a necessidade de uma lei que interpretasse os incisos X e XII do artigo 5º de maneira a abranger dados estáticos e móveis, informação e privacidade. Essa lacuna foi parcialmente preenchida pela promulgação da Lei Geral de Proteção de Dados (LGPD) e a inclusão do direito à proteção de dados pessoais como direito fundamental pela Emenda Constitucional nº 115, de 2022 (Brasil, 2018; Brasil, 2022).

A Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022, alterou a Constituição Federal para incluir a proteção de dados pessoais, inclusive nos meios digitais, como um direito fundamental. Essa emenda inseriu o inciso LXXIX ao artigo 5º, estabelecendo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Além disso, a emenda modificou o artigo 21, incluindo a competência da União para organizar e fiscalizar a proteção e o tratamento de dados pessoais (Brasil, 2022).

Dessa forma, a interpretação do direito à proteção de dados pessoais pela Suprema Corte brasileira começou a evoluir significativamente até 2020, adaptando-se melhor às exigências da era digital e reforçando a importância da proteção de dados no país.

2.1 Proteção de dados pessoais como Direito Fundamental no ordenamento jurídico brasileiro

A proteção de dados pessoais no Brasil evoluiu significativamente nos últimos anos, culminando na consolidação deste direito como fundamental no ordenamento jurídico brasileiro. A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, representa um marco regulatório importante, estabelecendo diretrizes claras sobre o tratamento de dados pessoais e assegurando a privacidade dos indivíduos (Brasil, 2018).

O artigo 5º, inciso X, da Constituição Federal de 1988 já protegia a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, prevendo que o direito à indenização pelo dano material ou moral decorrente de sua violação é garantido. No entanto, foi com a promulgação da LGPD que se concretizou uma proteção mais específica e abrangente aos dados pessoais. Segundo o artigo 1º da LGPD, "esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Brasil, 2018).

A importância da LGPD como um instrumento de proteção de direitos fundamentais é amplamente reconhecida. Como destaca o professor Danilo Doneda (2020, p. 34):

> A LGPD não apenas regulamenta o tratamento de dados pessoais, mas também se integra ao conjunto de normas constitucionais e infraconstitucionais que protegem os direitos fundamentais, reforçando a ideia de que a proteção de dados pessoais é uma extensão do direito à privacidade.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela mesma lei, desempenha um papel crucial na fiscalização e regulamentação do cumprimento da LGPD, garantindo que os direitos dos titulares dos dados sejam respeitados. Segundo a ANPD, "a proteção de dados pessoais é fundamental para assegurar a dignidade e o respeito aos direitos fundamentais das pessoas, fortalecendo a confiança nas relações entre indivíduos e instituições" (ANPD, 2021, p. 55).

A jurisprudência brasileira também tem avançado no reconhecimento da proteção de dados pessoais como um direito fundamental. Em uma decisão emblemática, o Supremo Tribunal Federal (STF) destacou que a proteção de dados pessoais deve ser entendida como uma extensão do direito à privacidade e da autodeterminação informativa, essenciais para a preservação da dignidade humana (Brasil, 2021).

A proteção de dados pessoais no Brasil não é apenas uma questão de regulamentação, mas uma afirmação de princípios fundamentais que garantem a liberdade e a privacidade dos indivíduos. A Lei Geral de Proteção de Dados (LGPD), juntamente com a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e o reconhecimento jurisprudencial, consolida este direito como essencial para o desenvolvimento democrático e a proteção da dignidade humana (Brasil, 2018).

A proteção de dados pessoais no ordenamento jurídico brasileiro reflete um compromisso robusto com a salvaguarda dos direitos fundamentais. Este avanço normativo e institucional é crucial para assegurar que os cidadãos possam exercer plenamente seus direitos em um ambiente cada vez mais digital e interconectado. A trajetória de reconhecimento e consolidação desse direito reflete a evolução do conceito de privacidade até a proteção de dados pessoais (Doneda, 2011).

A Constituição Federal de 1988 do Brasil foi um marco importante para a proteção da privacidade. Ela estabeleceu, no artigo 5º, incisos X e XII, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo das comunicações. Esses dispositivos garantem que os cidadãos tenham o direito de manter suas informações pessoais protegidas contra interferências e divulgação não autorizada (Brasil, 1988).

Com o avanço da tecnologia e a digitalização das informações, a privacidade ganhou novas dimensões. A coleta, armazenamento e processamento de dados pessoais por empresas e governos se intensificaram, aumentando os riscos de abusos e violações. Surgiu, então, a necessidade de uma legislação específica para proteger os dados pessoais dos cidadãos. A Lei n.º 13.709 foi promulgada em 14 de agosto de 2018, com o objetivo de proteger os dados da pessoa física, fundamentada nos direitos fundamentais como o respeito à liberdade de expressão, à privacidade, à inviolabilidade da intimidade, à honra e à imagem, princípios fundamentais da República Federativa do Brasil (Brasil, 2018).

Se no artigo 1º da LGPD[1] restava evidente o intuito "de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (Brasil, 2018), mesmo assim, não havia nenhuma decisão concreta da Suprema

[1] O artigo 1º da LGPD teve início de vigência e de vigor somente em 18 de setembro de 2018, quando da sanção e publicação da Lei n.º 14.058, de 17 de setembro de 2020, que adveio da Medida Provisória (MPV) n.º 959, de 29 de abril de 2020. Em 26 de agosto de 2020, em votação referente à conversão da MPV n.º 959 na Lei n.º 14.058/2018, o Congresso Nacional removeu o artigo o artigo 4º da Medida Provisória, que, alterando a redação do artigo 65, inciso II da LGPD, prescrevia vacatio legis até 3 de maio de 2021 para os artigos 1 a 51 e 60 a 65 desta lei (Brasil, 2020b; Dezan, 2020).

Corte do Canadá a respeito de um direito fundamental à proteção dos dados pessoais do indivíduo momento de sua promulgação (Brasil, 2018).

Em 7 de maio de 2020, ao deliberar em plenário as Ações Diretas de Inconstitucionalidade (ADIs) n.º 6387, 6388, 6389, 6390 e 6393, o Supremo Tribunal Federal, na relatoria da Ministra Rosa Weber, paralisou a aplicação da Medida Provisória n.º 954, de 17 abril de 2020, que suscitava o compartilhamento "de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado [STFC] e de Serviço Móvel Pessoal [SMP] com a Fundação Instituto Brasileiro de Geografia e Estatística [IBGE]", com o propósito de "suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei n.º 13.979, de 6 de fevereiro de 2020" (Brasil, 2020). Na resolução, o STF, por maioria, referendando a cautelar concedida pela Ministra Rosa Weber, e tendo como voto vencido apenas o Ministro Marco Aurélio, estabeleceu o entendimento de que existe um direito fundamental à proteção de dados que pode ser exigido tanto dos agentes privados quanto da administração pública direta e indireta, consequente de interpretação sistemática do artigo 5º, caput, e incisos X e XII da Constituição Federal de 1988, garantidor da privacidade, da liberdade individual e do livre desenvolvimento da personalidade (Brasil, 2020).

Em suma, basearam a decisão: (i) respeito à privacidade informacional e autonomia como resultado do direito da personalidade, positivados nos incisos I e II do artigo 2º da LGPD como fundamento para a proteção de dados pessoais no momento da decisão, mesmo que a lei ainda não tivesse sido aprovada e vigente; (ii) para garantir que os direitos não sejam violados, o tratamento de dados de pessoas naturalmente identificáveis deve aderir às proteções fundamentais garantidas pelo direito individual à privacidade (CRFB, artigo 5º, caput), da privacidade e do livre desenvolvimento da personalidade (CRFB, artigo 5º, incisos X e XII), de modo que '[o] compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados' (Brasil, 2020); (iii) limites impostos pelo Regulamento Sanitário Internacional (RSI 2005) relativos à utilização e partilha de dados pessoais para fins de saúde pública, que não podem ser excessivos em relação à finalidade nem conservados por tempo injustificadamente longo (artigo 45, § 2º, alíneas 'b' e 'd'); (iv) inadequação e impropriedade da norma promanada da MPV n.º 954/2020, compartilhando informações de identificação pessoal sobre usuários de serviços telefônicos com a administração indireta de interesse público legal (no caso, a fundação pública do IBGE); (v) a MPV n.º 954/2020, sem especificar como e com que finalidade o IBGE utilizaria dados coletados, impossibilita sua auditabilidade e avaliação de sua adequação e

necessidade, desrespeitando os princípios subjacentes ao processo legal em seu aspecto substantivo (CRFB, artigo 5º, inciso LIV); (vi) a MPV n.º 954/2020 desrespeitando os requisitos impostos por direitos por falta de mecanismo técnico ou administrativo '[...] apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados' (Brasil, 2020); (vii) ainda que dispusesse no caput do artigo 4º que a Fundação IBGE retiraria os dados compartilhados de suas bases de dados assim que descobrisse uma emergência de saúde pública relacionada ao coronavírus, a MPV n.º 954/2020, ao prever no parágrafo único a possibilidade de retenção dos dados por 30 (trinta) dias para fins de produção de estatística oficial, excedeu a finalidade do compartilhamento declarada; (viii) a vigência da MPV n.º 954/2020 durante a vacatio legis da LGPD poderia causar potenciais danos aos titulares dos dados (mais de cem milhões de usuários de telefonia móvel).

Foram paradigmáticos os votos da relatora, Ministra Rosa Weber, e dos Ministros Luiz Fux e Gilmar Mendes. A Ministra, mencionando os direitos fundamentais à liberdade individual (CRFB, artigo 5º, caput), à privacidade e ao livre desenvolvimento da personalidade (CRFB, artigo 5º, incisos X e XII), e apontando que "as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade", estabeleceu firmemente a existência de um direito fundamental à proteção de informações sobre indivíduos naturalmente identificáveis ou contatáveis (Brasil, 2020).

O Ministro Luiz Fux, afirmando expressamente o paradigmático caso do Tribunal Constitucional Alemão que, ao julgar a Lei do Censo, em 1983, fruto da constatação axiomática de que não existiriam dados irrelevantes na era digital, a autonomia informacional tornou-se um pilar da proteção de dados pessoais, o artigo 8º da Carta de Direitos Fundamentais da União Europeia que declara que todos têm direito à proteção dos dados pessoais que lhes digam respeito, o RSI da OMS e a LGPD, votou pela suspensão da eficácia da Medida Provisória n.º 954/2020, por violação aos "direitos fundamentais à proteção de dados e à autodeterminação informativa", que, de acordo com o Ministro, derivam "da garantia da inviolabilidade da intimidade e vida privada (CRFB, art. 5º, X), do princípio [fundamental] da dignidade da pessoa humana (CRFB, art. 1°, III) e da garantia processual do habeas data (CRFB, art. 5º, LXXII)" (Brasil, 2020).

O Ministro Gilmar Mendes falou sobre a necessidade de uma abertura permanente da Constituição aos avanços e revoluções tecnológicas, a fim de manter a Força Normativa da Constituição Federal de 1988. Em uma histórica retrospectiva, ele discutiu o trabalho pioneiro

de Warren e Brandeis sobre o direito à privacidade, bem como a posição formalista e negacionista de Tércio Sampaio Ferraz Junior sobre tal direito. “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”, de 1993, adotada pelo STF anteriormente, conforme MS n.º 21.729/DF e RE 418.416-8/SC, e a paradigmática jurisprudência firmada em 1983 pelo Tribunal Constitucional alemão, que proclamou o direito de autodeterminação do conhecimento. Por fim, afirmou a existência de um direito fundamental independente à proteção de dados pessoais como consequência da dignidade da pessoa humana, da proteção constitucional da privacidade e da reativação do habeas data (Brasil, 2020).

Esse direito fundamental, segundo o ministro, tem duas dimensões: a subjetiva, que costuma acompanhar o direito à autodeterminação dos dados cadastrais, cuja supressão requer justificativa do legislador (e do representante), que deve ser definida de forma explícita e precisa para limitar o tratamento "com suficiente precisão, precisão e clareza a cada área" que culmine em uma proibição, os princípios de importância e transparência; e a proteção objetiva e ativa do sujeito titular registrado, que impõe ao legislador o dever de proteger o direito de autodeterminação que transmite a informação. “normas de organização e procedimento [...] e [de] normas de proteção [...]”, cuja base de avaliação é consenso, conforme previsão do artigo 8.º da Carta de Direitos Fundamentais da União Europeia (Brasil, 2020).

À semelhança desse julgamento paradigmático, o Supremo Tribunal Federal confirmou a existência de um direito fundamental independente à proteção de dados pessoais na Constituição Federal de 1988 que pode ser usado contra atores privados ou públicos.

Por fim, não se pode deixar de mencionar a existência da PEC nº 17, de 2019, proposta e aprovada pelo Senado Federal e atualmente em tramitação na Câmara dos Deputados, que visa consagrar expressamente na Constituição Federal o direito à proteção dos dados físicos e digitais de pessoa natural identificada ou identificável, acrescentando o inciso XII-A ao artigo 5º, afirmando ainda a competência exclusiva da União para legislar sobre esta matéria, por meio de acréscimo do inciso XXX no artigo 22.

2.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

Em 14 de agosto de 2018, foi promulgada a Lei n.º 13.709, dispondo sobre o tratamento de dados pessoais, “[...] inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Brasil, 2018).

Apesar do significativo impacto do RGPD na LGPD, especialmente com a adoção do princípio do consentimento como núcleo substantivo deste texto, tal lei é fruto de um forte processo democrático e legislativo de proteção de dados pessoais, que se estima ter sido nascido em 2010.

Em 2010, iniciou-se um debate público sobre o direito à privacidade e proteção de dados pessoais. Nomeadamente, tal interlocução democrática deu-se tanto no "I Seminário de Proteção à Privacidade aos Dados Pessoais" realizado pelo Comitê Gestor da Internet no Brasil - CGI.br quanto pela promoção de pioneira consulta pública, pelo Ministério da Justiça, atinente a anteprojeto de lei relativa ao tema, a qual foi objeto de mais de 2.500 contribuições.

Como corolário do crescente e diálogo democrático acerca da matéria e da cada vez mais urgente necessidade de sua normatização, foi apresentado na Câmara dos Deputados, em 13 de junho de 2012, pelo então Deputado Federal Milton Monti, do PR, o Projeto de Lei n.º 4.060, que tinha por objetivo: "[...] garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem" (Brasil, 2012).

Pouco mais de um ano depois, em 13 de agosto 2013, foi apresentado no Senado Federal, pelo então Senador Antônio Carlos Valadares, do PSB, o Projeto de Lei do Senado n.º 330, que, similarmente, dispunha principalmente "sobre a proteção, o tratamento e o uso dos dados pessoais [...]" (Brasil, 2013).

No ano de 2016, especificamente no dia 13 de maio, a então Presidenta Dilma Rousseff apresentou à Câmara dos Deputados o Projeto de Lei nº 5.276, de 2016, resultado de consulta pública para a qual contribuíram mais de 40 instituições nacionais e internacionais.

Em resposta à recente revelação do escândalo de manipulação de dados do Facebook - Cambridge Analytica em março de 2018 e a plena implementação do RGPD em 25 de maio de 2018, o PL nº 4.060/2012 foi aprovado com urgência no Senado e enviado ao legislativo federal como Projeto de Lei do Senado nº 53 de 2018. Ricardo Ferraço foi relator do projeto.

O PLC nº 53/2018 foi aprovado com alterações em 10 de julho de 2018, e foi encaminhado para sanção, que culminou na promulgação da Lei nº 13.709 em 14 de agosto de 2018.

A primeira disposição para os efeitos da lei era que ela começaria a vigorar após 18 (dezoito) meses de sua publicação oficial. Não obstante, em 27 de dezembro de 2018, o então Presidente Michel Temer editou a MPV n.º 869, que, alterando a redação original do artigo 65 da Lei n.º 13.709/2018, fixou, no inciso I, o dia 28 de dezembro de 2018 como termo inicial de

vigência dos artigos 55-A a 58-B e, no inciso II, 24 (vinte e quatro) meses a partir da data de publicação da lei para outros artigos. Essa previsão permaneceu com a conversão da MPV na Lei n.º 13.853, de 8 de julho de 2019.

Em 29 de abril de 2020, o Presidente da República publicou a MPV nº 959, alterando a redação do artigo 65, inciso II, da LGPD e, assim, adiando a vigência dos artigos não mencionados neste inciso, que não os previstos no inciso I, para 3 de maio de 2021.

Por fim, em 18 de setembro de 2020, entrou em vigor a Lei Geral de Proteção de Dados Pessoais - com exceção dos artigos 52, 53 e 54 - conforme a Lei nº 13.709/2018 e a Medida Provisória nº 959/2020, que prorrogou a vigência dos artigos 1º a 51º e 55º a 65º da LGPD até 3 de maio de 2021. Para que a Lei tenha vigência plena, resta apenas o transcurso da vacatio legis prevista no inciso I-A do artigo 65, acrescido pela Lei n.º 14.010/2020, que prescreveu a entrada em vigor dos artigos 52 a 54, concernentes às sanções administrativas, em 1º de agosto de 2021.

Esta lei está em vigor desde 18 de setembro de 2020, excluindo as sanções administrativas, e a Autoridade Nacional de Proteção de Dados (ANPD), responsável pelo controle e sanção de indivíduos e autoridades e órgãos públicos, representou um ponto de virada indiscutível no ordenamento jurídico brasileiro quanto à proteção de dados pessoais físicos e digitais.

2.2.1 Fundamentos, regras e princípios basilares da Lei Geral de Proteção de Dados Pessoais e Direito dos Titulares de dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, Lei nº 13.709/2018, é fundamentada em diversos princípios que visam garantir a proteção dos dados pessoais e o respeito aos direitos fundamentais de privacidade e liberdade. Doutrinariamente, esses princípios são amplamente discutidos e analisados por especialistas em direito digital e proteção de dados. De acordo com Doneda (2020), o princípio da finalidade determina que o tratamento de dados pessoais deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular dos dados, significando que os dados não podem ser utilizados de forma incompatível com essas finalidades. Doneda e Mendes (2014) explicam que o princípio da adequação estabelece que o tratamento dos dados deve ser compatível com as finalidades informadas ao titular, garantindo que os dados coletados são relevantes e proporcionais ao objetivo pretendido. A necessidade implica que apenas os dados estritamente necessários para a realização das finalidades previstas serão coletados e tratados, minimizando a coleta excessiva de dados e promovendo um tratamento mais seguro e restrito (Doneda, 2020).

O princípio do livre acesso assegura aos titulares dos dados o direito de acessar e consultar a forma e a duração do tratamento, bem como a integralidade de seus dados pessoais, de forma facilitada e gratuita (Monteiro, 2018). Isso fortalece a transparência e a confiança entre o titular e o controlador. Segundo Wimmer (2019), a qualidade dos dados é essencial, garantindo que os dados sejam exatos, claros, relevantes e atualizados, conforme necessário para o cumprimento da finalidade de seu tratamento. A transparência exige que os titulares sejam informados de maneira clara, precisa e facilmente acessível sobre as práticas de tratamento de dados, incluindo a identidade do controlador, a finalidade do tratamento e os direitos dos titulares (Mendes, 2020).

Bioni (2019) afirma que o princípio da segurança obriga a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A prevenção na implementação de medidas proativas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais é essencial, reforçando a necessidade de práticas preventivas e a gestão de riscos. Sarlet (2013) destaca que o princípio da não discriminação impede a realização de tratamento de dados para fins discriminatórios, ilícitos ou abusivos, garantindo a proteção contra o uso de dados que possa resultar em discriminação ou prejuízo ao titular. O princípio da responsabilização e prestação de contas estabelece que os agentes de tratamento devem demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (Aranha, 2020).

A LGPD também se baseia em fundamentos doutrinários que embasam sua existência e aplicação, como o respeito à privacidade, que é um direito fundamental protegido pela LGPD e visa assegurar que os dados pessoais não sejam tratados sem a devida proteção (Bioni, 2019). O fundamento da autodeterminação informativa assegura o direito dos indivíduos de controlarem seus dados pessoais, permitindo que decidam sobre seu uso. A LGPD reconhece que a proteção de dados deve coexistir com outros direitos fundamentais, como a liberdade de expressão, informação, comunicação e opinião. Além disso, visa promover o desenvolvimento econômico e tecnológico e a inovação, de forma sustentável e equilibrada entre a proteção de dados pessoais e o avanço tecnológico e econômico (Mendes, 2020).

A proteção de dados pessoais deve harmonizar-se com os princípios da livre iniciativa, livre concorrência e defesa do consumidor, garantindo também a proteção dos consumidores. Este fundamento doutrinário reforça a proteção dos direitos humanos e a promoção da dignidade e cidadania, assegurando que o tratamento de dados respeite os direitos fundamentais dos titulares (Doneda, 2011). Esses princípios e fundamentos são essenciais para

a interpretação e aplicação da LGPD, garantindo que o tratamento de dados pessoais ocorra de maneira ética e responsável, conforme as normas estabelecidas e os direitos dos titulares.

A LGPD estabelece diretrizes essenciais para a proteção dos dados pessoais no Brasil. Ela visa assegurar o direito à privacidade e à proteção dos dados pessoais dos cidadãos, promovendo a transparência nas práticas de tratamento de dados e aumentando a confiança nas relações entre os titulares de dados e as organizações que os tratam.

Conforme o Artigo 2º, os principais fundamentos da LGPD incluem o respeito à privacidade, que visa garantir que os dados pessoais dos indivíduos sejam tratados de maneira que respeite a sua vida privada e intimidade. A autodeterminação informativa assegura que os titulares de dados tenham o direito de controlar como suas informações pessoais são coletadas e utilizadas, sendo informados sobre o tratamento de seus dados e tendo a capacidade de tomar decisões informadas sobre sua utilização. A LGPD também busca equilibrar a proteção de dados com a liberdade de expressão e informação, permitindo que os dados sejam tratados de maneira que não infrinja esses direitos fundamentais. A proteção contra o uso indevido de dados pessoais que possa comprometer a honra e a imagem dos indivíduos é outro pilar fundamental da LGPD, garantido pela inviolabilidade da intimidade, honra e imagem. Além disso, a lei reconhece a importância dos dados pessoais para o desenvolvimento econômico e tecnológico, promovendo uma regulamentação que permite a inovação enquanto protege os direitos dos indivíduos. Finalmente, a LGPD incentiva práticas inovadoras no tratamento de dados pessoais, desde que sejam implementadas de maneira ética e responsável.

Os princípios basilares da LGPD orientam o tratamento de dados pessoais, assegurando que esse processo seja realizado de maneira justa e transparente. Conforme o Artigo 6º, os principais princípios incluem a finalidade, que determina que os dados pessoais devem ser tratados para fins legítimos, específicos, explícitos e informados ao titular, sem desvios posteriores. A adequação exige que o tratamento dos dados seja compatível com as finalidades informadas ao titular, respeitando o contexto do tratamento. A necessidade limita a coleta de dados ao mínimo necessário para a realização de suas finalidades, evitando a coleta de dados excessivos ou irrelevantes. O livre acesso garante aos titulares de dados o direito de acessar, de forma facilitada e gratuita, os dados que lhes dizem respeito e a forma como esses dados estão sendo tratados. A qualidade dos dados é essencial, assegurando que os dados pessoais sejam precisos, claros, relevantes e atualizados conforme necessário para cumprir as finalidades do tratamento. A transparência exige que as informações sobre o tratamento de dados sejam claras, precisas e facilmente acessíveis aos titulares, proporcionando uma compreensão completa das práticas de tratamento. A segurança impõe que medidas técnicas e

administrativas sejam adotadas para proteger os dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A prevenção requer a adoção de medidas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. A não discriminação proíbe o uso dos dados pessoais para fins discriminatórios, ilícitos ou abusivos. Por fim, a responsabilização e prestação de contas exige que os agentes de tratamento demonstrem a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Alguns artigos específicos da LGPD merecem destaque por seu papel crucial na regulamentação da proteção de dados pessoais. O Artigo 7º estabelece as bases legais para o tratamento de dados pessoais, como o consentimento do titular, o cumprimento de obrigações legais e a execução de políticas públicas. O Artigo 18º garante os direitos dos titulares de dados, como a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos ou desatualizados, a anonimização, o bloqueio ou eliminação de dados desnecessários, e a portabilidade dos dados a outro fornecedor de serviço ou produto. O Artigo 37º estipula a obrigatoriedade de manutenção de registros das operações de tratamento de dados pessoais, evidenciando a conformidade com a LGPD. O Artigo 50º orienta sobre a necessidade de elaboração de regras de boas práticas e governança, incentivando as organizações a adotarem políticas internas que assegurem o cumprimento da LGPD.

A LGPD protege dados pessoais processados digitalmente e fisicamente, e suas regras gerais devem ser observadas tanto por pessoa física quanto por pessoa jurídica de direito privado. Dessa forma, a LGPD estabelece um marco regulatório robusto e abrangente para a proteção de dados pessoais no Brasil, assegurando direitos fundamentais e promovendo a transparência e a segurança no tratamento de dados (Brasil, 2018).

2.3 Direito dos titulares de Dados pessoais

Os direitos do titular de dados estão previstos no Capítulo III da Lei Geral de Proteção de Dados (LGPD), abrangendo os artigos 17 a 22. Fundamentada na dignidade humana, autodeterminação informativa e consentimento, a LGPD assegura a toda pessoa natural a titularidade de seus dados e a garantia dos direitos fundamentais de liberdade, intimidade e privacidade. O titular tem o direito, perante o controlador, a qualquer tempo, sem custos e mediante requisição expressa, de confirmação de existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou desconformes; portabilidade dos dados;

informação sobre o compartilhamento dos dados com entidades públicas ou privadas; informação sobre a possibilidade de não consentir com o tratamento e suas consequências; e solicitação de cópia eletrônica integral de dados pessoais em formato reutilizável (Brasil, 2018).

Além disso, a LGPD prevê o direito ao esquecimento no inciso VI do artigo 18, permitindo a retirada do consentimento previamente fornecido para uma finalidade específica e a eliminação dos dados tratados. Conforme o artigo 19, a satisfação de quaisquer desses pedidos deve ser providenciada pelo agente de tratamento, imediatamente em formato simplificado ou em até 15 dias da requisição, por meio de declaração completa e de fácil compreensão (Brasil, 2018).

Os direitos dos titulares de dados pessoais são um aspecto central na proteção da privacidade e na regulação do uso de informações pessoais, especialmente em um contexto onde a digitalização e o tratamento de dados se tornam cada vez mais onipresentes. No Brasil, esses direitos são amplamente protegidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que estabelece um conjunto de garantias para os indivíduos cujos dados são coletados, armazenados e processados. Um dos direitos fundamentais garantidos pela LGPD é o direito à informação. Os titulares de dados pessoais têm o direito de ser informados sobre o tratamento de seus dados, incluindo a finalidade, forma e duração do tratamento, identificação do controlador, compartilhamento de dados e responsabilidades dos agentes de tratamento. O direito de acesso permite que os titulares solicitem e obtenham uma cópia de todos os dados pessoais que estão sendo processados sobre eles, incluindo a confirmação de tratamento, acesso aos dados e informações sobre a origem dos dados (Brasil, 2018).

Os titulares têm o direito de corrigir dados incompletos, inexatos ou desatualizados, assegurando que as informações mantidas sejam precisas e reflitam a realidade. Podem solicitar a retificação de dados errados ou desatualizados e a inclusão de informações relevantes. Também podem requerer a anonimização, o bloqueio ou a eliminação de dados desnecessários ou excessivos, ou aqueles tratados em desconformidade com a lei. A anonimização transforma os dados em informações que não permitam a identificação do titular, o bloqueio suspende temporariamente o tratamento de determinados dados e a eliminação remove definitivamente os dados dos sistemas do controlador (Brasil, 2018).

A portabilidade dos dados permite que os titulares solicitem a transferência de seus dados pessoais para outro fornecedor de serviços ou produtos, de forma estruturada e interoperável, garantindo que a transferência não prejudique a continuidade dos serviços prestados. Os titulares podem solicitar a exclusão dos dados pessoais tratados com base no seu consentimento, reforçando a soberania sobre seus dados, incluindo a possibilidade de retirar o

consentimento a qualquer momento e a remoção dos dados coletados e processados com base no consentimento anterior (Brasil, 2018).

Os titulares têm o direito de saber com quem seus dados são compartilhados e para quais finalidades, garantindo transparência e controle sobre a disseminação dos dados pessoais. Isso inclui o conhecimento sobre as entidades que recebem os dados e o entendimento dos motivos e objetivos para os quais os dados são compartilhados (Brasil, 2018).

Com o avanço da inteligência artificial e do processamento automatizado de dados, a LGPD assegura que os titulares possam solicitar a revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais. Isso inclui a revisão de decisões que afetam significativamente o titular e são tomadas sem intervenção humana, além de explicações detalhadas sobre os critérios e a lógica utilizada no processo automatizado (Brasil, 2018).

Os titulares podem se opor ao tratamento de seus dados pessoais em determinadas circunstâncias, especialmente quando considerarem que o tratamento é inadequado ou desnecessário, como em casos de interesses legítimos do controlador ou para fins de marketing direto. Podem também apresentar reclamações à Autoridade Nacional de Proteção de Dados (ANPD) sobre o tratamento inadequado ou ilegal de seus dados pessoais, registrando queixas e preocupações junto à ANPD, que pode tomar ações contra controladores que violem a LGPD (Brasil, 2018).

Em casos de dano material ou moral decorrente do tratamento inadequado de dados pessoais, os titulares têm direito à indenização, garantindo que possam buscar reparação pelos danos sofridos através de procedimentos judiciais. A LGPD não apenas oferece um quadro robusto de direitos para os titulares de dados, mas também estabelece obrigações claras para os controladores e operadores de dados, promovendo um ambiente de transparência, segurança e responsabilidade (Brasil, 2018).

A implementação eficaz destes direitos é essencial para garantir a confiança dos cidadãos nas práticas de tratamento de dados e para assegurar a proteção da privacidade em um mundo cada vez mais digital. A Autoridade Nacional de Proteção de Dados desempenha um papel fundamental na supervisão e na garantia de que esses direitos sejam respeitados, fortalecendo o regime de proteção de dados no Brasil (Brasil, 2018).

3 APLICAÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: O CASO DO METRÔ DE SÃO PAULO

É indiscutível que a Lei n.º 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, se aplica à Administração direta e indireta. O referido artigo 1.º refere expressamente que a lei regula o tratamento de dados pessoais físicos ou digitais por parte de pessoas singulares ou coletivas de direito público ou privado. Sua cláusula única também acrescenta que as normas gerais da Lei são de interesse nacional e devem ser observadas pela União, Estados, União e Municípios (Brasil, 2018).

Com forte no inciso III do artigo 7º, excluídas as hipóteses de tratamento previstas no inciso III do artigo 4º, a que a lei não se aplica, tratamento e partilha de dados[2]. A administração pública pode ser exercida por pessoa física identificada ou identificável que reúna as condições de vigência da norma definida no parágrafo 3º, se for necessária para assegurar a ordem pública, o que estiver previsto em outras leis ou documentos de convênios administrativos, contratos, etc., desde que de acordo com o disposto no capítulo IV da Lei[3] (Brasil, 2018).

Pela localização topográfica do inciso III, assim como dos incisos II e X, são considerados casos excepcionais a que não se aplica direta e plenamente o princípio do consentimento, como principal vetor da autodeterminação informada prevista no inciso I (Brasil, 2018).

Mas a falta de consentimento do proprietário não significa arbitrariedade no tratamento. A Lei prevê, no § 3º do artigo 7º, que a finalidade, a boa-fé e o interesse público que justifiquem a disponibilização devem ser considerados no tratamento de dados pessoais publicamente disponíveis. O § 4º, ao liberar o titular da exigência de consentimento para o tratamento das informações por ele publicadas, protege seus direitos e a necessidade de cumprir os princípios estabelecidos por lei. Para evitar dúvidas, o § 6º estipula que a dispensa da exigência do consentimento do titular não isenta os subcontratantes, o utilizador e o subcontratante responsável de outras obrigações e dos princípios da lei (Brasil, 2018).

[2] A definição de "uso compartilhado de dados" consta do inciso XVI do artigo 5º, como sendo "[...] comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados" (Brasil, 2018a).

[3] Apesar de ser o inciso III do artigo 7º o mais expressamente aplicável à Administração Pública, não se olvida que, por exemplo, os incisos II, IV, V, VI, VII, VIII, IX e X também podem incidir no regime jurídico de direito público em que ela se inscreve.

Sobre o tratamento de dados pessoais sensíveis na administração pública, conforme disposto na Seção II do Capítulo II, a exceção ao princípio do consentimento voltou a se repetir em situações semelhantes às contidas no art. 7º e dos demais artigos da Seção I. O responsável pelo tratamento renuncia ao seu consentimento para cumprir obrigações legais ou regulamentares (artigo 11, inciso II, "a"), que pode ser pela pessoa ou pela administração, além disso, permite o tratamento conjunto de informações necessárias para realizar práticas gerais com base nas leis ou regulamentos da administração (artigo 11, inciso II, "b").

Outras hipóteses exigem dispensa de consentimento, ainda no inciso II do artigo 11, também são adequados para autoridades, são para investigações realizadas por órgãos de investigação[4], garantem o maior anonimato; exercício regular de direitos tanto em processo judicial como em processo administrativo ou arbitral; proteger a vida e a integridade física do proprietário ou de terceiros; nos cuidados de saúde, que devem ser prestados exclusivamente por profissionais de saúde, serviços de saúde ou instituição de saúde; e garantir a segurança do proprietário e antifraude (Brasil, 2018).

Outra disposição importante relativa ao tratamento de dados no desempenho de atividades administrativas foi estabelecida no § 2º do mesmo artigo 11, que, remetendo ao inciso I do artigo 23 da Lei, estipula que as normas legais, a finalidade e os procedimentos e práticas seguidos no tratamento e partilha de dados pessoais sensíveis e dados pessoais não sensíveis devem ser publicados e comunicados no sítio da Internet de uma pessoa coletiva de direito público. Por fim, no que concerne à Seção II, o artigo 13 dispõe que os órgãos de pesquisa poderão ter acesso a base(s) de dados pessoais durante pesquisas de saúde pública, que são tratadas apenas internamente e estritamente para fins de pesquisa, nas quais há a obrigação de implementar medidas de proteção contra ataques e vazamentos, sendo proibida a publicação de dados pessoais na divulgação de resultados (Brasil, 2018).

Além disso, é importante lembrar que, mesmo no caso do Estado e seus órgãos e instituições, o tratamento de dados pessoais, sensíveis ou não, segue o "ciclo de tratamento". Como regra geral, não deve haver tratamento eterno ou desnecessariamente prolongado, considerando a adoção do paradigma da autodeterminação informacional como fundamento da proteção de dados pessoais. É por isso que, na Seção IV do Capítulo II, os parâmetros usuais para suspensão do processamento de dados são definidos (Brasil, 2018).

[4] A definição do que seria um "órgão de pesquisa" consta do inciso XVIII do artigo 5º da Lei, com a seguinte redação: "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico" (Brasil, 2018a).

Em atenção ao artigo 15, a autoridade deve interromper o processamento dos dados se (i)o objetivo do processamento for alcançado ou os dados não forem mais necessários ou importantes para sua realização; ii) o fim do período de tratamento; (iii) se necessário, o titular da licença retirar o consentimento para proteger o interesse público internamente relacionado às atividades da administração, de modo que o despacho do inciso III do art. 7º; (iv) A ANPD decidirá, se a lei for violada, de acordo com as sanções cabíveis, conforme determinado no Capítulo VIII (Brasil, 2018).

Além disso, no final do tratamento, a obrigação de apagar os dados pessoais é regra, exceto nos termos do artigo 16, retenção para (i) cumprir a obrigação legal ou regulatória do controlador de acordo do inciso II do artigo 7º e da alínea "a" do inciso II do artigo 11 –; (ii) estudo por órgãos de pesquisa, garantida a anonimização, se possível, coadunando-se com as disposições do inciso IV do artigo 7º e da alínea "c" do inciso II do artigo 11 –; (iii) transferência para um terceiro que atenda aos requisitos legais de processamento contidos na seção I do Capítulo II; ou (iv) uso exclusivo do controlador, após devida anonimização (Brasil, 2018).

Todas essas menções a artigos dispersos no texto normativo da Lei n.º 13.709/2018 para ser capaz de mostrar que uma interpretação sistemática do padrão é necessária sob o risco de aplicação míope. Existem várias disposições relativas à aplicação da norma a uma autoridade pública externa ao Capítulo IV, mas que guardam perfeita e sistemática interlocução com a prescrição normativa geral do inciso III do artigo 7º.

Mesmo assim, é inegavelmente no Capítulo IV, continente dos artigos 23 a 32, que está disposto o núcleo normativo da aplicação da Lei ao Poder Público[5] (Silva, 1994).

Verte do artigo 23 a principal regra a ser observada pela Administração Pública. Conforme a disposição do caput, a Lei n.º 13.709/2018 deve ser observada pelas pessoas jurídicas de direito público contidas no artigo 1º da Lei n.º 12.527/2011, a Lei de Acesso à Informação (LAI). Esse dispositivo expressa o caráter temporário dessas leis e sujeita a esse regime a União, os Estados, o Distrito Federal e os Municípios. Em particular, a lei deve ser obedecida pelos órgãos públicos pertencentes ao executivo da administração própria, à administração legislativa, incluindo tribunais de recurso e ao judiciário, e ao ministério público

[5] A expressão "Poder Público" não tem acepção juridicamente plácida. É tanto usada como sinônimo de Administração direta e indireta quanto como significante da tríplice manifestação do Estado em Executivo, Legislativo e Judiciário (Silva, 1994). De qualquer sorte, o caput do artigo 23 da Lei n.º 13.709/2018, Lei de Proteção de Dados Pessoais, menciona expressamente o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do artigo 1º da Lei n.º 12.527/2011, Lei de Acesso à Informação, aplicável a órgãos públicos integrantes da administração direta e indireta. Desse modo, a plurivocidade da expressão não prejudica o presente estudo, que tem por objeto especificamente a aplicação da norma à Administração Pública, e se reportará à expressão tomando por base este sentido.

como instituição independente e sui generis. A lei também é observada pela gestão indireta, que são os órgãos municipais, fundações, empresas públicas e associações de economia mista[6], e outros sob controle direto ou indireto de entes federados, bem como os cartórios[7] (Brasil, 2018).

O processamento e compartilhamento de dados pelo governo é de natureza pública para atender a interesses públicos primários por meio do desempenho e cumprimento de obrigações sob a Lei do Serviço Público. O inciso I do artigo 23, com vistas a cumprir a regra geral contida no § 6º do artigo 7º e o pressuposto da transparência ativa, limita a necessidade de o Estado informar o subcontratante, preferencialmente no seu sítio eletrônico de fácil acesso, sobre as hipóteses com base nas quais os dados pessoais são tratados, nomeadamente quanto à finalidade e procedimentos e práticas usadas. O inciso II impõe outro requisito importante: que a pessoa jurídica de direito público indique quem é o responsável pelos dados. A lei já segue, portanto, as diretrizes normativas da Lei de Acesso à Informação, o que é um avanço notável na eletronização dos atos e procedimentos administrativos e no uso das tecnologias de informação e comunicação (Brasil, 2018).

No entanto, a lei sobre a obrigação de divulgação do tratamento de dados por órgãos e instituições estatais prevê que a ANPD pode regulamentar as formas de divulgação de suas atividades; que a obrigação de nomear uma autoridade de supervisão prevista no artigo não é cancelada por padrão 40 da LAI; e que os prazos e procedimentos de exercício de direito perante o Poder Público seguirão cada lei específica, sobretudo a Lei n.º 9.507/1997, para a retificação e o acesso à informação por meio de habeas data, a Lei n.º 9.784/1999, que dispõe sobre o processo administrativo, e a Lei n.º 12.527/2011, Lei de Acesso à Informação (Brasil, 2011).

É por isso que merece atenção o carácter normativamente horizontal da Lei Geral da Proteção de Dados Pessoais, que em vez de tentar desviar-se do conteúdo de outros regulamentos tematicamente semelhantes ou criar oposição aos mesmos, procurou harmonizar-se com estes diplomas, criando um efetivo sistema. proteção de dados pessoais (Silva, 2020).

Instrumentalizando o uso compartilhado de dados na administração pública mencionado no inciso III do artigo 7º, o artigo 25 estipula a obrigação de manter as informações, principalmente para uso comum, de forma interoperável e estruturada que permita a prestação

[6] Nos termos do artigo 24 da Lei n.º 13.709/2018, só será conferido tratamento equivalente ao da aplicação da Lei ao Poder Público para com as empresas públicas e as sociedades de economia mista quando estas estiverem operacionalizando e executando políticas públicas. Do contrário – isto é, quando estiverem sujeitas à disposição do artigo 173 da Constituição Federal, de exploração direta da atividade econômica –, o tratamento dispensado será aquele relativo às pessoas jurídicas de direito privado particulares (Brasil, 1988; Brasil, 2018a).

[7] Os parágrafos 4º e 5º do artigo 23 da Lei n.º 13.709/2018 dispõe que os serviços notariais e de registro, exercidos por delegação do Poder Público, mesmo que em caráter privado, se sujeitarão às regras e ao tratamento dispensados ao Poder Público, previstos no Capítulo IV. Ademais, é dever dos órgãos notariais e de registro fornecer à Administração Pública acesso eletrônico aos dados contidos em seus bancos de dados (Brasil, 2018a).

de serviços públicos e o alcance de objetivos públicos, bem como a descentralização das atividades administrativas e a disseminação dessas informações e para facilitar o acesso para isso da administração e outras agências e instituições[8]. A lei adotou um prisma segundo o qual o tratamento de dados deve cumprir funções públicas, que constituem um vetor de satisfação do interesse público, à semelhança do que prevê a LAI (Brasil, 2014; Brasil, 2018).

Portanto, a regra estabelecida no § 26 da LGPD é que o uso conjunto de dados pessoais pelo governo deve obedecer aos princípios definidos no artigo 6º da lei, em especial dever e tratamento adequado o propósito específico de implementar políticas públicas e satisfazer o interesse público, que é outra limitação ao processamento de dados pelo governo direta ou indiretamente (Brasil, 2018). Além disso, as pessoas jurídicas públicas mencionadas no título do artigo não estão, em princípio, autorizadas a divulgar os dados pessoais de seu banco de dados a um particular (Maldonado; Blum, 2020).

A proibição, que não deixa de ser uma das mais importantes e paradigmáticas da lei, contém muitas exceções, previstas no § 1º do artigo 26. Assim, por exemplo, a administração pode compartilhar e/ou transferir dados pessoais para pessoas jurídicas de direito privado se: o desempenho descentralizado de função pública por pessoa jurídica de direito privado exigir tal cessão para finalidade pública estritamente específica e determinada; os dados pessoais estejam disponíveis ao público de acordo com a proteção prevista na lei, nomeadamente as normas de tratamento do artigo 6.º; permitido por lei ou outra legislação; a transferência for pactuada com acordos (de gestão), contratos, etc., documentos que devam ser notificados à ANPD; e se o único e específico objetivo da transmissão de dados for prevenir fraudes e irregularidades ou proteger a segurança e integridade dos dados (Brasil, 2018).

Tais exceções se somam às hipóteses de compartilhamento de dados utilizadas pelo poder público contra a implementação de política pública para satisfação do interesse público e demais hipóteses mencionadas no caput do artigo. 7º, prescindem do consentimento do titular, perfazendo, como já dito, ressalva ao princípio do consentimento, com forte no artigo 27, embora não se furtem ao mencionado respeito às normas do artigo 6º. Em qualquer caso, cabe à administração pública informar a ANPD e os administradores do respectivo sítio eletrônico sobre a transferência ou compartilhamento de dados pessoais entre ela e uma entidade privada,

[8] A implementação de um formato interoperável de dados visa a permitir a interação recíproca entre sistema, sem a necessidade de replicação de dados. Para tanto, o Governo tem adotado o padrão de dados em formato aberto, o que não desconstitui o dever de mínima coleta e de atendimento à finalidade específica do tratamento (Cristóvam; Hahn, 2020; Schramm, 2020).

que ainda pode ser regulada por autoridade pública. , conforme parágrafo único deste artigo (Brasil, 2018).

Esta obrigação de informar a ANPD é uma das consequências da autoridade fiscalizadora, reguladora e sancionadora deste órgão, que poderá, nas condições dos artigos 29 e 30, alterar regras adicionais relativas à transferência e compartilhamento de dados pessoais e à exigência e autoridades responsáveis pela administração pública para obter informações precisas sobre a natureza dos dados e os detalhes do processamento, um requisito técnico adicional para emitir uma declaração para garantir o cumprimento da lei (Brasil, 2018).

Os dois últimos artigos do Capítulo IV são os Artigos 31 e 32, que constam da Seção II, que trata da responsabilidade dos entes públicos mencionados no Artigo 23. A regra aplica- se se não houver violação de lei. no artigo 37 parágrafo 6 da Constituição Federal, que trata da responsabilidade e responsabilidade do controlador e/ou controlador e das sanções cabíveis nos artigos 52-54 da ANPD[9].

Além disso, a ANPD tem a prerrogativa de exigir que os representantes da administração publiquem relatórios de impacto sobre os dados pessoais processados para fins de auditoria e polícia, bem como propor a implementação de padrões de segurança, boas práticas e boas práticas. de acordo com o Capítulo VII (Lorenzon, 2021; Maldonado; Blum, 2020).

No que toca à transferência internacional de dados[10] prevista no Capítulo V, a administração pública está sujeita à regra geral do princípio da equivalência, segundo a qual tal transferência é permitida por lei apenas para países ou organizações internacionais que, segundo análise da ANPD, assegurem proteção de dados pessoais equivalente à LGPD. (Brasil, 2018; Doneda, 2020). Tal análise pode ser solicitada pelas pessoas jurídicas de direito público nos termos do art 23, regulamentação do artigo ou se a transferência for necessária devido à cooperação jurídica internacional entre inteligência pública, investigação e processos judiciais de acordo com documentos jurídicos internacionais (Brasil, 2018).

[9] É importante esclarecer que, no caso do tratamento de dados pelo Poder Público, o controlador de dados será a própria pessoa jurídica de direito público (União, Estado, Distrito Federal e Município), mesmo que as obrigações típicas de controlador sejam dos órgãos públicos, por conta da desconcentração administrativa e a o operador de dados será ou pessoa natural ou pessoa jurídica de direito público ou privado contratada ou terceirizada pelo controlador. Assim, por exemplo, mesmo que o dever de transparência e a obrigação de nomeação de encarregado de dados seja do órgão público, a responsabilidade jurídica, no caso do controlador, será da União. É a ela, como controladora, e ao respectivo operador que se aplica o regime de responsabilidade previsto na Seção III do Capítulo VI da Lei n.º 13.709/2018, interpretado à luz do caput e do § 6º do artigo 37 da Constituição Federal de 1988. (Brasil, 2021; Schramm, 2020; Vivas, 2020).

[10] A expressão "transferência internacional de dados" é definida no inciso XV do artigo 5º da Lei n.º 13.709/2018 como sendo a "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro" (Brasil, 2018a).

Por fim, embora tanto as disposições relativas à transferência internacional de dados contidas no capítulo externo do Capítulo IV e apesar das explicações fornecidas sobre a aplicação da lei geral de proteção de dados pessoais na administração pública, a disposição constante do art. 20, o direito do titular à explicação e revisão das decisões tomadas exclusivamente com base no tratamento automático de dados pessoais e respeitantes aos seus interesses, levanta a questão da obrigação de fundamentar e controlar a decisão administrativa automática possibilitada pelo tratamento de dados pessoais, um problema (Brasil, 2018).

Assim, percebe-se que, embora o panorama geral da aplicação da norma nº 13.709/2018 tenha sido fragmentado, há problemas específicos na implementação da norma na administração pública que requerem maior aprofundamento.

3.1 Publicidade e dever de transparência na atividade

A necessidade do consentimento explícito, a transparência nas práticas de coleta e tratamento de dados e a segurança no manejo dessas informações são princípios centrais da LGPD que devem ser observados rigorosamente. A decisão judicial contra a Via Quatro reflete a importância de respeitar esses princípios, estabelecendo um precedente crucial para garantir que as tecnologias emergentes sejam implementadas de maneira ética e legal, protegendo a privacidade e os direitos dos indivíduos.

A administração pública tem o dever de agir de acordo com o princípio da divulgação, a fim de alcançar interesses gerais. A Constituição Cidadã sintetiza as prescrições necessárias ao cumprimento dessa tarefa e, portanto, o dever de agir em nome da transparência, como no caso dos incisos XIV, XXXIII, XXXIV e LXXII do artigo 5º e do caput, § 1º e inciso II do § 3º do artigo 37. Mas a lei também protege os direitos individuais à liberdade, à privacidade, à intimidade, à imagem, à honra e à integridade dos dados, como delineado nos incisos II, IV, VI, IX, X, XI, XII do artigo 5º (Brasil, 1988). Como afirmou Gilmar Ferreira Mendes, “A transparência é um princípio fundamental da administração pública e um elemento essencial para a democracia” (Mendes, 2018, p. 90).

No plano infraconstitucional, parece existir uma tensão dialógica entre a orientação normativa da Lei n.º 12.527/2011, a Lei de Acesso à Informação (LAI), que promove a abertura e publicidade como diretriz geral, e as diretrizes normativas da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). A LAI prioriza a abertura e publicidade, enquanto a LGPD prioriza o direito de autodeterminação e proteção de dados pessoais, com a necessidade de consentimento livre, informado e inequívoco do titular, exceto em casos específicos (Brasil,

2018). Como Michel Foucault observou, “onde há poder, há resistência” (Foucault, 1978), refletindo a complexa relação entre transparência e proteção de dados na administração pública.

A LAI interpreta essas leis com abordagens normativas, cuidando da proteção de informações pessoais relativas a uma pessoa física identificada ou identificável sujeita à restrição de acesso público, conforme os artigos 4º, inciso IV, e 6º, inciso III (Brasil, 2011). Por outro lado, a LGPD prevê a possibilidade de tratamento de dados pessoais sem consentimento prévio em determinadas circunstâncias, como no tratamento e partilha de informação necessária à implementação de políticas públicas definidas em leis de administração pública (Brasil, 2018).

Como apontou Danilo Doneda, "a legislação brasileira busca equilibrar a transparência governamental e a proteção dos dados pessoais, refletindo uma tensão entre a necessidade de publicidade e o direito à privacidade" (Doneda, 2005, p. 33).

Dessa tensão e da influência mútua de tais leis, surge uma preocupação com o limite normativo do dever de transparência, a observação geral da divulgação de informações de interesse público e o dever de proteção de dados pessoais. A questão é como o diálogo entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados deve ser interpretado de forma que prevaleça a harmonia normativa e evite antinomias (Brasil, 2018). Como afirmou Alessandro Acquisti, "a tensão entre transparência e privacidade representa um dos desafios mais críticos na era da informação" (Acquisti, 2014, p. 25).

Embora sejam muito complementares entre si, há contradições entre a LGPD e a LAI, que só podem ser superadas pelo executor das normas, passando do nível abstrato da necessidade para o nível concreto do ser, como interpretação sistemática e teológica.

No artigo 4º da LAI, a informação é definida como correspondendo a dados, processados ou não, e o processamento de dados é definido como correspondendo à produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, arquivo, armazenamento, avaliação, finalidade, exclusão ou controle de dados sobre. Dados pessoais significam informações sobre uma pessoa física identificada ou identificável. Conforme essa lei, o tratamento de informações pessoais, regulado no artigo 31, está ainda sujeito ao princípio geral de abertura e divulgação das atividades administrativas, com exceção da privacidade, honra e reputação do cidadão administrativo, bem como das suas liberdades e garantias pessoais, cujo acesso é limitado por 100 anos, nos termos do § 1º (Brasil, 2011).

Como Danilo Doneda pontua, a proteção de dados pessoais é um direito fundamental que deve ser harmonizado com outros direitos igualmente fundamentais, como a liberdade de expressão e o acesso à informação. A aplicação prática dessas normas requer uma

abordagem equilibrada e contextualizada, respeitando as especificidades de cada situação (Doneda, 2020).

Isso significa que para a Lei de Acesso à Informação (LAI), via de regra, o dever de divulgação e transparência se aplica até mesmo aos dados pessoais na realização de atos administrativos, sem menção de limitar o acesso a informações de pessoa singular identificada ou identificável que não sejam de natureza íntima, privada ou sensível (Schiefler, 2013).

A LGPD, por outro lado, define de forma semelhante e distinta dados pessoais como informações sobre pessoa natural identificada ou identificável nos termos do inciso I do artigo 5º, e confere ao titular dos dados amplos poderes no tratamento de seus dados, exigindo o cumprimento do princípio do tratamento definido no artigo 6º e a satisfação dos direitos do titular previstos no Capítulo III (Brasil, 2018). Diferentemente da LAI, a LGPD designa como titular o controle dos dados, com base no fato de que na atual conjuntura social, econômica e jurídica, a proteção dos dados pessoais deve ser ampla e independente da natureza dos dados pessoais. Esta lei atribui aos poderes públicos uma forte responsabilidade pela boa gestão e responsabilidade no tratamento dos dados (Brasil, 2018). Como Laura Schertel Mendes observa, A LGPD inaugura um novo patamar de proteção de dados pessoais no Brasil, ao reconhecer que a proteção de dados é um direito fundamental e, ao mesmo tempo, ao atribuir responsabilidades claras e rigorosas aos controladores e operadores de dados (Mendes, 2019).

Apesar dessas contradições, parece que a melhor hermenêutica dessas leis permite vislumbrar que ambas - o postulado normativo do Estado Democrático de Direito no Brasil, que perdura com a criação da república, de que todo poder emana do povo e que a atuação do Estado é sempre para o bem do povo e pautada pela dignidade humana - protegem os cidadãos como seu principal objetivo (Schiefler, 2013).

O primeiro passo para evitar conflitos entre esses padrões é entender que transparência não significa necessariamente abertura irrestrita. A divulgação de fatos e atos administrativos significa revelá-los à comunidade por meio de processos judiciais apropriados. A finalidade da transparência é revelar, explicar e esclarecer atos administrativos com o objetivo de comunicação efetiva entre o Estado e o cidadão. A abertura, por outro lado, não significa necessariamente acesso irrestrito, mas permitir o acesso dos cidadãos aos procedimentos e processos relevantes para eles (Carvalho Filho, 2019; Maretti; Monroe, 2020).

Isso deve ser entendido porque a ordem constitucional não formula como privilégio o direito de informação do indivíduo e as obrigações administrativas de divulgação e transparência da administração pública, mas, ao contrário, estabelece a obrigação de proteger os direitos e garantias dos cidadãos. Num Estado Democrático de Direito, o poder público não

é o titular dos interesses públicos, mas o seu guardião. A transparência e abertura devem ser interpretadas como meios para garantir os direitos fundamentais da administração civil, e não como deveres da administração pública de satisfazer seus próprios interesses (Cabral, 2020; Oliveira, 2008).

A LGPD tomou esse ponto de partida como diretriz para sua regulamentação geral e gestão. A lei inclui a transparência como um dos princípios a serem rigorosamente observados por um agente de processamento, conforme definido pelo art. 6º. Esta transparência de tratamento é sempre apoiada pela justificação desta necessidade, a determinação de um objetivo legal e suficiente, o direito a receber um tratamento de duração curta e gratuita e a sua consulta pessoal. A informação e a necessidade de tomar medidas preventivas e de segurança da informação, sem prejuízo de prestação de contas (accountability) e responsabilização do agente (Bioni, 2019; Brasil, 2018).

Do ponto de vista do tratamento por parte das autoridades, isso significou estabelecer o princípio da boa administração moderna como lastro para a atuação aberta do Estado no tratamento de dados pessoais. A base valorativa do princípio é garantida e democrática, assumindo que a pessoa é protagonista do espaço público, ao mesmo tempo ator individual e paciente no plano coletivo, da satisfação do interesse geral[11.] (Munõz; Maza, 2020).

Existem diversos artigos na LGPD que reforçam essas posições normativas e valorativas. O inciso III do art. 7º vincula o tratamento e a utilização comum das pessoas jurídicas de direito público à realização do fim geral do interesse público. O artigo 6º requer respeito ao propósito, tratamento mínimo e incentivado, abordagem de proprietário e transparência, prestação de contas e responsabilidade. Os artigos 41, 53 e 55-J, § 2º, implementam a participação popular como base da atividade do poder estatal. Todos esses regulamentos norm ativos cumprem as obrigações impostas pela LAI do poder público e as obrigações de transparência ativa e passiva, que protegem o direito fundamental à informação, não contra eles (Brasil, 2018).

Ao adotar tal postura hermenêutica e axiológica, a LGPD é amplamente compatível com a LAI, a transparência do compromisso governamental e os princípios de divulgação e

[11] Esclarecendo o paradigma da transparência e da publicidade como postulado de empoderamento da sociedade civil, e como premissa básica de um governo do povo, pelo povo e para o povo, Munõz e Maza (2020, p. 36) assertam que "La persona es la protagonista del espacio público y el epicentro de la acción pública, por lo que los gobernantes deben crear y adecuar las condiciones necesarias que permitan al ser humano el desarrollo de sus facultades y la satisfacción de sus legítimas aspiraciones. Para permitirles alcanzar sus aspiraciones debe garantizarse la libre participación en los asuntos comunes, pero también una salvaguarda libre de la injerencia del Estado y de terceros en su esfera íntima y personal. Los poderes públicos no son ni de los políticos ni de los funcionarios, son de las personas".

acesso à informação, sem esquecer a proteção da pessoa física identificada ou identificável como dado. Contratos temáticos de acordo com o art. 17. Em suma, pode afirmar-se que a transparência e abertura da administração pública não contrariam a proteção dos dados pessoais, pelo contrário, são condição parcial dessa possibilidade (Brasil, 2011).

Entretanto, a melhor interpretação não ignora as incompatibilidades entre essas leis, especialmente no que se refere ao disposto no artigo 31, § 1º, inciso I e § 3º, inciso V, da LAI (Brasil, 2011). Para a LGPD, conforme os artigos 1º, 2º, 3º, 4º, 6º, 7º, 9º, 17 a 22, a proteção da norma pertence a todos os dados pessoais, não apenas informações relacionadas à intimidade, privacidade, vida, honra e imagem (Brasil, 2018).

A LGPD estabelece um equilíbrio fundamental entre a transparência governamental e a proteção de dados pessoais, reconhecendo a importância da autodeterminação informativa em uma sociedade digitalizada e a necessidade de mecanismos de responsabilização claros para os controladores de dados (Bioni, 2019).

A razão dada no texto normativo do parágrafo é impedida pelo princípio da boa governança à luz do Estado Democrático de Direito, no qual esta lei permanece inserida no inciso V do § 3º do artigo 31 da LAI, de motivação abstrata e geral de proteger o interesse público ou geral dominante como suposto fundamento do consentimento desnecessário do titular. Isso é compatível com o dever da administração pública de observar os cuidados especiais e adequados decorrentes da LGPD e uma finalidade suficientemente motivada na implementação da política pública, incluindo a comunicação detalhada e transparente ao controlador de dados gerenciados por cidadãos (Brasil, 2018).

“A boa governança em matéria de dados pessoais implica não apenas a proteção e a segurança dos dados, mas também a transparência e a prestação de contas das atividades dos controladores, especialmente no setor público, onde a confiança dos cidadãos é fundamental” (Wimmer, 2020, p. 87).

Não existe uma solução hipotética categórica para a complexidade dos casos individuais relacionados com o equilíbrio entre a obrigação de divulgação administrativa e a transparência e o direito do titular à proteção dos dados pessoais. Como exemplo de situação em que esta última pode esfriar pela duplicação da primeira, está prevista a divulgação dos salários dos servidores públicos em um portal eletrônico de transparência (Brasil, 2018).

Neste caso, os dados fornecidos são os dados de um servidor que executa uma tarefa pública, mesmo que sejam intercalados com os dados de uma pessoa física que executa o serviço público correspondente, que em princípio não é uma violação do direito para proteger os dados pessoais. No entanto, importa referir que a publicação de informação do mesmo

servidor que não esteja estritamente relacionada com o desempenho de um cargo público seria ilegal, o que mesmo nesta hipótese acaba por ser uma forma bastante brutal de proteger tal direito (Brasil, 2018).

3.2 Proteção de dados pessoais no fornecimento de serviço público

A proteção de dados pessoais é essencial no fornecimento de serviços públicos, especialmente com a crescente digitalização e uso de tecnologias da informação. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabelece normas para o tratamento de dados pessoais, visando proteger os direitos fundamentais de liberdade e privacidade (Brasil, 2018).

De acordo com a LGPD, dados pessoais são todas as informações relacionadas a uma pessoa natural identificada ou identificável. O tratamento desses dados inclui atividades como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018). No contexto dos serviços públicos, proteger os dados pessoais é crucial para garantir a confiança dos cidadãos. As instituições públicas devem tratar as informações sensíveis de forma ética e conforme as disposições legais (Bioni, 2019).

Ainda em 2018, outra Ação Civil Pública (ACP) ganhou enorme repercussão, trazendo o debate da proteção dados para o cotidiano da população. No final de agosto de 2018, o Instituto Brasileiro de Defesa do Consumidor (Idec) ajuizou ACP contra a ViaQuatro, concessionária da Linha Amarela do metrô de São Paulo. O imbróglio surgiu em razão do anúncio de uma parceria com a AdMobilize – empresa com sede em Miami (EUA) – para lançamento das Portas Interativas Digitais (PIDs).

As PIDs funcionariam como um painel publicitário capaz de realizar análises agregadas das emoções dos passageiros do metrô. A partir de um piloto com a LG do Brasil e Hyperpharma, as PIDs passaram a coletar imagens de câmeras instaladas acima dos painéis publicitários. As imagens das câmeras, por sua vez, eram processadas com o software da AdMobilize, que identificaria as emoções das pessoas filmadas e registraria informações como estimativa de idade e sexo, possibilitando um modelo de negócios de "pay per look" ou "pay per face"[3] (Zanatta, 2020).

[3]As expressões são de Rodolfo Saccoman, presidente da AdMobilize. Cf. RINALDI, Camila. Entidades combatem câmeras do metrô de SP que leem emoções de passageiros para vender publicidade, TheIntercept Brasil, 31 de agosto de 2018. Disponível em: https://theintercept.com/2018/08/31/metro-cameras-acao-civil/?comments=1.

A LGPD impõe às entidades públicas a obrigação de tratar os dados pessoais apenas para finalidades legítimas, específicas, explícitas e informadas ao titular, conforme o princípio da finalidade (Brasil, 2018). Esse princípio é fundamental para evitar o uso inadequado dos dados e garantir a transparência no tratamento das informações. O princípio da adequação exige que o tratamento dos dados seja compatível com as finalidades informadas ao titular. As entidades públicas devem garantir que os dados coletados sejam relevantes, proporcionais e não excessivos em relação às finalidades para as quais são processados (Doneda, 2020). Além disso, o princípio da necessidade obriga as instituições a limitar a coleta e o tratamento de dados pessoais ao mínimo necessário para o cumprimento de suas finalidades. Essa prática ajuda a reduzir os riscos de violações de privacidade e garante uma gestão mais segura das informações (Monteiro, 2018).

A transparência é outro princípio essencial da LGPD. As entidades públicas devem fornecer aos titulares de dados informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados, incluindo a finalidade do tratamento, a forma e a duração do processamento, bem como os direitos dos titulares (Wimmer, 2019). No fornecimento de serviços públicos, é fundamental garantir que os dados pessoais sejam tratados com qualidade. Isso significa que as informações devem ser exatas, claras, relevantes e atualizadas conforme necessário para cumprir as finalidades do tratamento (Brasil, 2018).

A segurança dos dados é um aspecto crítico na proteção de informações pessoais no setor público. A LGPD impõe que as entidades públicas adotem medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, 2018). A prevenção de danos exige a adoção de medidas proativas para evitar a ocorrência de incidentes que possam comprometer a privacidade dos dados pessoais. Isso inclui a implementação de políticas de segurança da informação e a realização de treinamentos periódicos para os funcionários (Bioni, 2019).

Outro caso polêmico é o da exploração de dados obtidos pelas câmeras do metrô de São Paulo/SP, as quais liam e analisavam por meio de um software as emoções dos passageiros pela leitura facial dos mesmos, com o intuito de vender-lhes publicidade direcionada (Documento sem título (11), 2023).

---

[4]Rede Latino-Americana de Estudos de Vigilância, constituída por sociólogos, antropólogos, cientistas políticas e juristas. Ver www.lavits.org.

[5]Programa de Educação Tutorial da Faculdade de Direito da Universidade de São Paulo. Foi fundado por José Eduardo Faria na década de 1970. Atualmente, é coordenado pelo professor Rafael Mafei. Ambos são professores do Departamento de Filosofia e Teoria Geral do Direito da USP.

A não discriminação é outro princípio importante da LGPD. Ela proíbe o tratamento de dados para fins discriminatórios, ilícitos ou abusivos, garantindo que os dados pessoais não sejam utilizados de maneira que possa causar danos aos titulares (Sarlet, 2013). A responsabilidade e a prestação de contas requerem que as entidades públicas demonstrem a adoção de medidas eficazes para garantir o cumprimento das normas de proteção de dados. As instituições devem manter registros detalhados das operações de tratamento de dados e estar preparadas para prestar contas à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares (Aranha, 2020).

A proteção de dados pessoais no fornecimento de serviços públicos também envolve a gestão de riscos e a elaboração de relatórios de impacto à proteção de dados, conforme exigido pela LGPD. Esses relatórios avaliam os riscos relacionados ao tratamento de dados e propõem medidas para mitigá-los (Brasil, 2018). A participação dos titulares de dados é essencial para a efetiva proteção de informações pessoais. A LGPD garante aos cidadãos o direito de acesso, correção, exclusão e portabilidade de seus dados, além de permitir a oposição ao tratamento em determinadas circunstâncias (Brasil, 2018).

A criação de políticas de privacidade claras e acessíveis é uma prática recomendada para as entidades públicas. Essas políticas devem informar os cidadãos sobre como seus dados são coletados, usados, armazenados e protegidos (Monteiro, 2018). A capacitação contínua dos funcionários das entidades públicas é fundamental para a proteção de dados pessoais. Treinamentos regulares sobre a LGPD e práticas de segurança da informação ajudam a garantir que todos estejam cientes de suas responsabilidades e das melhores práticas de proteção de dados (Wimmer, 2019).

A colaboração entre diferentes órgãos públicos pode facilitar a implementação de políticas de proteção de dados mais eficazes. Compartilhar experiências e boas práticas contribui para o fortalecimento das medidas de segurança e privacidade (Bioni, 2019). A implementação de tecnologias seguras é crucial para a proteção de dados pessoais no setor público. Ferramentas como criptografia, controle de acesso e monitoramento de sistemas ajudam a proteger as informações contra acessos não autorizados e violações (Doneda, 2020).

A auditoria periódica das práticas de proteção de dados é uma medida importante para garantir a conformidade com a LGPD. As auditorias ajudam a identificar possíveis falhas e áreas de melhoria, promovendo a transparência e a responsabilização (Brasil, 2018). A comunicação clara e eficaz com os cidadãos sobre suas práticas de proteção de dados é essencial. Informar os cidadãos sobre seus direitos e como exercê-los fortalece a confiança nas instituições públicas (Monteiro, 2018).

A responsabilidade pelas violações de dados deve ser claramente atribuída. A LGPD estabelece que as entidades públicas são responsáveis por garantir a proteção dos dados pessoais e devem responder por qualquer falha na segurança dessas informações (Brasil, 2018). A gestão de incidentes de segurança deve ser eficiente e rápida. As entidades públicas devem ter planos de resposta a incidentes que permitam a identificação, contenção e mitigação de quaisquer violações de dados (Wimmer, 2019).

A proteção de dados pessoais deve ser considerada em todas as fases do ciclo de vida dos dados, desde a coleta até o descarte. Implementar práticas de segurança em todas essas etapas ajuda a minimizar os riscos de violação de privacidade (Doneda, 2020). O uso ético dos dados pessoais é fundamental para a proteção de informações no setor público. As entidades devem garantir que os dados sejam usados apenas para fins legítimos e em conformidade com os princípios da LGPD (Sarlet, 2013).

A transparência na contratação de serviços de terceiros é crucial. As entidades públicas devem garantir que os fornecedores de serviços também cumpram as normas de proteção de dados e adotem medidas de segurança adequadas (Bioni, 2019). A criação de comitês de privacidade pode ajudar a monitorar e implementar as políticas de proteção de dados. Esses comitês podem atuar como órgãos consultivos, fornecendo orientação e supervisão contínua (Aranha, 2020).

A utilização de tecnologias de anonimização e pseudonimização é uma prática recomendada para proteger a privacidade dos cidadãos. Essas técnicas ajudam a minimizar os riscos associados ao tratamento de dados pessoais (Brasil, 2018).

Endler (2000) diz que a internet é de suma importância como uma ferramenta para melhorar a gestão dos serviços públicos. Ele enfatiza que a internet pode facilitar a prestação de serviços públicos, mas também aponta desafios como a exclusão digital e a necessidade de políticas que garantam o acesso equitativo à tecnologia. "Os governos têm a função de garantir o acesso ao cidadão a essas novas tecnologias, usando-as como incentivadoras da democracia e não como barreiras onde existam os que têm acesso e os excluídos" (Endler, 2000, p. 345).

Diniz *et al*. (2009) também identificam a importância das tecnologias de informação e comunicação (TICs) para a modernização da administração pública e a prestação de serviços públicos eficientes e transparentes. Diniz diz que para analisar a implantação do governo eletrônico se deve enfatizar na necessidade de avaliar os impactos das TICs na gestão pública e nos serviços ao cidadão. "Consequentemente, temas como desempenho, eficiência, eficácia, transparência, mecanismos de controle, qualidade do gasto público e prestação de

contas foram associados ao processo de construção de programas de governo eletrônico" (Diniz *et al*., 2009, p. 45).

No entanto, a coleta e a falta de transparência no tratamento de dados pessoais podem funcionar como vetor de violação à privacidade, extrapolando os limites da vida privada das pessoas e visando as mais diversas aplicações, geralmente de cunho financeiro (Barbosa; Silva, 2019). Logo, não é a coleta e o processamento de dados por si sós que podem causar danos e violar direitos dos indivíduos. O problema reside na falta de clareza de como esses dados são efetivamente coletados e o que é feito com eles. Negligenciá-lo pode ocasionar novos problemas de imensas proporções (Barbosa; Silva, 2019).

Os serviços públicos na internet possibilitam uma constante adaptação às necessidades do cidadão. O layout da interface pode ser flexível, os órgãos podem gerar novos serviços e novas funcionalidades e incluí-los sem maiores problemas operacionais. Isso é viabilizado com o uso de constantes pesquisas de satisfação que podem alimentar banco de dados com os diferentes perfis de usuários e suas necessidades (Read, 2000).

Autores como Gil-Garcia e Pardo (2005) ao classificarem os principais desafios e fatores críticos de sucesso na implementação de um projeto de governo eletrônico indicam que as principais preocupações estão no limite entre a transparência e o sigilo dos dados dos cidadãos nas questões relacionadas à integração e compatibilidade tecnológica e nos problemas de continuidade orçamentária e rigidez burocrática, indicando que o sucesso depende fortemente do adequado tratamento dos aspectos tecnológicos, organizacionais, legais e políticos (RAP, 2019).

Existem exceções à proibição de compartilhamento de dados pessoais pela administração pública, conforme previsto na LGPD, com destaque nas condições sob as quais os dados podem ser compartilhados, como para fins de desempenho descentralizado de função pública, disponibilidade pública dos dados, autorização legal, e prevenção de fraudes e irregularidades. "A transferência for pactuada com acordos (de gestão), contratos, etc. documentos que devam ser notificados à ANPD" (Brasil, 2018).

Portanto, há preocupação comum com a proteção de dados pessoais e a inclusão digital no contexto do governo eletrônico. Endler (2000) e Diniz *et al*. (2009) enfatizam a importância da internet e das TICs para a modernização dos serviços públicos, mas também reconhecem os desafios relacionados à exclusão digital e à necessidade de políticas inclusivas. A LGPD, por sua vez, estabelece diretrizes claras para o compartilhamento de dados pessoais, visando proteger a privacidade dos cidadãos enquanto permite a eficiência administrativa.

Finalmente, a promoção de uma cultura de privacidade dentro das instituições públicas é essencial. Incentivar uma atitude proativa em relação à proteção de dados contribui para a construção de um ambiente mais seguro e respeitoso em relação aos direitos dos cidadãos (Bioni, 2019).

4 ANÁLISE DO CASO DO METRÔ DE SÃO PAULO

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, tem como objetivo central a proteção dos direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Esta lei estabelece diretrizes claras para o tratamento de dados pessoais, fiscalização tanto ao setor privado quanto ao setor público, e é um marco regulatório importante para a modernização da gestão de dados no Brasil (Lei nº 13.709, de 14 de agosto de 2018).

A Via Quatro, supervisão responsável pela operação da Linha Amarela do Metrô de São Paulo, se viu envolvida em uma controvérsia jurídica significativa devido ao uso de tecnologias de reconhecimento facial nas estações de metrô. A implementação dessas tecnologias, projetada para melhorar a segurança e o controle de acesso, levantou preocupações quanto à conformidade com a LGPD, especialmente no que diz respeito ao consentimento dos titulares dos dados e à transparência das práticas de coleta e tratamento de dados (Ramos, 2020).

A Via Quatro é uma concessionária privada que atua na gestão e operação da Linha 4-Amarela do Metrô de São Paulo. Fundada em 2006, a empresa foi criada com o objetivo de trazer inovação e eficiência ao sistema de transporte metroviário da cidade, através de um contrato de Parceria Público-Privada (PPP). Esse modelo de gestão permite a combinação de investimentos privados e públicos, visando à melhoria da infraestrutura e dos serviços oferecidos à população (Sant'Anna, 2024).

A concessionária é responsável por toda a operação da Linha Amarela, incluindo a manutenção das estações e dos trens, a segurança dos passageiros e a implementação de novas tecnologias que aprimorem a experiência dos usuários. A Via Quatro destaca-se por utilizar trens modernos e automatizados, além de adotar práticas que buscam garantir a sustentabilidade e a eficiência energética (Oliveira, 2024). Inaugurada em 2010, a Linha 4-Amarela é uma das linhas mais importantes do sistema de transporte público de São Paulo. Com um traçado que liga a região oeste à região central da cidade, a linha é essencial para a mobilidade urbana, conectando áreas densamente povoadas e importantes centros de comércio, trabalho e educação (Oliveira, 2023).

A Linha Amarela possui algumas características que a diferenciam das demais linhas do metrô paulistano:

1. Tecnologia de Ponta: A Linha Amarela foi a primeira linha totalmente automatizada do sistema metroviário brasileiro. Os trens operam sem condutores, utilizando tecnologia de ponta que garante maior segurança e eficiência na operação (Monteiro, 2023).

2. Integração com outras linhas: A linha oferece fácil integração com outras linhas do metrô e da Companhia Paulista de Trens Metropolitanos (CPTM), facilitando a vida dos passageiros que se deslocam por diferentes regiões da cidade (Sant'Anna, 2023).

3. Redução de Tempo de Viagem: Com uma operação eficiente e intervalos menores entre os trens, a Linha Amarela contribui significativamente para a redução do tempo de viagem dos passageiros, melhorando a fluidez do transporte público (Oliveira, 2023).

4. Atendimento a Grandes Polos: A linha atende importantes polos de atração de pessoas, como o bairro de Pinheiros, a Avenida Paulista e a região da Luz, que abriga diversos órgãos públicos e centros culturais (Monteiro, 2023).

5. Capacidade de Transporte: Com trens modernos e estações amplas, a Linha Amarela foi projetada para atender a alta demanda de passageiros, contribuindo para a redução da lotação nas demais linhas do metrô e melhorando a distribuição do fluxo de passageiros na rede (Oliveira, 2023).

A Via Quatro, ao operar a Linha Amarela, desempenha um papel crucial na mobilidade urbana de São Paulo. A eficiência, modernidade e confiabilidade dos serviços prestados são fundamentais para garantir que milhões de paulistanos possam se deslocar de maneira rápida, segura e confortável pela cidade (Oliveira, 2023). A integração da linha com outras modalidades de transporte público também é um fator chave para a conectividade e acessibilidade da rede de transporte, promovendo uma melhor qualidade de vida para os habitantes da grande metrópole brasileira (Sant'Anna, 2023).

A ação judicial movida contra a Via Quatro foi motivada pela coleta de dados pessoais dos passageiros sem o devido consentimento. A Via Quatro utilizou tecnologias de reconhecimento facial nas estações de metrô para capturar dados biométricos dos usuários, supostamente para fins de segurança. No entanto, a ausência de autorização explícita dos passageiros para o tratamento desses dados levantou sérias preocupações sobre a conformidade com a LGPD (Doneda, 2021).

Além da coleta de dados sem consentimento, a ação judicial também revelou que as câmeras de segurança instaladas nas estações de metrô foram utilizadas para fins comerciais e publicitários. A Via Quatro empregou essas câmeras para monitorar e analisar o comportamento dos passageiros, utilizando os dados coletados para direcionar campanhas publicitárias e gerar lucro a partir do perfil dos usuários. Essa prática foi considerada uma violação grave da privacidade dos passageiros, uma vez que os dados foram utilizados para finalidades não autorizadas e alheias à segurança pública (Santos, 2020).

A revelação dessas práticas gerou uma forte reação negativa do público e de órgãos de defesa dos consumidores. Os passageiros expressaram indignação e preocupação com a invasão de sua privacidade e o uso indevido de seus dados pessoais. A situação chamou a atenção de acadêmicos e especialistas em privacidade e proteção de dados, como Doneda (2020) e Mantelero (2017), que argumentaram sobre as implicações legais e éticas da coleta de dados sem consentimento explícito e seu uso para fins comerciais.

Danilo Doneda (2020), um dos principais especialistas em privacidade e proteção de dados no Brasil, destacou que a coleta de dados biométricos sem consentimento e seu uso para fins comerciais violam a LGPD e os direitos fundamentais dos cidadãos. Doneda ressalta a necessidade de transparência e consentimento explícito no tratamento de dados pessoais, bem como a importância de limitar a coleta de dados apenas ao estritamente necessário para a finalidade declarada, no caso, a segurança dos passageiros.

Belli (2021), especialista em governança da internet e proteção de dados, também enfatizou a importância de uma abordagem rigorosa na aplicação da LGPD. Belli argumenta que a intervenção ativa de organizações de defesa dos direitos dos consumidores e a aplicação rigorosa da LGPD são essenciais para proteger a privacidade dos cidadãos e assegurar que as práticas de coleta de dados sejam transparentes e respeitem os direitos fundamentais dos indivíduos.

A decisão da 8ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo (TJSP) contra a Via Quatro foi fundamentada em princípios essenciais da Lei Geral de Proteção de Dados Pessoais (LGPD). A análise dos fundamentos da decisão revela a aplicação rigorosa da legislação brasileira de proteção de dados, destacando pontos cruciais que servem como precedentes para futuros casos similares (Mantelero, 2017).

Um dos pilares da decisão foi a proibição da coleta de dados pessoais sem a devida autorização dos titulares. A Via Quatro, ao implementar tecnologias de reconhecimento facial sem obter o consentimento prévio dos passageiros, violou um dos princípios básicos da LGPD. A coleta de dados pessoais sem autorização explícita configura uma grave infração, uma vez que compromete a privacidade dos indivíduos e contraria o direito fundamental de proteção de seus dados pessoais (Doneda, 2020).

Outro fundamento central da decisão foi a ênfase na necessidade de consentimento explícito para o tratamento de dados pessoais. A LGPD estipula que o tratamento de dados pessoais deve ser realizado com base em uma das hipóteses legais previstas, sendo o consentimento explícito um dos principais fundamentos. No caso da Via Quatro, a ausência de consentimento dos passageiros para a coleta e o uso de seus dados biométricos tornou a prática

ilegal. O Tribunal destacou que o consentimento deve ser informado, inequívoco e fornecido de forma livre pelos titulares dos dados (Belli, 2021).

A decisão judicial também abordou o uso indevido de câmeras de segurança pela Via Quatro. As câmeras, inicialmente instaladas para fins de segurança, foram utilizadas para fins comerciais e publicitários, o que configura uma clara violação dos princípios da LGPD. A lei exige que o tratamento de dados pessoais seja realizado para finalidades específicas, legítimas e claramente informadas aos titulares. No caso da Via Quatro, o desvio da finalidade original das câmeras de segurança, sem o consentimento dos passageiros, foi considerado uma violação dos princípios de finalidade específica e consentimento (Mantelero, 2017).

O Tribunal sublinhou que a utilização de dados pessoais para finalidades diferentes daquelas para as quais foram originalmente coletados requer um novo consentimento dos titulares. A falta de transparência na comunicação das finalidades do tratamento de dados e o desrespeito à necessidade de um consentimento específico foram pontos cruciais na fundamentação da decisão (Doneda, 2020).

A decisão da 8ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo (TJSP) teve importantes repercussões financeiras para a Via Quatro. Inicialmente, a concessionária foi condenada ao pagamento de R$ 100 mil a título de dano moral coletivo. No entanto, a gravidade das violações à LGPD e a necessidade de um maior impacto punitivo e dissuasório levaram ao aumento do valor para R$ 500 mil. Este aumento significativo no valor da indenização reflete a seriedade com que o tribunal tratou a violação dos direitos de privacidade dos passageiros e a importância de assegurar o cumprimento rigoroso da LGPD (Doneda, 2018).

A indenização de R$ 500 mil foi destinada ao Fundo de Defesa de Direitos Difusos (FDD), um fundo administrado pelo Ministério da Justiça e Segurança Pública. O FDD tem como objetivo financiar projetos que visem à reparação de danos ao meio ambiente, ao patrimônio público e a outros interesses difusos e coletivos. A reversão da indenização para o FDD garante que os recursos sejam utilizados em prol da sociedade, promovendo ações que beneficiem a coletividade e reforcem a proteção dos direitos dos consumidores (Bioni, 2021).

O Instituto Brasileiro de Defesa do Consumidor (Idec) foi um dos principais intervenientes no caso, defendendo a proibição da coleta e tratamento de dados biométricos sem a autorização prévia dos titulares. O Idec argumentou que a prática da Via Quatro de utilizar reconhecimento facial sem o consentimento explícito dos passageiros violava diretamente os princípios da LGPD, especialmente no que se refere à necessidade de consentimento informado e à finalidade específica do tratamento de dados. O Idec destacou a importância de proteger a

privacidade dos consumidores e de assegurar que as práticas de coleta de dados sejam transparentes e respeitem os direitos fundamentais dos indivíduos (Monteiro, 2021).

Em sua defesa, a Via Quatro alegou a irretroatividade da LGPD, argumentando que as práticas de coleta de dados ocorreram antes da plena vigência da lei e, portanto, não deveriam ser julgadas sob seus preceitos. Além disso, a empresa sustentou que a mera detecção de imagens não constituía tratamento de dados pessoais conforme definido pela LGPD (Cardozo, 2021). A Via Quatro tentou minimizar a gravidade das acusações, alegando que as práticas adotadas eram necessárias para a segurança e eficiência operacional da Linha Amarela (Cardozo, 2018).

O relator do caso no TJSP, ao analisar os argumentos das partes, considerou a falta de provas apresentadas pela Via Quatro para justificar a necessidade e a legalidade do tratamento de dados biométricos sem consentimento. O relator destacou que a empresa não conseguiu demonstrar de maneira convincente que as práticas adotadas eram essenciais para a segurança ou que haviam sido implementadas de acordo com os princípios da LGPD. Em sua decisão, o relator confirmou a violação dos direitos dos passageiros e a necessidade de aplicação das sanções previstas na legislação de proteção de dados (Bioni, 2021).

A decisão judicial contra a Via Quatro e suas consequências destacam a relevância e a aplicação prática da Lei Geral de Proteção de Dados Pessoais (LGPD) no contexto da administração pública e das organizações que operam em parceria com o setor público. Este caso exemplifica como a LGPD deve ser implementada para proteger os direitos dos titulares de dados pessoais e garantir que as práticas de coleta e tratamento de dados sejam conduzidas de maneira ética e legal (Doneda, 2021).

Uma das principais lições aprendidas com este caso é a reafirmação da importância do consentimento explícito dos titulares de dados pessoais. A LGPD exige que qualquer coleta e tratamento de dados pessoais sejam realizados com base em uma das hipóteses legais previstas, sendo o consentimento uma das mais fundamentais. No caso da Via Quatro, a ausência de consentimento explícito dos passageiros para a coleta de dados biométricos configurou uma violação direta da LGPD. Esta situação sublinha a necessidade de que todas as entidades, públicas ou privadas, obtenham o consentimento claro e informado dos indivíduos antes de procederem com a coleta e tratamento de seus dados pessoais (Monteiro, 2021).

A transparência é outro princípio crucial destacado pela LGPD, e a decisão judicial contra a Via Quatro reforça sua importância. As organizações devem informar claramente os titulares dos dados sobre quais informações estão sendo coletadas, para quais finalidades serão usadas, e quais medidas de segurança estão sendo implementadas para proteger esses dados. A

falta de transparência nas práticas da Via Quatro levou a um uso indevido dos dados pessoais dos passageiros, violando não apenas a confiança dos usuários, mas também as disposições legais (Bioni, 2021).

Além disso, a segurança no tratamento de dados pessoais é uma exigência crítica da LGPD. As organizações precisam adotar medidas adequadas para proteger os dados contra acessos não autorizados, vazamentos e outras formas de processamento ilegal. No caso da Via Quatro, a inadequada proteção e uso dos dados coletados resultou em consequências legais e financeiras significativas (Doneda, 2021).

A decisão da 8ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo (TJSP) contra a Via Quatro estabelece um precedente importante para a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Este caso demonstra como os tribunais estão dispostos a aplicar rigorosamente as disposições da LGPD para garantir a proteção dos direitos dos titulares de dados. Ao impor uma penalidade significativa à Via Quatro e aumentar o valor do dano moral coletivo, a decisão envia uma mensagem clara de que violações à LGPD não serão toleradas. Este precedente é crucial para orientar futuras decisões judiciais e para incentivar as empresas a adotarem práticas de conformidade com a legislação de proteção de dados (Bioni, 2021).

A decisão judicial sublinha a responsabilidade das empresas na proteção dos dados pessoais dos cidadãos. As organizações que operam no Brasil, sejam elas públicas ou privadas, devem estar cientes de suas obrigações sob a LGPD e garantir que suas práticas de coleta e tratamento de dados estejam em conformidade com a lei. A Via Quatro, ao não obter o consentimento explícito dos passageiros e ao utilizar dados biométricos para finalidades não autorizadas, falhou em proteger a privacidade dos indivíduos. Este caso ressalta a necessidade de as empresas implementarem políticas de privacidade claras, realizarem avaliações de impacto à proteção de dados e adotarem medidas de segurança eficazes para proteger os dados pessoais que coletam e tratam (Doneda, 2021).

O tratamento rigoroso das violações à LGPD pela justiça brasileira é outro impacto significativo da decisão contra a Via Quatro. A imposição de uma multa elevada e a determinação de que a indenização seja revertida para o Fundo de Defesa de Direitos Difusos (FDD) refletem a seriedade com que o tribunal abordou o caso. Esta abordagem rigorosa serve como um aviso para outras empresas sobre as consequências legais e financeiras de não cumprirem com a LGPD. A decisão demonstra que a justiça brasileira está comprometida em garantir que os direitos de privacidade dos cidadãos sejam respeitados e que qualquer desrespeito às disposições da LGPD será severamente penalizado (Monteiro, 2021).

Esse caso da Via Quatro é um exemplo notável de governo eletrônico, onde a digitalização e o uso de tecnologias de informação e comunicação (TICs) impactam significativamente a administração pública e a prestação de serviços. A implementação de tecnologias de reconhecimento facial pela Via Quatro, apesar de controversa, reflete a tendência de modernização e digitalização dos serviços públicos, visando eficiência e segurança. Contudo, a falta de conformidade com a LGPD sublinha a importância de equilibrar inovação tecnológica com a proteção dos direitos fundamentais dos cidadãos. Como ressalta Luciano Floridi, 'a proteção da privacidade é um dos pilares da sociedade da informação, e a governança de dados deve sempre buscar um equilíbrio entre inovação e direitos fundamentais (Floridi, 2014).

A necessidade do consentimento explícito, a transparência nas práticas de coleta e tratamento de dados e a segurança no manejo dessas informações são princípios centrais da LGPD que devem ser observados rigorosamente. A decisão judicial contra a Via Quatro reflete a importância de respeitar esses princípios, estabelecendo um precedente crucial para garantir que as tecnologias emergentes sejam implementadas de maneira ética e legal, protegendo a privacidade e os direitos dos indivíduos. Como destaca Doneda, a efetiva proteção de dados pessoais depende da observância rigorosa dos princípios de transparência, consentimento e segurança, que são essenciais para a confiança e a proteção dos direitos fundamentais em uma sociedade cada vez mais digitalizada (Doneda, 2020).

Autores como Doneda (2020) e Wimmer (2019) destacam a importância de um equilíbrio entre transparência e proteção de dados na administração pública, enfatizando a necessidade de políticas claras e práticas responsáveis para garantir a confiança dos cidadãos nas instituições públicas. A intervenção do Idec e a aplicação rigorosa da LGPD neste caso sublinham a relevância de uma fiscalização ativa e da adoção de medidas rigorosas para proteger os dados pessoais dos cidadãos, promovendo uma governança de dados mais segura e transparente.

5 CONCLUSÃO

O estudo responde de maneira abrangente ao questionamento sobre como é concedido o tratamento de dados pessoais pela administração pública quando do fornecimento de um serviço público à luz da LGPD, visto que este aborda a implementação prática da LGPD, utilizando o caso da Via Quatro e a decisão judicial da 8ª Câmara de Direito Público do TJSP como exemplos de como a LGPD deve ser inovadora na prática. Além disso, destaca a importância de seguir os princípios estabelecidos pela LGPD, especialmente em relação à coleta e tratamento de dados pessoais, incluindo a exigência de consentimento explícito dos titulares dos dados e a necessidade de transparência no uso de tecnologias de monitoramento.

A análise do caso da Via Quatro e a decisão da 8ª Câmara de Direito Público do Tribunal de Justiça do Estado de São Paulo (TJSP) fornecem lições valiosas sobre a aplicação prática da Lei Geral de Proteção de Dados Pessoais (LGPD) na administração pública e no setor privado.

O caso Via Quatro serve como um exemplo claro de como a LGPD deve ser implementada na prática. A decisão judicial destacou a importância de seguir os princípios estabelecidos pela LGPD, especialmente no que diz respeito à coleta e tratamento de dados pessoais. A exigência de consentimento explícito dos titulares de dados e a necessidade de transparência no uso de tecnologias de monitoramento, como câmeras de segurança, são aspectos essenciais que devem ser observados rigorosamente por todas as entidades públicas e privadas.

O respeito às diretrizes da LGPD é fundamental para proteger os direitos de privacidade e liberdade dos cidadãos. A lei estabelece um framework que garante que os dados pessoais sejam tratados de maneira ética e segura. Este caso enfatiza que a obtenção de consentimento claro e informado é crucial para o processamento de dados pessoais. Além disso, a transparência nas práticas de coleta e uso de dados reforça a confiança do público nas instituições que manuseiam suas informações pessoais.

As consequências da violação da LGPD são severas, tanto do ponto de vista legal quanto financeiro. A decisão contra a Via Quatro, que aumentou a indenização por dano moral coletivo para R$ 500 mil e destinou esse valor ao Fundo de Defesa de Direitos Difusos (FDD), serve como um aviso contundente para outras empresas. As penalidades não apenas implicam em multas significativas, mas também em danos reputacionais que podem ter um impacto duradouro nas operações das empresas. A justiça brasileira demonstrou seu compromisso em aplicar rigorosamente a LGPD, assegurando que qualquer violação dos direitos de privacidade dos cidadãos seja adequadamente punida.

A necessidade contínua de conscientização e adequação às normas de proteção de dados pessoais é crucial em projetos de infraestrutura pública, como a Linha 4 do Metrô de São Paulo. Com a implementação crescente de tecnologias avançadas para melhorar a eficiência e a segurança do transporte público, surge também a necessidade de garantir que os dados dos usuários sejam protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD).

A conscientização sobre a proteção de dados é essencial para todos os envolvidos no projeto, desde gestores até funcionários operacionais. Isso inclui treinamentos regulares sobre as melhores práticas de segurança da informação e a importância de proteger dados pessoais. A LGPD impõe obrigações rigorosas sobre como os dados pessoais devem ser coletados, armazenados e utilizados, e a não conformidade pode resultar em penalidades significativas. Portanto, é fundamental que todos os stakeholders estejam cientes dessas responsabilidades e adotem medidas proativas para assegurar a conformidade contínua.

A relevância das decisões judiciais e administrativas em relação à proteção de dados no contexto da Linha 4 do Metrô de São Paulo não pode ser subestimada. Tais decisões servirão como precedentes importantes para futuras interpretações e aplicações da LGPD no Brasil. Por exemplo, um caso recente envolvendo a coleta e uso de dados biométricos dos passageiros pode definir padrões sobre como esses dados devem ser tratados em termos de consentimento, finalidade e segurança.

Decisões judiciais bem fundamentadas podem fornecer clareza sobre aspectos ainda ambíguos da LGPD, orientando as empresas e entidades públicas sobre as melhores práticas para garantir a privacidade e a proteção dos dados pessoais. Essas decisões também podem ajudar a moldar a política pública e a regulamentação, promovendo um ambiente onde a inovação tecnológica e a proteção de dados caminham lado a lado.

Para a Linha 4 do Metrô de São Paulo, isso significa que cada decisão tomada em relação à gestão de dados pessoais deve considerar não apenas a conformidade com a LGPD, mas também o impacto potencial dessas decisões em futuros projetos de infraestrutura. A implementação de tecnologias como sistemas de reconhecimento facial ou plataformas de bilhetagem eletrônica deve ser cuidadosamente planejada e executada com um foco claro na proteção de dados.

REFERÊNCIAS

ACQUISTI, Alessandro. A tensão entre transparência e privacidade representa um dos desafios mais críticos na era da informação. In: **The Economics of Personal Data and the Economics of Privacy**. 2. ed. New York: Springer, 2014.

ANPD. **Autoridade Nacional de Proteção de Dados**. 2022. Disponível em: https://www.gov.br/anpd/pt-br. Acesso em: 10 jun. 2024.

BIONI, Bruno. A LGPD estabelece um equilíbrio fundamental entre a transparência governamental e a proteção de dados pessoais reconhecendo a importância da autodeterminação informativa em uma sociedade digitalizada e a necessidade de mecanismos de responsabilização claros para os controladores de dados. In: **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. São Paulo: RT, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 jun. 2024.

BRASIL. **Decisão do Supremo Tribunal Federal sobre a proteção de dados pessoais como direito fundamental**. 2023. Disponível em: http://www.stf.jus.br. Acesso em: 10 jun. 2024.

BRASIL. **Emenda Constitucional nº 115 de 10 de fevereiro de 2022**. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 12 jun. 2024.

BRASIL. **Julgamento das Ações Diretas de Inconstitucionalidade (ADIs) n.º 6387, 6388, 6389, 6390 e 6393 pelo Supremo Tribunal Federal**. 2023. Disponível em: http://www.stf.jus.br. Acesso em: 12 jun. 2024.

BRASIL. **Julgamento do MS n.º 21.729/DF e do RE n.º 418.416-8/SC pelo Supremo Tribunal Federal**. 2015. Disponível em: http://www.stf.jus.br. Acesso em: 05 jun. 2024.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709 de 14 de agosto de 2018. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 jun. 2024.

BRASIL. **Medida Provisória nº 954 de 17 de abril de 2020**. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 23 jun. 2024.

BRASIL. **Projeto de Lei do Senado nº 330 de 13 de agosto de 2013**. 2013. Disponível em: http://www.senado.leg.br/atividade/materia/getTexto.asp?t=145682&tp=1. Acesso em: 09 jun. 2024.

BRASIL. **Projeto de Lei nº 4.060 de 13 de junho de 2012**. 2012. Disponível em: http://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=540400. Acesso em: 12 jun. 2024.

CABRAL, A. B. **Administração Pública e Transparência**. Rio de Janeiro: FGV, 2020.

CARVALHO FILHO, J. M. **Manual de Direito Administrativo**. São Paulo: Atlas, 2019.

CONJUR. **Uso de Tecnologias de Reconhecimento Facial e LGPD**: O Caso Via Quatro. 2020. Disponível em: http://www.conjur.com.br. Acesso em: 12 jun. 2024.

CPTM. **Companhia Paulista de Trens Metropolitanos**. 2023. Disponível em: http://www.cptm.sp.gov.br. Acesso em: 10 jun. 2024.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. Rio de Janeiro: Renovar, 2020.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2011.

EXAME. **Decisão do TJSP no Caso Via Quatro e a Aplicação da LGPD**. 2021. Disponível em: http://www.exame.com. Acesso em: 01 jun. 2024.

FOUCAULT, Michel. Onde há poder há resistência. In: **Microfísica do Poder** 4. ed. Rio de Janeiro: Graal, 1978.

IDEC. **Instituto Brasileiro de Defesa do Consumidor**. 2021. Disponível em: http://www.idec.org.br. Acesso em: 01 jun. 2024.

JOTA. **Caso Via Quatro**: Reconhecimento Facial e a LGPD. 2023. Disponível em: http://www.jota.info. Acesso em: 13 jun. 2024.

LORENZON, M. **Princípios de Segurança da Informação**. Curitiba: Juruá, 2021.

MALDONADO, P.; BLUM, J. **Transferência Internacional de Dados**. Florianópolis: Habitus, 2020.

MARETTI, F.; MONROE, J. **Governança e Proteção de Dados**. Belo Horizonte: Del Rey, 2020.

MENDES, Gilmar Ferreira. A transparência é um princípio fundamental da administração pública e um elemento essencial para a democracia. In: **Direitos Fundamentais e Controle de Constitucionalidade**. 2. ed. São Paulo: Saraiva, 2018.

MENDES, Laura Schertel. A LGPD inaugura um novo patamar de proteção de dados pessoais no Brasil ao reconhecer que a proteção de dados é um direito fundamental e ao mesmo tempo ao atribuir responsabilidades claras e rigorosas aos controladores e operadores de dados. Esta lei reflete um avanço significativo na direção de uma governança robusta e transparente dos dados pessoais. In: **Direito e Tecnologia**. 3. ed. Rio de Janeiro: Elsevier, 2019.

METRÔ DE SÃO PAULO. **Linha 4-Amarela**. 2020. Disponível em: http://www.metro.sp.gov.br. Acesso em: 01 jun. 2024.

MUNÕZ, R.; MAZA, J. **Proteção de Dados na Era Digital**. Porto Alegre: Síntese, 2020.

OLIVEIRA, M. R. **Proteção de Dados Pessoais**. São Paulo: Atlas, 2008.

RAMOS, João. Reconhecimento Facial e Privacidade: Desafios Jurídicos. **Revista Brasileira de Direito Digital**, v. 5, n. 2, p. 45-67, 2020.

SCHIEFLER, G. A. **Direito à Informação**: Aspectos Jurídicos da Transparência Administrativa. São Paulo: Saraiva, 2013.

SILVA, D. **Comentários à Constituição de 1988**. São Paulo: Malheiros, 1994.

SILVA, V. A. **Direito Digital e Proteção de Dados**. Brasília: Thesaurus, 2020.

VIA QUATRO. **Sobre a Via Quatro**. 2024. Disponível em: http://www.viaquatro.com.br. Acesso em: 01 jun. 2024.

WIMMER, Miriam. A boa governança em matéria de dados pessoais implica não apenas a proteção e a segurança dos dados, mas também a transparência e a prestação de contas das atividades dos controladores especialmente no setor público onde a confiança dos cidadãos é fundamental. In: **Governança Digital**: Princípios e Práticas. Brasília: ENAP, 2020.