A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E O COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS PÚBLICOS

THE GENERAL PERSONAL DATA PROTECTION LAW AND DATA SHARING AMONG PUBLIC AGENCIES

Gabriela Calábria Araújo Moraes dos Santos[1]

ISBN: 978-85-7872-854-0
DOI: 10.56089/978-85-7872-854-0

RESUMO

O artigo examina a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), e seus reflexos no compartilhamento de dados pessoais entre órgãos públicos. Analisam-se os conceitos e princípios da lei, as regras do Capítulo IV sobre o tratamento de dados pelo poder público e a exigência de interoperabilidade prevista no art. 25. Em seguida, estuda-se a interpretação conferida pelo Supremo Tribunal Federal no julgamento conjunto da ADI nº 6.649/DF e da ADPF nº 695/DF, que fixou parâmetros para o compartilhamento de dados no âmbito da Administração Pública Federal. Por fim, aborda-se a Lei nº 14.129/2021 e sua relação com o compartilhamento de dados protegidos por sigilo fiscal, nos termos do art. 198 do Código Tributário Nacional. A pesquisa, de natureza bibliográfica, documental e jurisprudencial, conclui que o uso compartilhado de dados pessoais entre órgãos públicos é legítimo e favorece a eficiência administrativa, desde que vinculado a finalidade específica, limitado ao mínimo necessário e acompanhado da preservação do sigilo e de mecanismos de segurança e responsabilização.

Palavras-chave: LGPD; proteção de dados pessoais; compartilhamento de dados; interoperabilidade; Administração Pública.

ABSTRACT

This article examines Law No. 13.709/2018, the General Data Protection Law (LGPD), and its implications for the sharing of personal data between public bodies. It analyzes the concepts and principles of the law, the rules of Chapter IV on the processing of data by public authorities, and the interoperability requirement stipulated in Article 25. Next, it studies the interpretation given by the Supreme Federal Court in the joint judgment of

[1] Gabriela Calábria, Advogada, graduada em Direito pela Universidade Federal de Pernambuco, especialista em Direito Administrativo, Assessora Jurídica no Tribunal de Contas de Pernambuco.

ADI No. 6.649/DF and ADPF No. 695/DF, which established parameters for data sharing within the Federal Public Administration. Finally, it addresses Law No. 14.129/2021 and its relationship with the sharing of data protected by tax secrecy, under the terms of Article 198 of the National Tax Code. This research, of a bibliographical, documentary, and jurisprudential nature, concludes that the shared use of personal data among public bodies is legitimate and favors administrative efficiency, provided it is linked to a specific purpose, limited to the minimum necessary, and accompanied by the preservation of confidentiality and security and accountability mechanisms.

Keywords: LGPD; personal data protection; data sharing; interoperability; Public Administration.

INTRODUÇÃO

A Administração Pública é uma das maiores detentoras de dados pessoais do país. Para prestar serviços, executar políticas públicas e fiscalizar o cumprimento da lei, os órgãos públicos coletam e tratam diariamente informações sobre milhões de cidadãos.

O compartilhamento dessas informações entre os órgãos confere maior eficiência à atuação estatal. Contudo, quando envolve dados pessoais, essa prática precisa ser compatibilizada com a proteção de dados, elevada à condição de direito fundamental pela Emenda Constitucional nº 115/2022.

A Lei nº 13.709/2018 (LGPD) ocupa posição central nesse debate. Além de estabelecer princípios e regras gerais, a lei dedica um capítulo específico ao tratamento de dados pelo poder público e disciplina o uso compartilhado de dados entre órgãos e entidades públicas.

Diante desse cenário, o objetivo deste artigo é analisar em que condições a LGPD admite o compartilhamento de dados pessoais entre órgãos públicos e quais deveres são impostos aos entes envolvidos. A pesquisa adota metodologia bibliográfica, documental e jurisprudencial.

Para tanto, o estudo examina, inicialmente, os conceitos e princípios da LGPD e as regras do seu Capítulo IV. Em seguida, aborda o art. 25 e o conceito de interoperabilidade. Na sequência, analisa o julgamento da ADI nº 6.649/DF e da ADPF nº 695/DF pelo STF. Por fim, trata da Lei nº 14.129/2021 e do compartilhamento de dados protegidos por sigilo fiscal.

Sabe-se que o tratamento de dados pessoais pelo poder público guarda uma série de peculiaridades, decorrentes da necessária compatibilização entre o exercício de prerrogativas estatais típicas e os princípios estabelecidos no ordenamento jurídico vigente.

Por meio da Emenda Constitucional nº 115/2022, alterou-se a Constituição para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, acrescendo ao texto do art. 5º o seguinte inciso LXXIX: “é assegurado, nos termos da

lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

O tratamento de dados pessoais não é tema novo, contudo, o processamento desses dados pelo Estado brasileiro vinha sendo negligenciado. No desempenho das atividades públicas, a Administração passa a ser detentora de milhares de dados, sendo imprescindível a sua proteção, sem, no entanto, impossibilitar o seu compartilhamento entre os órgãos públicos. É por meio dessa troca que se confere maior eficiência ao labor estatal, como já mencionado (Coutinho; Marcon, 2023, p. 164-165).

Fixou-se, também, por meio da retromencionada EC, a competência da União para legislar sobre a proteção e tratamento de dados pessoais (art. 21, XXVI). Nesse contexto, ganha relevância a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), ainda mais quando analisado o compartilhamento de dados sigilosos entre órgãos públicos.

Por meio de legislações de tamanha magnitude e pertinência, evidencia-se a fundamental importância do direito administrativo à concretização do direito constitucional: ao passo em que o segundo traceja as linhas estruturais da organização estatal, o primeiro, de forma dinâmica, satisfaz os comandos constitucionais por meio da regulamentação de atividades (Nobre Júnior, 2020, p. 19), como no caso da proteção de dados pessoais.

De tal maneira, o poder público adequa-se à nova realidade na medida em que, com a crescente necessidade de tratamento dos dados pessoais, deve, também, garantir a concreta proteção desses dados (Coutinho; Marcon, 2023, p. 163).

A LGPD, de 14 de agosto de 2018, versa sobre o tratamento de dados pessoais inseridos em bases de dados digitais, os quais ostentam a natureza de acesso restrito por razões que serão oportunamente evidenciadas:

> Art. 1º 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.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

A fim de traçar uma melhor resposta para as indagações às quais essa pesquisa pretende responder, é essencial a análise de certos dispositivos da LGPD, com ênfase nos que tratam do compartilhamento de dados entre instituições públicas, decerto que os dados a que se refere são os de titularidade de pessoas naturais que gozam do direito à privacidade e livre desenvolvimento, o que não é o caso das pessoas jurídicas de direito público.

Ressalve-se, desde já, que a LGPD não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, ou atividades de investigação e repressão de infrações penais (art. 4º, III, *d*), não sendo esse, de igual modo, o objeto do presente estudo, que excetua o compartilhamento de

dados sigilosos para fins de segurança pública, *lato sensu*.

O art. 5º da Lei 13.709/2018 é o responsável por definir fundamentais conceitos para sua plena compreensão, sendo os principais:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> [...]
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> [...]
>
> IX - agentes de tratamento: o controlador e o operador; [...]
>
> XVI - uso compartilhado de dados: 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;
>
> [...]
>
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A legislação pressupõe, portanto, o uso compartilhado de bancos de dados pessoais por órgãos e entidades públicas, desde que no cumprimento de suas competências legais e mediante autorização específica para uma das modalidades de tratamento pré-existentes. Ademais, além das posições de controlador e operador, ambos considerados agentes de tratamento de dados, existe a figura da Autoridade

Nacional de Proteção de Dados (ANPD), órgão da Administração Pública responsável pelo fiel cumprimento da LGPD no Brasil, entre outras funções.

Destaque-se que os dados anonimizados, considerando a impossibilidade de identificação do titular dos dados, não se confundem com os dados pessoais, exceto nas hipóteses em que o processo de anonimização for ou puder ser revertido (art. 12 da Lei nº 13.709/2018). Tratam-se de informações distintas e às quais não será dado enfoque.

O art. 6º da LGPD estabelece os princípios que devem reger a atividade de tratamento de dados pessoais. Destaque-se os mais relevantes: boa-fé, finalidade, propósito legítimo, específico, explícito, adequação, necessidade, segurança dos dados e prevenção da ocorrência de danos.

Somado a isso, o art 7º autoriza o tratamento de dados pessoais pela Administração Pública, assim como o uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, sem a necessidade de consentimento do titular (art. 11, II, *b*).

Reservou-se o Capítulo IV da Lei para disciplinar o tratamento específico de dados pessoais pelo poder público.

REFLEXÕES SOBRE O CAPÍTULO IV DA LEI Nº 13.709/2018

Inicialmente, rememore-se que, nos termos do art. 31, § 1º, I, da Lei nº 12.527/2011, o tratamento das informações pessoais que se referem à intimidade, vida privada, honra e imagem terão o seu acesso restrito, independente de classificação posterior de sigilo, desde a data da sua produção.

Fazendo menção à LAI, o art. 23 da LGPD permite o tratamento de dados pessoais por instituições públicas para a execução de suas competências legais ou para o cumprimento de atribuições legais do serviço, não desobrigando os agentes de tratamento da observância dos princípios gerais e da garantia dos direitos dos titulares das informações:

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

> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e
> IV - (VETADO).
>
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
>
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Do colacionado extrai-se a necessidade de informação das hipóteses de realização de tratamento de dados pessoais, conforme previsão legal, e de indicação de um encarregado para o tratamento dos dados pessoais, cabendo à ANPD dispor sobre as formas de publicidade das operações de tratamento.

Ainda segundo a norma, os mesmos princípios gerais também precisam ser observados no caso de compartilhamento de dados pessoais pelo poder público, o que, para além da admissão, recebe considerável enfoque pela Lei nº 13.709/2018:

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

O compartilhamento de que trata a LGPD, consoante previamente mencionado, envolve a comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais (art. 5º, XVI), para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III):

> (há a) possibilidade do compartilhamento dos dados pessoais pelos órgãos entre si, mediante a observância de critérios como propósitos legítimos, específicos e explícitos sobre o seu tratamento, limitado ao mínimo indispensável ao atendimento do interesse público e em estrita observância à LGPD. (Borges; Monte, 2023, p. 147)

No tocante ao compartilhamento de informações e a primazia do interesse público, Nobre Júnior (2019, p. 53) afirma que se tem valorizado, principalmente no estrangeiro, a constatação da presença do interesse público no plano real, o que vai além da mera abstração legal.

Nos termos do art. 30 da Lei nº 13.709/2018, a ANPD poderá estabelecer normas complementares para o uso compartilhado de dados pessoais, cabendo

também a ela, de acordo com o art. 55-J, zelar pela observância da proteção de dados pessoais, do sigilo das informações quando protegidos por lei, ou quando a quebra do sigilo violar os fundamentos do art. 2º da LGPD: o respeito à privacidade (inciso I), a autodeterminação informativa (inciso II), a inviolabilidade da intimidade, da honra, da imagem (inciso IV), os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (inciso VII), entre outros.

Os arts. 46, 47 e 49 exigem a adoção, por todos os agentes de tratamento de dados, de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais em posse do poder público, o que inclui, decerto, os órgãos públicos receptores das informações em um processo de compartilhamento de dados restritos:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
>
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Ficam os dados pessoais, portanto, disponíveis tão somente aos agentes autorizados para tratamento. Evita-se, dessa forma, a utilização de informações pessoais de forma inadequada ou, de maior gravidade, ilícita. A proteção de dados pessoais é um direito fundamental essencial na sociedade moderna, amparado pela Constituição, e que merece atenção em todos os processos de compartilhamento de informações entre órgãos públicos, sendo a privacidade um bem jurídico que recebe a proteção do Estado como forma de cumprimento do escopo de resguardo da sociedade e primazia do interesse público.

O vazamento de informações ou o uso dos dados para fins diversos do que se designou de início deve resultar em uma responsabilização administrativa do agente público, podendo servir, inclusive, como fundamento para pedidos de indenização por danos morais (Coutinho; Marcon, 2023, p. 170).

Aponte-se, ainda que brevemente, que parte da doutrina discorda da utilização da expressão “proteção de dados”, considerando que ela não reproduz, de forma fiel, a essência da disciplina: “não são os dados que são protegidos, mas a pessoa à qual se referem” (Doneda, 2003, p. 118).

Para finalizar a seção, ressalte-se que o conteúdo do art. 25 da LGPD exige que os dados pessoais sejam mantidos em “formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas e à prestação de serviços públicos”, merecendo proeminência.

O ART. 25 DA LGPD E O CONCEITO DA INTEROPERABILIDADE NA CRIAÇÃO DE PLATAFORMAS DE COMPARTILHAMENTO DE DADOS

“Substantivo femino. Qualidade do que é interoperável. Capacidade de um sistema para interagir e comunicar com outro.”[2] O conceito de interoperabilidade apresentado pelo Dicionário Priberam da Língua Portuguesa introduz, com precisão, o objeto do presente subtópico.

Trata-se, destarte, de conceito que afirma a necessidade dos sistemas desenvolvidos pelos órgãos públicos serem compatíveis e utilizáveis por todas as possíveis entidades que integram o processo de cooperação e titularizam o compartilhamento de dados entre órgãos públicos.

Reitere-se que aqui se analisa as plataformas interoperáveis de compartilhamento entre entes que compõem a Administração Pública, não sendo objeto de interesse as que promovam o acesso dos cidadãos a dados abertos. Sobre essas, há alguns anos, o Brasil vem adotando instrumentos verdadeiramente inovadores que simplificam o cotidiano dos administrados. Faltam, porém, tecnologias interoperáveis que permitam o intercâmbio de informações entre os órgãos públicos.

Não apenas no art. 25 da LGPD se faz menção à interoperabilidade no ordenamento jurídico nacional, tendo o conceito sido devidamente regulamentado por meio do retromencionado Decreto nº 10.046/2019.

Trata-se do decreto responsável por, entre outras finalidades, melhor conceituar o que se chama de “interoperabilidade”, o que define como sendo a “capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais troquem dados” (art. 2º, XVIII). Nos termos do normativo, tal capacidade pode ser adquirida por meio de plataformas de interoperabilidade, que são o “conjunto de ambientes e ferramentas tecnológicas, com acesso controlado, para o compartilhamento de dados da administração pública federal entre órgãos e entidades especificados no art. 1º” (art. 2º, XXI).

Essa necessária interconexão entre sistemas é uma das mais delicadas e problemáticas características dentro da estrutura administrativa brasileira. Em verdade, apesar das diversas menções na legislação nacional, a depender do contexto, a

[2] Disponível em: https://dicionario.priberam.org/interoperabilidade. Acesso em: 01 jul. 2023.

interoperabilidade não passa de letra morta (Santanna, 2022, p. 69), dificultando o processo de cruzamento de informações e o consequente compartilhamento de dados entre órgãos públicos.

Nos tempos atuais, com o crescente processo de modernização da Administração Pública, que passa a ser digital, ainda não existem programas ou políticas consolidadas para colocar em prática esse atributo que é um dos vértices dessa Administração Pública eletrônica. Permanece a mentalidade de implantação de sistemas isolados para o *e-Gov*, dificultando o estabelecimento de sistemas em rede que favoreçam a real existência de um poder público cuja prioridade seja a colaboração administrativa entre suas estruturas, facilitando o compartilhamento de informações (Santanna, 2022, p. 70-71).

O estreitamento das relações entre entidades públicas por meio de sistemas interoperáveis, ou seja, integrados, tecnicamente compatíveis, seja para fins sociais, públicos ou arrecadatórios, dificulta o cometimento de ilícitos e aperfeiçoa a eficiência estatal, (Santanna, 2022, p. 71), devendo ser o elemento prioritário para quem pretende aprimorar o compartilhamento de dados entre órgãos públicos, em especial o compartilhamento de informações classificadas.

Isso porque, considerando o dever de proteção do sigilo atribuído aos dados classificados, sistemas interoperáveis facilitam a garantia da segurança da informação por meio de plataformas que conseguem ser acessadas pelos agentes sem a necessidade, por exemplo, de uma efetiva transferência da informação, mas apenas de um mero repasse de acesso.

Imperiosa, pois, a reversão do atual cenário brasileiro, para que o escopo do art. 25 seja cumprido e os dados em posse do poder público sejam mantidos em formato interoperável e estruturado para uso compartilhado, como forma, inclusive, de perpetuar a cultura de cooperação entre órgãos, favorecendo o diálogo entre as esferas administrativas. Para Gustavo Santanna (2022, p. 78), a interoperabilidade e a cooperação são duas faces da mesma moeda.

A INTERPRETAÇÃO CONCEDIDA PELA SUPREMA CORTE À LGPD NO COMPARTILHAMENTO DE DADOS SIGILOSOS EM POSSE DA ADMINISTRAÇÃO PÚBLICA: A ADI Nº 6.649/DF E A ADPF Nº 695/DF

Um ponto de partida da jurisprudência do Supremo Tribunal Federal acerca do tema, que merece maior destaque por facilitar a compreensão dos termos básicos em que se deve dar o compartilhamento de dados de acesso restrito entre órgãos públicos, foi o julgamento conjunto da ADI nº 6.649/DF e da ADPF nº 695/DF.

Trata-se de ações ajuizadas, respectivamente, pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB) e pelo Partido Socialista Brasileiro (PSB), sob o argumento de violação do direito à privacidade no compartilhamento de dados pessoais entre órgãos públicos e a inconstitucionalidade do Decreto nº 10.046/2019.

A União, em contrapartida, defende a necessidade do compartilhamento para

uma maior eficiência administrativa, tendo o decreto cumprido a sua finalidade de desburocratização para o desempenho da função pública.

Manifestando-se nos autos, em termos citados nos votos proferidos pelos nobres julgadores, a Advocacia-Geral da União (AGU) aduziu ser "nítida a preocupação do Decreto 10/046/2019 em adotar mecanismos de segurança da informação aptos a garantir o compartilhamento seguro dos dados nas plataformas de interoperabilidade", ponderando que:

> ao reforçar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais, o Decreto 10.046/2019 deixa claro que todo o processo de compartilhamento de dados pessoais deve seguir os mecanismos de segurança da informação nela previstos", razão pela qual "não há falar em omissão por parte do Estado na busca por um compartilhamento seguro de dados pessoais".[3]

Pelo exposto, para além das demais questões processuais e inconstitucionalidades suscitadas, vislumbra-se uma contraposição entre o direito à privacidade e a primazia do interesse público no compartilhamento de dados em posse da Administração Pública Federal.

Conforme previamente delimitado, o foco do presente trabalho é a análise do compartilhamento de dados de acesso restrito sob a ótica da transparência administrativa e os demais termos que devem ser observados pela Administração Pública a um escorreito intercâmbio de informações. Apesar do inerente tangenciamento, o direito à privacidade não é tema de aprofundamento.

Com as atenções direcionadas para a LGPD, em julgamento ocorrido no Plenário do STF no dia 15 de setembro de 2022, conferiu-se interpretação conforme a Constituição ao Decreto nº 10.046/2019, especificando alguns critérios a serem observados pelas instituições para a governança no compartilhamento de dados pessoais, de acesso restrito, no âmbito da Administração Pública Federal. Vide trecho da ementa:

> [...] 3. O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. [...]

Em complemento, restou assim decidido, finalizados os pronunciamentos e

[3] ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15/09/2022, DJe 19/06/2023, p. 10 do acórdão.

realizada a votação do colegiado:

> No mérito, por maioria, julgou parcialmente procedentes os pedidos, conferindo interpretação conforme ao Decreto 10.046/2019, traduzida nos seguintes termos: **1. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.**
>
> 2. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida **publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais,** "fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". 3. O acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes acima arroladas, **cabendo ao Comitê Central de Governança de Dados**, no exercício das competências aludidas nos arts. 21, incisos VI, VII e VIII do Decreto 10.046/2019: 3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem real necessidade de acesso aos dados pessoais nele reunidos. Nesse sentido, a **permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º, inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018**; [...]
>
> **3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.** [...] 5. **O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018**, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo. 6. A transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstasnos estatutos dos servidores públicos federais, municipais e estaduais. **Por fim, o Tribunal declarou, com efeito pro futuro, a inconstitucionalidade do art. 22 do Decreto 10.046/19**, preservando a atual estrutura do Comitê Central de Governança de Dados pelo prazo de 60 dias, a contar da data de publicação da ata de julgamento, a fim de garantir ao Chefe do Poder Executivo prazo hábil para (i) atribuir ao órgão um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas; e (ii) conferir aos seus integrantes garantias mínimas contra influências indevidas.

Verifica-se, assim, um reforço por parte da Suprema Corte dos princípios e garantias fundamentais dispostas na LGPD, além da possibilidade de responsabilização civil do Estado por eventuais danos gerados aos particulares no processo de tratamento ou compartilhamento de dados pessoais (art. 42 e seguintes da LGPD).

Em seu voto, o relator ressaltou a existência de um direito fundamental autônomo à proteção de dados pessoais, nos termos da ADI nº 6.387/DF,[4] de relatoria da Ministra Rosa Weber, tendo sido previamente construída pelo STF "uma dogmática constitucionalmente adequada para o que se tem chamado de era digital, berço de uma sociedade fundada no desenvolvimento tecnológico e no intercâmbio de informações digitais":[5]

> Aqui também, nos casos ora em julgamento, surge outra auspiciosa oportunidade para que a Corte, no contexto das relações entre os gestores públicos e os titulares de dados pessoais, examine o âmbito de proteção do direito à autodeterminação informativa, mais precisamente **os limites e as salvaguardas institucionais que se aplicam ao compartilhamento de informações entre órgãos e entidades da administração pública federal**.
>
> (ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15/09/2022, DJe 19/06/2023, p. 25 do acórdão).

De forma incisiva, o relator, Min. Gilmar Mendes, defendeu o compartilhamento de dados entre órgãos públicos como forma de aplicação do princípio da eficiência administrativa:

> A partir de agora, a Administração Pública se valerá de mecanismos menos intrusivos, como o compartilhamento de dados, para evitar pagamentos indevidos a pessoas falecidas e combater fraudes no âmbito da seguridade social. Por meio de integração de bases de dados, informações que já se encontram em posse de órgãos públicos federais serão utilizadas para dispensar a prova de vida. Basta que o cidadão tenha sacado dinheiro em agências bancárias, solicitado renovação de carteira de identidade ou habilitação, passaporte ou registro de votação, para que seja considerado vivo. Deparamo-nos, aqui, com exemplo real de legítima utilização do compartilhamento de dados em benefício do cidadão. (p. 74 do acórdão)

Outrossim, pronunciando-se acerca da restrição de acesso a dados pessoais, elucida importante questão acerca do compartilhamento de dados restritos, aduzindo que tal nível engloba informações que, apesar de sigilosas, podem vir a ser acessadas por todos os órgãos e entidades que compõem a Administração Pública Federal.

[4] ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, DJe 12/11/2020.

[5] ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15/09/2022, DJe 19/06/2023, p. 24 do acórdão.

Os critérios estabelecidos almejam, no entanto, impedir, exclusivamente, o acesso do público externo:

> O evento preocupa, na medida em que, por definição, o nível de compartilhamento restrito engloba dados que, apesar de sigilosos, podem ser livremente acessados por todos os órgãos e entidades da Administração Pública Federal. Cuida-se, assim, de categoria que almeja impedir o acesso do público externo a dados cujo sigilo seja imprescindível à segurança da sociedade e do Estado, sem obstaculizar o livre fluxo das informações entre os diferentes órgãos que compõem o aparelho estatal.
>
> Por permitirem ampla difusão de dados sensíveis entre entidades governamentais, os limites impostos pelo nível de compartilhamento restrito oferecem proteção inadequada para a tutela dos valores estruturantes da LGPD. (p. 32 do acórdão)

Sobre a proteção de dados pessoais e o compartilhamento entre órgãos públicos, acrescenta a necessidade de evolução da Administração para adequar-se à evolução tecnológica, sendo fundamental a mediação entre as garantias de autodeterminação informativa e de proteção dos dados pessoais nos cenários de compartilhamento de informações, o que deve ser realizado de forma comedida:

> Os riscos inerentes à era digital devem ser considerados na leitura e na aplicação da Constituição Federal de 1988. Aliás, ousaria dizer que nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica. (p. 41 do acórdão)
>
> [...] a intervenção estatal na esfera privada deve (i) envolver apenas o universo de dados estritamente necessário para o alcance das finalidades eleitas; e (ii) ser acompanhada do incremento dos protocolos e mecanismos de segurança do sistema de informação, de acordo com o grau de risco gerado pela relativização do direito fundamental à autodeterminação informativa (p. 50 do acórdão)
>
> Assim, é clara a necessidade de temperar os valores constitucionais da eficiência da Administração Pública com o regime constitucional de tutela dos direitos individuais, particularmente as garantias de autodeterminação informativa e de proteção dos dados pessoais (art. 5º, caput e incisos X, XII e LXXIX, da Constituição Federal). (p. 61 do acórdão)
>
> Nossa legislação federal, portanto, contempla um plexo de disposições normativas que impõem à Administração Pública a difícil tarefa de implementar bancos de dados de natureza interoperável, desenvolvidos para permitir o compartilhamento eletrônico de informações entre órgãos governamentais, sem prejuízo da irrestrita observância dos princípios gerais e mecanismos de proteção elencados na Lei Geral de Proteção de Dados Pessoais. (p. 73 do acórdão)

Outro ponto relevante no texto do acórdão é o do controle de acesso. Para o

relator, deve-se implementar mecanismos eletrônicos rigorosos de controle de acesso, facilitadores de eventuais responsabilizações por mau uso, cabendo ao Comitê Central a instituição de medidas de segurança compatíveis com a legislação regente.

Em sequência, da leitura do voto proferido pelo Min. André Mendonça, pode-se depreender relevantes considerações no tocante aos desafios enfrentados pela Administração digital para a proteção de dados pessoais em economias globalizadas (p. 151 do acórdão), tendo sido ressaltado, inclusive, as inúmeras vantagens práticas da adoção do compartilhamento de dados na ambiência estatal, como o aumento da capacidade de tomada de decisões informadas, o favorecimento de políticas públicas baseadas em evidências, o estabelecimento de economia baseada em informações e um maior planejamento e possibilidade de resposta emergencial, incrementando, desse modo, a eficiência pública (p. 152 do acórdão).

O Min. Nunes Marques, por sua vez, ressaltando ser um tema novo na jurisprudência pátria, aduz a necessidade de atenção sobre as consequências práticas das teses fixadas, reconhecendo a existência de dois extremos interpretativos que devem ser evitados: o primeiro, excessivamente restritivo, que impede o compartilhamento de dados entre órgãos da Administração Pública. Já o segundo, excessivamente liberal, que libera e incondiciona qualquer compartilhamento (p. 197 do acórdão).

Posiciona-se favorável, nos termos da relatoria, à imposição de um limite vinculado ao atendimento de interesse público que justifique o compartilhamento:

> O primeiro, sob o pretexto de proteger a intimidade e a privacidade das pessoas, obstaria a migração da Administração Pública para o estágio contemporâneo de evolução de organizações públicas e privadas que já trabalham guiadas por dados (data driven), e frustraria também a eficácia prática de uma série de políticas públicas que demandam naturalmente a varredura de dados distribuídos entre vários órgãos.
>
> [...] Na zona intermediária entre os dois extremos, existe espaço para que a Administração possa, sim, conceber soluções gerenciais automatizadas para problemas de negócio próprios de sua atividade, mediante o compartilhamento de dados entre os diversos órgãos públicos, respeitando os direitos dos titulares dos dados pessoais, assim como o direito fundamental de acesso à informação. (p. 197-198 do acórdão)
>
> [...] Constata-se, a partir desses exemplos, a ausência de fundamento constitucional para afirmar-se que é vedado o compartilhamento de dados pessoais entre órgãos do poder público. Aliás, é só olhar a realidade prática da Administração para ver o despropósito que uma tal proibição induziria. Como a Administração descobriria eventual acumulação indevida de cargos públicos ou o recebimento de remuneração acima do teto constitucional se não fossem trocadas informações entre órgãos públicos? Como ela fiscalizaria a correção de uma informação prestada por um candidato a um cargo público caso não pudesse pedir o compartilhamento de dados constantes do registro original? Como a polícia de trânsito conseguiria exercer fiscalização se não pudesse acessar a base de dados dos registros de veículos? Como poderia ser checada a validade de um certificado de vacinação, se não houvesse compartilhamento de dados? (p. 200-201 do acórdão)

Reforça-se, portanto, a permissão de acesso a dados pessoais por outros órgãos públicos apenas mediante a existência de propósitos legítimos, específicos e explícitos para o seu tratamento. A finalidade dos critérios é, primordialmente, evitar o compartilhamento dos dados pessoais em tratamento com pessoas externas aos órgãos e com entidades que não possuam competências legais semelhantes, cujo acesso aos documentos objeto da proteção poderia gerar danos passíveis de responsabilização do Estado, na figura do órgão detentor das informações restritas.

Apresenta-se mais uma razão, agora de ordem jurisprudencial, para a garantia do sigilo atribuído às informações compartilhadas entre órgãos públicos, quando encaminhadas sob esse *status*, reiterado o compartilhamento limitado ao mínimo necessário e o dever de atendimento da finalidade informada.

Sobre o julgamento, surgem uma série de observações relacionadas à constatação, pela Suprema Corte, da redação genérica dos decretos que regulamentam as tecnologias incorporadas ao aparato estatal, incluindo as de segurança para proteção de dados pessoais no compartilhamento entre órgãos públicos. Para o aumento da eficiência da Administração Pública, não são construídos, de forma concreta, os alicerces indispensáveis para a adoção de um governo efetivamente digital, cabendo ao STF, residualmente e em consequência, a fixação desses parâmetros mínimos de proteção (Borges; Monte, 2023, p. 149).

A maioria das organizações que compõem a Administração Pública permanecem inaptas e sem a devida estruturação ao atendimento das exigências legais para o tratamento de dados de acesso restrito, demandando um redesenho institucional para um escorreito compartilhamento dos dados pessoais entre órgãos públicos (Borges; Monte, 2023, p. 149).

Aqui, no que concerne à interpretação concedida à LGPD e decretos regulamentadores, garante-se o direito à privacidade: informações sobre pessoas jurídicas de direito público não gozam dessa prerrogativa. Dessa forma, eventuais sigilos ou restrições atribuídas a informações sobre entes públicos devem ser pautadas em lei ou em razões de ordem lógica que justifiquem a restrição ao acesso (art. 4º, III, c/c art. 23, VIII, e art. 24, da Lei nº 12.527/2011).

Demonstrou-se que, estabelecidas as relações de cooperação, é evidente que o compartilhamento de dados entre órgãos que compõem a Administração Pública, incluindo os dados classificados por grau de sigilo, afigura-se majoritariamente benéfico. Entretanto, faz-se necessária a devida atenção e responsabilização do setor público pelo tratamento dos dados por ele coletados e compartilhados.

A LEI Nº 14.129/2021: AS INTERSEÇÕES COM A LGPD E A MENÇÃO AO COMPARTILHAMENTO DE DADOS PROTEGIDOS POR SIGILO FISCAL

A Lei nº 14.129/2021, mencionada no art. 5º, § 3º, I, *b*, do Decreto nº 10.046/2019, como sendo de observância obrigatória para o compartilhamento de dados

nos níveis de categorização restrito e específico, datada de 29 de março de 2021, dispõe sobre os princípios, regras e instrumentos para o governo digital e para o aumento da eficiência pública, alterando, também, alguns dispositivos da LAI.

Em seu art. 3º, IX, afirma a necessidade dos órgãos públicos atuarem de forma integrada para a prestação dos serviços públicos, possibilitando o compartilhamento de dados pessoais em ambiente seguro, observada a imprescindibilidade do intercâmbio, e o compartilhamento de dados sigilosos, quando cabível.

Refere-se, de forma específica, ao compartilhamento de informações protegidas por sigilo estabelecido em lei, citando, especificamente, o sigilo fiscal e financeiro:

> IX - a atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle dos serviços públicos, com o compartilhamento de dados pessoais em ambiente seguro quando for indispensável para a prestação do serviço, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e, quando couber, com a transferência de sigilo, nos termos do art. 198 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e da Lei Complementar nº 105, de 10 de janeiro de 2001;

Isso porque o art. 198 do Código Tributário Nacional (Lei nº 5.172/1966), por exemplo, possibilita o compartilhamento de informações protegidas por sigilo fiscal entre órgãos que compõem a Administração Pública, desde que comprovada a instauração regular de um processo administrativo e existente finalidade investigativa em decorrência da prática de infração administrativa.

Na mesma linha das legislações e decretos anteriormente analisados, condiciona o compartilhamento, entretanto, à preservação do sigilo:

> Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.
>
> § 1º Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes:
>
> I – requisição de autoridade judiciária no interesse da justiça;
>
> II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa.
>
> § 2º O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo,

que formalize a transferência e assegure a preservação do sigilo.

O CTN, em complemento à Lei nº 14.129/2021, destarte, fortalece a cooperação e assistência mútua entre as Fazendas da União, Estados e Municípios, possibilitando a permuta de informações, inclusive as sigilosas, entre autoridades administrativas.

Desse modo, compreende-se que o compartilhamento de informações e documentos protegidos por sigilo fiscal, devidamente autorizado pela legislação regente, não representa a quebra do sigilo instituído pelo órgão de origem, mas a mera transferência dos dados, devendo a natureza sigilosa ser mantida durante todo o tratamento de informações pelo órgão receptor. É esse, inclusive, o entendimento que vem sendo adotado pelo STF e pelo Superior Tribunal de Justiça.[6]

Regressando às disposições gerais da Lei nº 14.129/2021, o art. 10 reitera a necessidade de observação dos termos da LAI para a classificação da informação quanto ao grau de sigilo, e a possibilidade de limitação de acesso aos dados por servidores autorizados e terceiros interessados.

No art. 16, disciplina-se que a administração de cada ente federado, na busca por um avançado governo digital, poderá editar uma estratégia própria, respeitada a sua competência e na busca por uma compatibilização com as demais estratégias adotadas por outros entes e pela Administração Pública Federal. Trata-se de dispositivo que materializa o escopo cooperativo que deve imperar entre os entes federativos, traduzindo uma tendência de integração e cooperação que se estende aos órgãos públicos.

No Capítulo IV, o qual dispõe sobre o "governo como plataforma", reitera-se o dever de respeito à privacidade dos dados pessoais e sensíveis, nos termos da LGPD, possibilitando, também, o intercâmbio de dados entre órgãos e entidades dos diferentes poderes e esferas da federação, respeitados os dispositivos legais constantes nas legislações relacionadas (art. 29, § 1º, VII e IX).

Outra importante disposição da Lei nº 14.129/2021 refere-se às solicitações para compartilhamento da base de dados em posse de determinado órgão público para fins de pesquisa acadêmica. Sobre o tema, afirma que os órgãos gestores dos dados poderão disponibilizar os dados de pessoas físicas e jurídicas em transparência ativa, desde que anonimizados os dados protegidos por sigilo ou com restrição de acesso, nos termos da LAI (art. 36).

De forma específica, também faz menção à interoperabilidade de dados entre

[6] [...] Logo, não se verifica a violação do sigilo fiscal do recorrente. Isso porque o Supremo Tribunal Federal, julgando conjuntamente as ADIs 2.386/DF, 2.390/DF, 2.397/DF e 2.859/DF, assentou inexistir quebra de sigilo na hipótese de haver intercâmbio de informações sigilosas no âmbito da Administração Pública, conforme preceitua o art. 1º da Lei Complementar n. 104/2001, ao inserir o § 1º, inciso II, e o § 2º ao art. 198 do CTN. (p. 19 do acórdão) [...] deve ser realçado que as informações fiscais do recorrente foram obtidas pela comissão sindicante através dos dados armazenados nos sistemas internos da Receita Federal, sendo certo que tais informações não foram divulgadas a terceiros. Por isso, a Administração Pública agiu dentre dos limites legais e constitucionais, não se cogitando quebra de sigilo fiscal. (p. 21 do acórdão) (AREsp n. 1.068.263/RJ, relator Ministro Napoleão Nunes Maia Filho, relator para acórdão Ministro Benedito Gonçalves, Primeira Turma, julgado em 20/2/2020, DJe de 5/3/2020).

órgãos públicos, disciplinando a necessidade de atenção aos requisitos de segurança da informação, das limitações tecnológicas, e da relação custo-benefício da interoperabilidade, sendo de responsabilidade dos órgãos os custos de adaptação de seus sistemas e bases de dados (art. 38, I, c/c art. 41).

CONCLUSÃO

O estudo demonstrou que a LGPD não impede o compartilhamento de dados pessoais entre órgãos públicos. Ao contrário, a lei admite expressamente o uso compartilhado para a execução de políticas públicas e o cumprimento de competências legais, sem necessidade de consentimento do titular.

Essa permissão, contudo, é condicionada. O tratamento deve atender à finalidade pública, observar os princípios do art. 6º, sobretudo os da finalidade, adequação e necessidade, e ser acompanhado de publicidade sobre as hipóteses de tratamento e de medidas de segurança aptas a evitar acessos indevidos.

Verificou-se, também, que a interoperabilidade exigida pelo art. 25 ainda não se concretizou de forma satisfatória. A persistência de sistemas isolados dificulta o intercâmbio de informações, embora plataformas integradas possam facilitar a proteção do sigilo, ao permitir o acesso controlado sem a transferência efetiva dos dados.

O julgamento da ADI nº 6.649/DF e da ADPF nº 695/DF reforçou esses parâmetros. O STF afastou a ideia de oposição entre interesse público e proteção de dados e exigiu propósito legítimo, compatibilidade com a finalidade, limitação ao mínimo necessário, controle de acesso e responsabilização do Estado e de seus agentes em caso de abuso.

A Lei nº 14.129/2021, em conjunto com o art. 198 do CTN, confirmou que o intercâmbio de dados protegidos por sigilo fiscal entre órgãos públicos não representa quebra de sigilo, mas sua transferência. A natureza sigilosa da informação deve, portanto, ser mantida pelo órgão receptor durante todo o tratamento.

Conclui-se que o compartilhamento de dados pessoais entre órgãos públicos é legítimo e benéfico à eficiência administrativa. Sua validade, porém, depende do respeito à finalidade, do compartilhamento mínimo, da preservação do sigilo atribuído na origem e da adoção de mecanismos de segurança e responsabilização.

REFERÊNCIAS

Borges, Dayana de Moura; Monte, Rafaela Guerra. Administração Pública dos clips à inteligência artificial: os impactos das transformações digitais na proteção de dados pessoais. *In*: Nobre Júnior, Edilson Pereira; Cocentino, Nathália Nóbrega (org.). **Direito administrativo e administração pública digital**. Belo Horizonte: Dialética,

2023, p.122-157.

Coutinho, Luciana Maria Silveira Gomes; Marcon, Cecília Figueiredo. Tratamento de dados pelo poder público. *In*: Nobre Júnior, Edilson Pereira; Cocentino, Nathália Nóbrega (org.). **Direito administrativo e administração pública digital**. Belo Horizonte: Dialética, 2023, p. 160-178.

Doneda, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 4, n. 16, p. 117-133, out./dez. 2003. Disponível em: https://scholar.google.it/citations?view_op=view_citation&hl=pt-BR&user=gSv2oD4AAAAJ&cstart=20&pagesize=80&citation_for_view=gSv2oD4AAAAJ:2osOgNQ5qMEC. Acesso em: 24 jul. 2023.

Nobre Júnior, Edilson Pereira. A LINDB e a influência da realidade na função administrativa: o texto versus o contexto. **Interesse Público**, Belo Horizonte, v. 22, n. 123, p. 17-32, set./out. 2020. Disponível em:https://pt.scribd.com/document/649961890/Texto-1-LINDB-Edilson-Nobre-230524-154130-1 #. Acesso em: 05 mai. 2023.

Nobre Júnior, Edilson Pereira. **As normas de direito público na lei de introdução ao direito brasileiro**: paradigmas para interpretação e aplicação do direito administrativo. São Paulo: Contracorrente, 2019.

Santanna, Gustavo da Silva. **Administração pública eletrônica**: o caminho para a implantação de serviços públicos 4.0. Londrina: Thoth, 2022.