A LEI Nº 12.527/2011 (LEI DE ACESSO À INFORMAÇÃO) E O COMPARTILHAMENTO DE DADOS DE ACESSO RESTRITO

LAW 12,527/2011 (ACCESS TO INFORMATION ACT) AND THE SHARING OF RESTRICTED-ACCESS DATA

ISBN: 978-85-7872-853-3
DOI: 10.56089/978-85-7872-853-3

Gabriela Calábria Araújo Moraes dos Santos[1]

RESUMO

O artigo analisa a Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI) e seus principais decretos regulamentadores sob a ótica do compartilhamento de dados de acesso restrito entre órgãos públicos. Parte-se da premissa constitucional de que a publicidade é a regra e o sigilo, a exceção, para examinar as hipóteses de restrição de acesso previstas no Capítulo IV da LAI, incluindo a classificação das informações em graus de sigilo e o tratamento das informações pessoais. Em seguida, são estudados os Decretos nº 7.724/2012, nº 7.845/2012 e nº 10.046/2019, com foco nas regras de segurança, credenciamento e governança do compartilhamento de dados. A pesquisa, de caráter bibliográfico e documental, conclui que o ordenamento admite o intercâmbio de informações sigilosas entre órgãos públicos, desde que o órgão receptor assuma os mesmos deveres de sigilo, segurança e auditabilidade impostos ao órgão de origem, limitando o uso dos dados à finalidade que justificou o compartilhamento.

Palavras-chave: Lei de Acesso à Informação; transparência administrativa; informação sigilosa; dados pessoais; compartilhamento de dados.

ABSTRACT

This article analyzes Law No. 12.527/2011 (the Access to Information Law – LAI) and its primary regulatory decrees, focusing on the sharing of restricted-access data among public agencies. Based on the constitutional premise that transparency is the rule and confidentiality the exception, the study examines the grounds for restricting access as set forth in Chapter IV of the LAI, including the classification of information by levels of confidentiality and the handling of personal data. Subsequently, it examines Decrees No. 7.724/2012, No. 7.845/2012, and No. 10.046/2019, with an emphasis on security, accreditation, and governance rules for data sharing. Through bibliographic and

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

documentary research, the study concludes that the legal framework permits the exchange of confidential information between public agencies, provided that the receiving agency assumes the same obligations regarding confidentiality, security, and auditability as those imposed on the originating agency, while limiting the use of the data to the specific purpose that justified the sharing.

Keywords: Access to Information Law; administrative transparency; confidential information; personal data; data sharing.

INTRODUÇÃO

O direito de acesso à informação é garantia fundamental prevista na Constituição de 1988 e instrumento essencial ao controle da Administração Pública. A Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação (LAI), deu concretude a esse direito ao fixar regras gerais de transparência para todos os entes federativos.

A LAI, porém, não trata apenas da relação entre o Estado e o cidadão. Seus dispositivos também alcançam o tratamento das informações em posse do poder público e, por consequência, o compartilhamento de dados entre os próprios órgãos que compõem a Administração.

Esse ponto ganha relevância quando os dados compartilhados são sigilosos ou dizem respeito à intimidade das pessoas. Nesses casos, a cooperação entre órgãos precisa ser compatibilizada com as restrições de acesso previstas em lei, sob pena de violação ao interesse público e aos direitos fundamentais.

Nesse contexto, o objetivo deste artigo é identificar em que termos a LAI e seus regulamentos autorizam o compartilhamento de dados de acesso restrito entre órgãos públicos e quais deveres recaem sobre quem recebe essas informações. Utiliza-se metodologia bibliográfica e documental, com análise da legislação e da doutrina.

O trabalho está dividido em duas partes. A primeira examina o Capítulo IV da LAI, que trata das restrições de acesso, da classificação das informações e do tratamento de dados pessoais. A segunda analisa os Decretos nº 7.724/2012, nº 7.845/2012 e nº 10.046/2019.

A Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação, doravante invocada pela sigla “LAI”, conhecida por parte da doutrina como a “nova Lei da Transparência” (Martins, p. 4), é um marco jurídico para a fixação de sistemas de gestão da informação.

Em decorrência de compromisso firmado pelo governo brasileiro por ocasião do *Open Government Partnership* (Cruz, 2017, p. 220), regulamenta, fundamentalmente, o direito fundamental de acesso à informação, previsto no retromencionado inciso XXXIII do art. 5º da CRFB, e no inciso II do § 3º do art. 37 do mesmo diploma, que assim dispõem:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
>
> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
>
> § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:
>
> II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;

Tal instrumento normativo pretende conferir ampla efetividade ao direito fundamental à informação, garantindo a transparência e o controle da Administração Pública, de forma a superar o reducionismo da publicidade como sendo medida suficiente para legitimar a ação administrativa (Medeiros; Wacheleski, p. 1). A norma define uma série de princípios que devem orientar as ações dos órgãos públicos. Mais do que publicidade, almeja-se a transparência administrativa (Rosa, 2017, p. 195).

Trata-se de legislação infraconstitucional cujos dispositivos devem ser observados por todas as esferas da Administração Pública, ou seja, pela União, Estados, Distrito Federal e Municípios. Subordinam-se a ela (i) todos os órgãos públicos integrantes da administração direta dos três poderes, incluindo os Tribunais de Contas; (ii) os que integram a administração indireta; e (iii) as entidades privadas sem fins lucrativos que recebem recursos públicos para realização de ações de interesse público (arts. 1º e 2º da Lei nº 12.527/2011).

"Está-se diante de uma lei nacional e não federal", possuindo apenas alguns de seus dispositivos a eficácia limitada à Administração Federal em decorrência objetiva da autonomia político-administrativa dos demais entes da Administração (Nobre Júnior, 2017, p. 257).

O referido diploma legal rege, entre outros escopos, o tratamento de dados pelo poder público, incluindo, decerto, o compartilhamento de dados e informações de acesso restrito entre os entes administrativos, razão pela qual é um dos principais objetos da presente análise. Logo no inciso I do art. 3º, a LAI reafirma o direito à informação como fundamental, exigida a transparência na atuação do Estado, em especial da Administração Pública, após a promulgação da Constituição (Nobre Júnior, 2017, p. 252). Ademais, reitera a diretriz constitucional de "observância da publicidade como preceito geral e do sigilo como exceção". Dessa forma, em um contexto de compartilhamento de dados entre órgãos públicos, em uma primeira análise, não há de existir impedimento a esse ato de cooperação: o intercâmbio de informações, ainda que promovidos, na prática, por meio de instrumentos de cooperação (convênios administrativos) ou solicitações a casos específicos, "impõe-se independente de

requisição formal, com os meios viabilizados pela tecnologia da informação, nos termos do art. 3º, incisos II e III, o que se denomina de “dever de transparência ativa” (Nobre Júnior, 2017, p. 260).

Mas isso no tocante aos dados abertos, aos quais não incide qualquer dever de sigilo da informação. O art. 4º da LAI conceitua a “informação sigilosa” como sendo “aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”.

Sopesado um dos objetivos políticos da LAI, realizada uma interpretação histórica, sistemática e teleológica do ordenamento jurídico vigente, infere-se a influência da derrocada do segredo como prioridade de um Estado Democrático de Direito, sendo o sigilo um dos pilares de regimes autoritários (Nobre Júnior, 2017, p. 250). Nesse contexto, observa-se a existência de algumas possibilidades de redução da transparência administrativa a seu substrato negativo no compartilhamento de dados entre órgãos públicos, aos quais se pode impor o sigilo como forma de garantia de direitos fundamentais.

Para Vanice Regina do Valle (2014, p. 125), a obtenção de uma informação em posse de um dos órgãos da Administração Pública não se opera de forma instantânea, devendo submeter-se a um ciclo de tratamento, motivo pelo qual é possível a restrição da transparência e a negativa do pedido de compartilhamento nas hipóteses em que o ciclo de conhecimento da informação não se aperfeiçoou, por exemplo. É esse, inclusive, o teor do art. 7º, § 3º, da LAI, que dispõe que o direito de acesso a informações que embasam decisões ou atos administrativos apenas é garantido após a publicação do ato principal.

De forma específica, o Capítulo IV da LAI, seguindo os comandos do art. 5º, XXXIII da CRFB, disciplina as restrições de acesso à informação, as quais são de observância obrigatória em processos de compartilhamento de dados entre entes da Administração Pública, considerado o interesse público e a proteção da própria sociedade, respeitado o núcleo estabelecido na norma constitucional (Medeiros; Wacheleski, p. 6).

1 O CAPÍTULO IV DA LAI E O COMPARTILHAMENTO DE DADOS CLASSIFICADOS EM GRAU DE SIGILO

1.1 Da restrição de acesso a informações sob a égide do interesse público ou da proteção da sociedade: o dever de preservação do sigilo no compartilhamento de dados

Inicialmente, rememore-se o conceito de informação sigilosa contido no art. 4º da Lei nº 12.527/2011: “aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”. Serão abordados neste subtópico os principais dispositivos que regulamentam a matéria, em específico os que interferem no compartilhamento de dados sigilosos entre entes que compõem a Administração.

O art. 6º da Lei 12.527/2011, no que concerne ao acesso a informações e a sua

divulgação, afirma competir aos órgãos e entidades do poder público assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e possível restrição de acesso (art. 6º, III, da Lei nº 12.527/2011).

A Seção I do Capítulo IV do mesmo diploma legal dispõe, de forma específica e reforçando a excepcionalidade do segredo (Nobre Júnior, 2017, p. 265), a impossibilidade de negativa de acesso a informação que seja necessária para a tutela judicial ou administrativa de direitos fundamentais, afirmando, ainda, que o disposto na lei não exclui ou excetua as hipóteses legais de sigilo, segredo de justiça ou segredo industrial (arts. 21 e 22).

A Seção II do Capítulo IV, que aqui adquire maior relevância, classifica a informação quanto ao grau e prazo de sigilo, conceituando o que se considera, nos termos do já mencionado art. 4º, informação imprescindível à segurança da sociedade ou do Estado, às quais, ainda que não ostentem o caráter prévio de sigilo, podem ser atribuídas restrições de acesso:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
>
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
> III - pôr em risco a vida, a segurança ou a saúde da população;
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

As informações e dados em posse dos órgãos e entidades públicas devem, ainda, ser classificadas em ultrassecreta, secreta ou reservada, com prazos máximos de restrição de acesso de 25 anos, 15 anos e 5 anos, respectivamente, observado o seu teor e imprescindibilidade à segurança da sociedade ou do Estado. Findo o prazo, que deve ser o menos restritivo possível, serão de acesso público (art. 24 da Lei nº 12.527/2011).

Portanto, do texto legal, extrai-se a possibilidade de conferir sigilo a determinada informação com base em norma autorizadora, ou, alternativamente, nos termos da Lei de Acesso à Informação, uma restrição de acesso aos dados imprescindíveis à segurança da sociedade ou do Estado. Isso porque o direito de acesso à informação não ostenta colorido absoluto, sendo da alçada da lei formal a definição de situações em que não

incidirá o acesso imediato e irrestrito à informação pública (Nobre Júnior, 2017, p. 265).

Em termos práticos, o que se opera é uma restrição de acesso a determinada informação com base em sigilo determinado por lei ou que se faça necessário à garantia da segurança da sociedade ou do Estado, quando o cumprimento da transparência administrativa, em sua plenitude, demonstraria-se majoritariamente prejudicial.

Para conferir maior clareza aos conceitos, explique-se: informação classificada, nos termos do art. 24 da LAI, é toda aquela submetida a qualquer dos três graus de sigilo previstos no texto legal. Já a informação sigilosa é aquela cuja restrição de acesso ocorre em virtude de sua classificação ou por hipótese legal de sigilo. Trata-se de definição formulada pelo Gabinete de Segurança Institucional no Tratamento da Informação Classificada e Credenciamento de Segurança.[2]

Dessa forma, "toda informação classificada é sigilosa, porém nem toda informação sigilosa é classificada". Aqui, para fins didáticos, utilizar-se-á a nomenclatura de "dados sigilosos" ou "classificados" para todas as informações que possuem acesso restrito.

A questão a ser melhor analisada é o compartilhamento desses dados cujo acesso foi restringido ou cujo sigilo tenha sido atribuído na fonte, de forma a promover um escorreito intercâmbio de informações entre órgãos que compõem o poder público.

Chegando à Seção III do Capítulo IV, obtém-se maiores esclarecimentos relacionados à proteção e controle das informações tidas como sigilosas. O *caput* do art. 25 reitera, de forma similar ao já abordado art. 6º, III, ser dever do Estado o controle do acesso e divulgação de informações sigilosas produzidas por seus órgãos. No tocante ao compartilhamento, o § 2º do art. 25 da LAI dispõe que "o acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo".

Aponta-se, ainda que de forma tímida, para a necessidade de preservação do sigilo atribuído aos dados na origem pelos órgãos que passam a tratá-los após o compartilhamento das informações. Tendo sido imposto ao Estado o dever de informar, certo é que se atribua também a ele o dever de controle do acesso e divulgação de informações sigilosas de sua posse (Nobre Júnior, 2017, p. 258).

A lei, em diversos de seus artigos, dispõe acerca do processo para obtenção da informação. Em sua maioria, tratam-se de dispositivos direcionados à sociedade, *stricto sensu,* diverso o processo de obtenção das informações pelo poder público, que se dá, em sua maioria, pela assinatura de convênios administrativos ou instrumentos congêneres que facilitam o processo de compartilhamento de informações, conforme previamente esclarecido. Outra questão de destaque, também abordada pela Lei de Acesso à Informação, é o tratamento de dados pessoais, merecendo especial atenção o compartilhamento desses dados, de natureza restrita, entre os órgãos que compõem a Adminstração Pública. Em verdade, são os dados pessoais informações às quais usualmente se atribui determinado nível de restrição de acesso, passando a serem, portanto, sigilosas. O normativo, ao optar por destacar esse tipo de dado, almeja conferir maior prestígio e estabelecer critérios individualizados para o seu tratamento, dada a

[2] [8] Disponível em: https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/perguntas-frequentes-1/perguntas-sobre-tratamento-da-infor macao-classificada-e-credenciamento-de-seguranca-lai. Acesso em: 24 jul. 2023.

fundamentalidade de sua existência e a maior necessidade de segurança.

1.2 Do tratamento e compartilhamento de dados pessoais

A seção V da LAI é a responsável por dispor acerca do tratamento das informações pessoais. Em seu art. 31, faz menção à transparência administrativa, dispondo:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> IX - **terão seu acesso restrito, independentemente de classificação de sigilo** e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> X - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
>
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido
>
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
>
> I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
> II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III - ao cumprimento de ordem judicial;
> IV - à defesa de direitos humanos; ou
> V - à proteção do interesse público e geral preponderante.
>
> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
>
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

O tratamento das informações, usualmente, deve ser feito, conforme a legislação, de forma transparente, o que difere da restrição de acesso às informações pessoais, sobre as quais se depreende que a restrição opera de forma distinta ao sigilo anteriormente mencionado, na medida em que a norma afirma a necessidade de restrição de acesso a dados pessoais independente de classificação e por um prazo máximo consideravelmente superior, de cem anos.

Possuem acesso a esses dados relativos à intimidade, vida privada, honra e imagem, portanto, os agentes públicos legalmente autorizados e as pessoas às quais as informações se referem, autorizado o acesso por terceiros mediante previsão legal ou prévio consentimento dos seus titulares. Prevê-se, ainda, nos termos do § 2º do art. 31, a devida responsabilização dos agentes por uso indevido das informações.

O que merece especial atenção no presente estudo é, no entanto, o inciso V do § 3º do art. 31, o qual afirma a inexigibilidade do consentimento dos titulares dos dados pessoais quando estes fizerem-se necessários à proteção do interesse público e geral preponderante. Nesses termos, pode-se concluir, ainda que preliminarmente, a possibilidade de compartilhamento de dados pessoais entre entes da Administração Pública, desde que atendida a premissa de aferição do interesse público e cujo uso limite-se à atuação do órgão receptor, sob pena de caracterização de uso indevido dos dados em tratamento.

Seguindo essa linha de raciocínio, o § 5º do art. 31 da Lei nº 12.527/2011 aduz que regulamento próprio será responsável por dispor acerca dos procedimentos para tratamento de informação pessoal pelos órgãos do poder público. Tal função é cumprida com determinado grau de êxito pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), objeto de capítulo próprio.

Foram publicados, ainda, uma série de decretos regulamentadores da Lei nº 12.526/2011, os quais serão agora analisados sob a ótica da operacionalização do tratamento e compartilhamento de dados sigilosos entre órgãos públicos, buscando os dispositivos que permitam um maior esclarecimento dos termos que devem reger esses processos de intercâmbio de informações entre entes da Administração Pública. Ressalte-se que serão mencionados os principais dispositivos, sem menção aos que não se relacionam ao tema do presente estudo ou que meramente reproduzem artigos da LAI.

2.UMA ANÁLISE DOS PRINCIPAIS DECRETOS REGULAMENTADORES DA LEI DE ACESSO À INFORMAÇÃO

De proêmio, ressalte-se que o campo de aplicação dos decretos regulamentadores que serão agora analisados restringe-se, formalmente, aos órgãos do Poder Executivo Federal, decerto que servem de modelo para a regulamentação nos demais entes federativos, que, respeitada a autonomia administrativa,[3] devem produzir seus próprios atos normativos, observada a Lei Maior.

Ressalte-se, também, a possibilidade e efetiva existência de regulamentações específicas elaboradas por cada órgão público, que, por meio de resoluções, portarias normativas ou instrumentos análogos, editam atos normativos próprios acerca do tratamento e compartilhamento de informações sigilosas, adotados os comandos legais

[3] Art. 18. A organização político-administrativa da República Federativa do Brasil compreende a União, os Estados, o Distrito Federal e os Municípios, todos autônomos, nos termos desta Constituição. Art. 25. Os Estados organizam-se e regem-se pelas Constituições e leis que adotarem, observados os princípios desta Constituição. § 1º São reservadas aos Estados as competências que não lhes sejam vedadas por esta Constituição.

e constitucionais pertinentes.

2.1 Decreto nº 7.724/2012

O Decreto nº 7.724/2012, publicado em 16 de maio de 2012, é um dos instrumentos regulamentadores da Lei de Acesso à Informação (Lei nº 12.527/2011). Seu principal objetivo é estabelecer procedimentos e regras para garantir o acesso à informação pública e a sua divulgação, com foco, também, na transparência das ações governamentais.

Conforme previamente exposto, no conjunto de regras do direito administrativo brasileiro é incomum o uso da expressão “transparência“. No entanto, tal decreto, principalmente em seus Capítulos III e IV, faz menção expressa à transparência administrativa, distinguindo a transparência ativa da transparência passiva (Nobre Júnior, 2017, p. 256).

A primeira, a transparência ativa, refere-se ao dever dos órgãos públicos de promover, independente de requerimento, a divulgação de informações de interesse geral, tanto as por eles produzidas quanto as custodiadas, respeitados os termos da LAI (art. 7º do Decreto nº 7.724/2012).

Já a segunda, a transparência passiva, diz respeito ao dever inerente aos órgãos e entidades públicas de criarem e manterem serviços de informação para o processamento dos pedidos de acesso à informação, que poderão ser formulados por qualquer pessoa física ou jurídica.

Como já mencionado, os processos de cooperação entre órgãos públicos, em sua maioria, estabelecem-se sob termos de convênios administrativos previamente assinados, os quais preveem o repasse de informações e dados de interesse do órgão para o desempenho de suas competências funcionais, respeitadas as limitações ao repasse e as disposições legais.

Aos casos em que não há um fluxo pré estabelecido de compartilhamento de dados entre os órgãos públicos envolvidos na transação, o art. 13 do Decreto nº 7.724/2012 destaca que pedidos de acesso a informações não serão atendidos caso demonstrem-se genéricos, desproporcionais, desarrazoados ou que exijam trabalhos adicionais de análise, consolidação e interpretação de dados e informações.

Realizando uma interpretação teleológica da norma supracitada, que supera a lógica formal e dirige a atenção do intérprete conforme o fim colimado pelo dispositivo (Maximiliano, 2017, p. 150), pode-se extrair, com certo grau de certeza, que a finalidade de sua edição foi evitar o uso indevido de dados em posse do poder público, além de uma mobilização infundada de recursos, pelos órgãos detentores da informação, para a organização específica dos dados a serem disponibilizados a outros requerentes, nos moldes das solicitações a eles endereçadas.

Porém, o acesso à informação a que se refere o decreto não se aplica às hipóteses de sigilo previstas na legislação, a exemplo do sigilo fiscal, bancário, de serviços no mercado de capitais ou segredo de justiça, nos termos do seu art. 6º. A essas informações, aplica-se a regra geral de tratamento restrito das informações sigilosas, nos termos da classificação estabelecida e respeitado o prazo de sigilo deferido aos dados em

específico. Nesse ponto, o decreto apenas reproduz os dispositivos da LAI.

Sobre as informações pessoais, também ratifica o conteúdo da Lei nº 12.527/2011, mencionando a possibilidade de divulgação ou acesso por terceiros autorizados, como as entidades do poder público, aos dados pessoais, quando existente a finalidade de proteção do interesse público (art. 57, V).

Além disso, dispõe, em seu art. 58, I, cuja redação foi recentemente alterada pelo Decreto nº 11.527/2023, que as informações pessoais não podem sofrer restrições de acesso quando houver o intuito de prejudicar processos de apuração de irregularidades em que o titular das informações seja parte ou interessado.

Dessa maneira, compreende-se que não há menções explícitas ao compartilhamento de dados sigilosos ou de acesso restrito entre órgãos que compõem a Administração Pública. Entretanto, seu conteúdo inicia o processo de esclarecimento dos termos aos quais restam submetidos os processos de tratamentos de dados pelo poder público, ratificando o dever de preservação do sigilo, nas hipóteses legalmente admitidas, impondo a transparência dos dados como regra, e limitando o atendimento das solicitações de acesso a dados à demonstração de finalidade idônea, específica e bem delimitada, que não exija maiores esforços de consolidação e organização da informação por parte do órgão público que a possua.

2.2 Decreto nº 7.845/2012

Agora, de forma específica, o Decreto nº 7.845, publicado em 14 de novembro de 2012, é o responsável por regulamentar os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, nos termos da Constituição e da Lei nº 12.527/2011. Do mesmo modo, tem o seu campo de aplicação restrito ao Poder Executivo Federal, nos termos do *caput* de seu art. 1º.

No inciso XVIII do art 2º, para efeitos do decreto, define o tratamento de informação classificada como sendo “o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo”.

Nos termos do art. 37 da Lei nº 12.527/2011, no Poder Executivo Federal, compete ao Núcleo de Segurança e Credenciamento, órgão central de credenciamento de segurança, credenciar pessoas para o tratamento de informações classificadas (art. 3º do Decreto nº 7.845/2012), existindo outras entidades, como o Comitê Gestor da Segurança da Informação e o Gabinete de Segurança Institucional (arts. 5º e 6º), com funções específicas relacionadas à cadeia de controle e tratamento de informações classificadas.

Nessa mesma cadeia, devem existir, também, os intitulados “órgãos de registro”, que, entre outras competências, habilitam postos de controle nos órgãos e entidades públicas para o armazenamento e tratamento de informações classificadas em qualquer grau de sigilo (art. 7º). No Poder Executivo Federal, podem ser os ministérios ou órgãos de nível equivalente (art. 2º, XIII). Os postos de controle, por sua vez, devem garantir a

segurança da informação classificada sob sua responsabilidade (art. 9º, II), podendo ser uma unidade de órgão ou entidade pública ou privada, desde que habilitada.

A habilitação dos órgãos e entidades públicas para o credenciamento de segurança condicionam-se à comprovação de qualificação técnica suficiente para garantir a segurança da informação classificada, além de dever ser designado um gestor de segurança e credenciamento (art. 10, I e II).

Ressalte-se que aos órgãos de registro possibilita-se a celebração de ajustes, convênios e termos de cooperação com outros órgãos públicos habilitados para o credenciamento de segurança e tratamento de informações classificadas (art. 14), restringindo o acesso, divulgação e tratamento de informações classificadas às pessoas com necessidade de conhecê-las, credenciadas ou autorizadas por legislação (art. 18).

Excepcionalmente, admite-se a celebração do que se intitula Termo de Compromisso de Manutenção de Sigilo (TCMS), sob o qual a informação classificada será disponibilizada a pessoa que se obrigará a manter o sigilo dos dados disponibilizados, sob pena de responsabilização penal, civil e administrativa (art. 18, parágrafo único).

O decreto preocupou-se, de forma incisiva, com os processos de segurança da informação classificada, dispondo acerca da obrigatoriedade de serem mantidas em condições especiais de segurança (art. 30). Os dados classificados como ultrassecretos ou secretos devem ser armazenados, inclusive, em ambientes que ofereçam segurança compatível com o grau de sigilo, devendo os meios eletrônicos fazerem uso de sistemas de tecnologia da informação atualizados e prevenidos contra ameaças de quebra de segurança (art. 30, § 2º).

Em qualquer grau de sigilo, os meios eletrônicos devem possuir recursos criptográficos adequados (art. 31), entendendo-se esses recursos como a conversão de dados de um formato legível a um formato codificado, que só podem ser lidos ou processados após um processo de descriptografia. Trata-se do formato mais simples e importante para que informações classificadas não sejam extraviadas e utilizadas para fins não idôneos (Kaspersky).

Principalmente nos processos de transmissão da informação, o decreto regulamenta a necessidade de controle e registro de acesso às informações classificadas, que deverá ser garantido, no mínimo, por uso de certificado digital (art. 38, §§ 1º, 3º e 4º).

2.3 O Decreto nº 10.046/2019

Já o Decreto nº 10.046, de 09 de outubro de 2019, cuida da governança no compartilhamento de dados na Administração Pública Federal, instituindo o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Trata-se de decreto que regulamenta não só a Lei de Acesso à Informação, mas a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, legislação à qual será concedido capítulo próprio.

Em suas disposições gerais, afirma estabelecer as diretrizes para o compartilhamento de dados entre os órgãos e entidades da Administração Pública Federal

e demais poderes da União, objetivando, entre outros escopos, promover a melhoria da qualidade e da fidedignidade dos dados custodiados, aumentando a eficiência das operações internas (art. 1º, IV e V). O § 2º do art. 1º exclui de sua regulamentação, exclusivamente, os dados protegidos por sigilo fiscal, sob gestão da Secretaria Especial da Receita Federal do Brasil.

Muitas são as finalidades e discussões em torno do decreto, cuja constitucionalidade vem sendo objeto de diversas ações em tramitação no Supremo Tribunal Federal. Aqui, a análise se restringe ao compartilhamento de dados de acesso restrito entre os órgãos da Administração Pública.

Nessa toada, o art. 2º, VIII, conceitua o compartilhamento de dados como sendo a "disponibilização de dados pelo seu gestor para determinador recebedor de dados". Em sequência, a confidencialidade como sendo a "propriedade que impede que a informação fique disponível ou possa ser revelada à pessoa natural, sistema, órgão ou entidade não autorizado e não credenciado" (art. 2º, IX); e a governança de dados como o "exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos" (art. 2º, XV).

Outra definição que merece a devida atenção refere-se ao "mecanismo de compartilhamento de dados": "recurso tecnológico que permite a integração e a comunicação entre aplicações e serviços do recebedor de dados e dos órgãos gestores de dados, tais como serviços web, cópia de dados, lago de dados compartilhado e plataformas de interoperabilidade" (art. 2º, XX).

O acima mencionado conceito de interoperabilidade adquiriu especial relevância no ordenamento jurídico nacional com a publicação da LGPD, que regulamenta uma série de aspectos do que se intitulou governo eletrônico. Diante de sua relevância no compartilhamento de dados de acesso restrito entre órgãos públicos, será melhor analisado no tópico 4.2 do presente trabalho.

Ainda no que se refere ao compartilhamento de dados, o Decreto nº 10.046/2019 afirma que a informação em posse do Estado deverá ser compartilhada da forma mais ampla possível. Todavia, estabelece, também em seu art. 3º, I, uma ressalva acerca do dever de observância das restrições legais para o compartilhamento, dos requisitos de segurança da informação e demais disposições da LGPD.

Mas o que é de extrema relevância a essa análise, no entanto, é o inciso II do mesmo dispositivo, que disciplina: "o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade[4] impostos ao

[4] "A palavra "auditar" já existe no nosso dicionário e significa fazer a auditoria de. "Auditoria", por sua vez, significa processo de exame e validação de um sistema, atividade ou informação. A partir dessa palavra, criou-se "auditável", por um processo de derivação que inseriu o sufixo -vel para indicar a possibilidade de praticar ou sofrer a ação de auditar. Ou seja, algo "auditável" é algo que é possível auditar. A partir dessa nova palavra, criou-se "auditabilidade", outra derivação, dessa vez com o acréscimo do sufixo-idade – com as devidas adaptações –, a fim de formar um termo que expressasse a ideia de condição do que é "auditável". Além disso, a palavra também tem origem no termo "*auditability*", que é da Língua Inglesa e não tinha correspondente em Língua Portuguesa. O conceito de "auditabilidade" alude a soluções que promovem confiança na informação. É a qualidade de algo que se pode analisar de maneira metódica e a capacidade de aferir práticas com características explicativas e informações rastreáveis, de modo a ensejar uma análise crítica das informações fornecidas." (Fernandes)

custodiante dos dados". Reitera-se, no dispositivo regulamentador, a possibilidade de compartilhamento de dados sigilosos, explícito, agora, o dever de preservação de sigilo e auditabilidade pelo órgão recebedor dos dados.

Sobre os dados pessoais, após uma série de alterações promovidas pelo Decreto nº 11.266/2022, regulamenta:

> Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> V - nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação;
>
> VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais;
>
> [...]
>
> IX - a limitação do compartilhamento de dados pessoais ao mínimo necessário para o atendimento da finalidade informada, nos termos do disposto no inciso III do caput do art. 6º da Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais, e o cumprimento integral dos requisitos, das garantias e dos procedimentos estabelecidos na referida Lei, no que for compatível com o setor público.

Do inciso IX do supracitado artigo, depreende-se a limitação do compartilhamento de dados pessoais ao mínimo necessário para o atendimento da finalidade informada para o tratamento, devendo ser cumpridos todos os procedimentos e garantias estabelecidas na LGPD.

De mais a mais, o Capítulo II do referido decreto estabelece três níveis de compartilhamento de dados: (i) o compartilhamento amplo, referente aos dados públicos e sem restrição de acesso; (ii) o compartilhamento restrito, acerca dos dados protegidos por sigilo e cuja concessão de acesso pode ser dada para todos os órgãos de que trata o art. 1º, objetivando a execução de políticas públicas; e (iii) o compartilhamento específico, sobre os dados protegidos por sigilo e cujo acesso restringe-se a órgãos específicos, para os fins previstos em lei (art. 4º).

Sobre esse último, o compartilhamento e regras são definidos pelo gestor de dados, devendo a categorização do nível de compartilhamento ser por ele também realizada (art. 4º, § 1º).

Para os órgãos integrantes da Administração Pública Federal, inclusive, o decreto dispensa a celebração de convênios ou instrumentos congêneres para o compartilhamento de dados, observadas as diretrizes regulamentares e legais (art. 5º). Ainda sobre o compartilhamento de dados nos níveis de categorização restritos e específicos, o que aqui mais interessa, disciplina:

> Art. 5º Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º, observadas as diretrizes do art. 3º e o disposto na Lei nº 13.709, de 2018.
>
> § 3º O compartilhamento de dados nos níveis de categorização restritos e específicos serão autorizados pelo gestor de dados e **seu processo será formalizado por documentos de interoperabilidade cuja solicitação seguirá os critérios estabelecidos pelo Comitê Central de Governança de Dados**, em observância:
>
> I - aos dispositivos:
>
> a) da **Lei nº 13.709, de 2018** - Lei Geral de Proteção de Dados Pessoais;
> b) da **Lei nº 14.129, de 29 de março de 2021**; e
> c) da **Lei nº 12.527, de 18 de novembro de 2011**;
>
> II - às orientações da Autoridade Nacional de Proteção de Dados; e
>
> III - às normas correlatas.
>
> § 4º Nas solicitações de interoperabilidade que envolvam dados pessoais, serão explicitados, além do disposto no § 3º:
>
> **I - o propósito legítimo, específico e explícito**
>
> **II - a compatibilidade com a finalidade**; e
>
> **III - o compartilhamento do mínimo necessário para atendimento da finalidade.**
>
> Art. 7º As plataformas de interoperabilidade contemplarão os requisitos de sigilo, confidencialidade, gestão, auditabilidade e segurança da informação necessários ao compartilhamento de dados, conforme regras estabelecidas pelo Comitê Central de Governança de Dados.
>
> Parágrafo único. As ferramentas de gestão da plataforma de interoperabilidade incluirão meios para que o gestor de dados tenha conhecimento sobre o controle de acesso e o consumo dos dados.

Assim, o compartilhamento de dados nos níveis restrito e específico, ou seja, restrito aos órgãos enumerados no decreto ou especificamente indicados no processo específico de intercâmbio de informações, deverá sempre ser formalizado por documentos de interoperabilidade, observadas as três leis analisadas por este trabalho, a LAI, a LGPD e a Lei nº 14.129/2021 (que será analisada adiante).

Fazendo acréscimos ao previamente apresentado art. 3º, no que tange aos dados pessoais, disciplina a necessidade de ser explicitado, quando do compartilhamento, o propósito legítimo e específico do ato, a compatibilidade entre a ação e a sua finalidade, e o dever de tratar-se de um compartilhamento mínimo de informações. Para o compartilhamento específico de dados, modalidade mais restrita, dispõe, ainda, o dever de condicionamento do compartilhamento à concessão de acesso pelo gestor dos dados, assim como o integral atendimento dos requisitos por ele definidos, incluindo o dever de implementação de todos os mecanismos de segurança da informação.

Outrossim, os dados recebidos por compartilhamento específico não podem ser retransmitidos pelos órgãos receptores, exceto quando existir autorização expressa do gestor de dados, anterior ou posterior ao recebimento:

> Art. 14. O compartilhamento específico de dados está condicionado:
>
> I - à concessão de permissão de acesso pelo gestor de dados; e
>
> II - ao atendimento dos requisitos definidos pelo gestor de dados como condição para o compartilhamento.
>
> § 1º Os requisitos exigidos pelo gestor de dados de que trata o inciso II do caput serão compatíveis com aqueles adotados internamente pelo próprio gestor de dados no tratamento da mesma informação.
>
> § 2º Os dados recebidos por compartilhamento específico não serão retransmitidos ou compartilhados com outros órgãos ou entidades, exceto quando previsto expressamente na autorização concedida pelo gestor de dados ou se houver posterior permissão desse.
>
> Art. 15. O órgão interessado em acessar dados sujeitos a compartilhamento específico enviará os documentos de interoperabilidade para o gestor de dados, observados as normas, as condições e os requisitos de acesso por ele estabelecidos, nos termos do disposto no inciso III do caput do art. 4º, e fundamentará o pedido e especificará os dados solicitados no maior nível de detalhamento possível.
>
> § 3º O recebedor de dados por compartilhamento específico é responsável por implementar e seguir as regras de segurança da informação estabelecidas pelo gestor de dados de compartilhamento específico, conforme o disposto no inciso III do caput do art. 4º.

Para total compreensão dos dispositivos, o decreto conceitua o gestor de dados como sendo o “órgão ou entidade responsável pela governança de determinado conjunto de dados” (art. 2º, XIII).

Por fim, em suas disposições finais e transitórias, confere ao Comitê Central de Governança de Dados, órgão que institui, a competência para dirimir eventuais controvérsias no compartilhamento de dados entre órgãos federais, e para revisar a categorização dos níveis de compartilhamentos de dados (art. 26, *caput* e § 4º).

CONCLUSÃO

A análise demonstrou que a LAI reafirma a publicidade como preceito geral e o sigilo como exceção. Ainda assim, o direito de acesso à informação não é absoluto, admitindo restrições fundadas em lei ou na imprescindibilidade da informação para a segurança da sociedade e do Estado.

Quanto ao compartilhamento, verificou-se que a LAI não impede o intercâmbio de

dados sigilosos entre órgãos públicos. O art. 25, § 2º, contudo, impõe a quem obtém acesso à informação classificada o dever de resguardar o sigilo, o que indica que a restrição atribuída na origem deve acompanhar o dado.

No caso das informações pessoais, a lei estabelece restrição de acesso independentemente de classificação e pelo prazo máximo de cem anos. O consentimento do titular é dispensado quando os dados forem necessários à proteção do interesse público e geral preponderante, desde que o uso se limite à atuação do órgão receptor.

Os decretos regulamentadores reforçam essa lógica. O Decreto nº 7.724/2012 condiciona o atendimento de pedidos a finalidades específicas e proporcionais. O Decreto nº 7.845/2012 exige credenciamento, ambientes seguros, recursos criptográficos e controle de acesso para as informações classificadas.

O Decreto nº 10.046/2019, por sua vez, explicita que o recebedor de dados sigilosos assume os deveres de sigilo e auditabilidade do custodiante. Também limita o compartilhamento de dados pessoais ao mínimo necessário e veda a retransmissão de dados recebidos por compartilhamento específico sem autorização do gestor.

Conclui-se que o compartilhamento de dados de acesso restrito entre órgãos públicos é admitido, mas condicionado à preservação do sigilo, à segurança da informação e à vinculação à finalidade. Esses deveres são complementados pela Lei Geral de Proteção de Dados Pessoais, que disciplina de forma específica o tratamento de dados pessoais pelo poder público.

REFERÊNCIAS

Cruz, Cláudio Silva da. Contas públicas: transparência e credibilidade. *In*: Oliveira, Aroldo Cedraz de (coord.). **O controle da administração pública na era digital**. 2. ed. Belo Horizonte: Fórum, 2017, p. 215-237.

Fernandes, Jacoby. **Você sabe o que é "auditabilidade"? Essa palavra existe mesmo?**. Disponível em:https://jacoby.pro.br/site/voce-sabe-o-que-e-auditabilidade-essa-palavra-existe-mesmo/. Acesso em: 25 jul. 2023.

Kaspersky. **O que é criptografia de dados?** Definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 10 ago. 2023.

Martins, Humberto. **Lei da transparência e sua aplicação na administração pública**: valores, direito e tecnologia em evolução. Disponível em: https://www.stj.jus.br/internet_docs/ministros/Discursos/0001182/LEI%20DA%20TRANSPA R%C3%8ANCIA%20E%20SUA%20APLICA%C3%87%C3%83O%20NA%20ADMINISTRA%C3%87%C3%83O%20P%C3%9ABLICA%20VALORES,%20DIREITO%20E%20TEC NOLOGIA%20EM%20EVOLU%C3%87%C3%83O.pdf. Acesso em: 25 jul. 2023.

Maximiliano, Carlos. **Hermenêutica e aplicação do direito**. 21. ed. Rio de Janeiro:

Forense, 2017.

Medeiros, Clayton Gomes de; Wacheleski, Marcelo Paulo. **A lei de acesso à informação e o princípio da transparência na administração pública**. Disponível em: http://www.publicadireito.com.br/artigos/?cod=4740fcb3becc721b. Acesso em: 08 ago. 2023.

Nobre Júnior, Edilson Pereira. A transparência administrativa e a Lei 12.527/2002. **Revista da Faculdade de Direito UFMG**, Belo Horizonte, n. 70, p. 249-276, jan./jun. 2017.Disponível em:https://revista.direito.ufmg.br/index.php/revista/article/view/1848. Acesso em: 05 mai. 2023.

Rosa, Antônio Quintino. Visão estratégia: governança e planejamento. *In*: Oliveira, Aroldo Cedraz de (coord.). **O controle da administração pública na era digital**. 2. ed. Belo Horizonte: Fórum, 2017, p. 173-213.

Valle, Vanice Regina Lírio do. Lei nº 12.527/2011 e o planejamento da ação estatal: uma interpretação orientada a prevenir a desinformação. **Revista de Direito Administrativo**, Rio de Janeiro, n. 267, p. 109-133, set./dez. 2014. Disponível em: https://periodicos.fgv.br/rda/article/view/46460/44451. Acesso em: 08 jun. 2023.