EXCELENTÍSSIMO SENHOR MINISTRO DO SUPREMO TRIBUNAL FEDERAL GILMAR MENDES

Arguição de Descumprimento de Preceito Fundamental n. 695/DF

O **LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET – LAPIN**, doravante também denominado "LAPIN", já qualificado nos autos do processo em epígrafe, vem, respeitosamente, perante Vossa Excelência, na qualidade de *AMICUS CURIAE*, apresentar

MANIFESTAÇÃO

nos termos do artigo 138, do Código de Processo Civil, c/c o artigo 323, do Regimento Interno do Supremo Tribunal Federal, pelos fatos e fundamentos a seguir.

SUMÁRIO

I. BREVE SÍNTESE

a. Da demanda

Trata-se de Arguição de Descumprimento de Preceito Fundamental ajuizada pelo Partido Socialista Brasileiro (PSB) em face da realização de acordo entre a Agência Brasileira de Inteligência (ABIN) e o Serviço Federal de Processamento de Dados (Serpro) para o compartilhamento de dados pessoais relativos aos registros de carteiras de habilitação de mais de 76 milhões de brasileiros.

Arguiu-se que compartilhamento de tal magnitude envolvendo dados pessoais violaria o direito à liberdade e à dignidade da pessoa humana, constantes nos art. 1º, III, e art. 5º, *caput* da Constituição, bem como os direitos à privacidade, à proteção de dados pessoais e à autodeterminação informativa, preceitos fundamentais protegidos pela Constituição Federal nos art. 5º, *caput* e incisos X e XII, e conforme jurisprudência desta Corte na ADI 6.387.

De acordo com a Postulante, tal compartilhamento traria riscos para a privacidade dos indivíduos, pois o volume de tal operação de compartilhamento afetaria a autodeterminação informativa de milhões de brasileiros indiscriminadamente. Por isso, essa operação não teria passado pelo crivo de um teste de proporcionalidade entre a magnitude de dados requisitados e os imagináveis propósitos buscados pelo sistema de inteligência, que não foram deixados claros pela ABIN.

Tudo isso se agravaria considerando que os trabalhos da Comissão Mista de Controle das Atividades de Inteligência no Congresso Nacional, responsável pela fiscalização da atuação da ABIN (art. 6º, Lei 9.883/99), estão suspensos por conta da pandemia do COVID-19.

Nesse sentido, em seu pedido principal, o Requerente requereu que o compartilhamento de dados baseado no acordo entre ABIN e Serpro fosse cessado imediatamente.

Subsidiariamente, foi pedida a interpretação conforme à Constituição dos artigos 1º, *caput* e incisos e 3º, incisos I, V e VI do Decreto 10.046/19 ("Decreto"),

para que, em casos que envolvam o tratamento de dados pessoais: **(i)** o rol do art. 1º seja considerado taxativo e exaustivo, de modo que o tratamento respeite o princípio da finalidade; **(ii)** se afaste a possibilidade de adequação da atividade de inteligência dentro do rol do art. 1º; e **(iii)** se garanta que o compartilhamento de dados na Administração Pública seja balizado pelos princípios de proteção de dados previstos na LGPD.

Por fim, houve o pedido de medida liminar determinando que houvesse a suspensão do compartilhamento e a proibição de acesso de tais informações pela ABIN e que se julgasse procedente a presente ADPF, afastando definitivamente a possibilidade do compartilhamento.

Em decisão interlocutória, o Excelentíssimo Ministro Relator Gilmar Mendes não concedeu a liminar pleiteada no que diz respeito ao pedido principal, tendo em vista a revogação do acordo realizado entre ABIN e o Serpro, conforme comunicação da Advocacia Geral da União.

Contudo, o Relator julgou subsistir relevância constitucional na matéria, considerando que o regime jurídico de compartilhamento de dados na Administração Pública é questão de extrema importância para a proteção do direito constitucional à privacidade.

Diante disto, **o Laboratório de Políticas Públicas e Internet - LAPIN vem, perante este Supremo Tribunal Federal, apresentar sua manifestação a respeito do tema**, visando contribuir com a discussão por meio de insumos a respeito de mecanismos a serem adotados para uma governança de dados na Administração Pública Federal brasileira que assegure o respeito à proteção de dados pessoais.

b. Desta manifestação

A presente ação constitucional toca em pontos de extrema importância para o exercício e a defesa do direito à proteção de dados pessoais, considerado "categoria autônoma de direito fundamental na ordem constitucional brasileira" pelo Ministro Gilmar Mendes na decisão interlocutória proferida nestes autos.

O papel da Administração Pública Federal (APF) no tratamento de dados pessoais pressupõe uma abordagem diferente daquele realizado pelas

organizações privadas. Enquanto estas utilizam dados principalmente para fins comerciais e, espera-se, sob o comando do próprio titular das informações, os propósitos do setor público são mais voltados ao oferecimento de serviços essenciais ao indivíduo.

Nesses casos, a relação entre controlador (Estado) e titular de dados (cidadão) é mais próxima a uma **dependência** do indivíduo do que a uma livre escolha de alocação de recursos econômicos para este ou aquele ente privado.[1]

Por conta disso, a regulação da interoperabilidade de dados entre entes estatais deve ser feita com o maior cuidado possível para proteger os direitos fundamentais previstos na Constituição. **Uma análise detalhada do Decreto 10.046/2019, a quem compete esse papel, é fundamental para julgar como o Estado pretende proteger os dados da população.**

Tendo isso em vista, **esta manifestação explora como o Decreto 10.046/2019 regula o tratamento de dados pessoais no âmbito da Administração Pública Federal (APF)**, tendo em vista a própria manifestação do Ministro Relator a respeito de como a análise da legislação tem especial importância nesse contexto para garantir o exercício do direito à proteção de dados. Será dado especial enfoque na forma como o disposto no Decreto se relaciona com os princípios de proteção de dados previstos na Lei Geral de Proteção de Dados (LGPD).

Para tanto, em primeiro lugar, será explorado como a LGPD se aplica ao tratamento de dados pelo setor público (**Seção II**), e, com base nisso, trataremos do art. 1º do Decreto 10.046/2019 para compreender a quais tipos de tratamento ele se aplica (**Seção III**).

Posteriormente, o enfoque será nos conceitos criados pelo Decreto e como eles se relacionam (ou deveriam se relacionar) com os termos utilizados pela LGPD (**Seção IV**). Em seguida, exploraremos os níveis de compartilhamento de dados estipulados pelo Decreto, ponto fundamental para a definição de quem terá acesso a quais dados e para quais fins dentro da Administração Pública

[1] BLACK, G. & STEVENS, L. ***Enhancing Data Protection and Data Processing in the Public Sector****: The Critical Role of Proportionality and the Public Interest.* Script Ed, Volume 10, *Issue* 1, Abril 2013. DOI: 10.2966/scrip.100113.93. P. 98,

Federal (**Seção V**). Este tema em específico é central para compreender o grau de compatibilidade do Decreto com os princípios e direitos previstos na LGPD.

As principais **conclusões** a que chegamos por este trabalho são:

1. O **rol do art. 1º do Decreto 10.046/2019 deve ser interpretado como taxativo**, não incluindo atividades de inteligência, segurança pública nem qualquer outro elemento que esteja fora do escopo da LGPD, de acordo com seu art. 4º;
2. Vários **conceitos apresentados pelo Decreto causam confusão com a LGPD** e já têm dado margem a falhas na governança de dados pessoais pela Administração Pública Federal (APF);
3. Da forma como estão apresentados, os dispositivos referentes aos **níveis de compartilhamento de dados previstos nos arts. 4º ao 15 do Decreto não garantem o cumprimento dos princípios e direitos previstos na LGPD**
4. O teor do Decreto 10.046/2019 falha também ao promover transparência, dado que **viola inclusive o disposto na Lei de Acesso à Informação (LAI)**.

Ao final, concordamos com a visão dos Proponentes desta ação de que uma **interpretação conforme à Constituição é necessária** para garantir que o Decreto seja aplicado de modo a garantir a proteção de dados no âmbito da Administração Pública Federal.

II. DA APLICAÇÃO DA LGPD NO TRATAMENTO DE DADOS PELO SETOR PÚBLICO

O regime geral de proteção de dados pessoais surge a partir do desenvolvimento histórico do conceito de privacidade[2], consubstanciado em uma Lei Geral de Proteção de Dados (LGPD) e no reconhecimento da proteção de dados pessoais como direito fundamental. Dessa forma, a adoção da norma geral busca definir diretrizes para serem respeitadas em todos os tratamentos de dados pessoais realizados na sociedade regulada, seja o tratamento realizado por particulares, seja por órgãos públicos. Esse modelo se espelha no adotado por diversos outros ordenamentos, como, por exemplo, o europeu, o canadense e o australiano.[3]

A LGPD, marco desse paradigma, foi promulgada e sancionada em 2018 e está em *vacatio legis*. Já o direito fundamental à proteção de dados pessoais foi reconhecido em decisão recente deste Tribunal, no julgamento de Medida Cautelar nas Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6393, 6390 (doravante referenciadas também como "ADI 6387")[4].

Isto posto, a LGPD aponta o sistema principiológico[5] a ser respeitado pelos agentes de tratamento particulares e públicos. Esses princípios coexistirão com normas setoriais, as quais poderão trazer previsões específicas não abarcadas pela construção regulatória geral, mas em concordância com o que ela dispõe. Isso faz com que se assemelhem à sistemática da legislação concorrente adotada pela Constituição Federal Brasileira, pela qual as normas específicas devem respeitar a norma geral[6].

---

[2] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar. 2006. Pp. 7-30.

[3] MENDES, Laura S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. Pp. 47-55.

[4] MENDES, Laura S. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais**. Portal Jota. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em 08.07.2020.

[5] Conforme o artigo 6º da Lei 13.709/18, as atividades de tratamento de dados pessoais deverão observar a boa-fé e diversos princípios expressamente previstos nos incisos deste artigo.

[6] MENDES, Laura S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. Pp. 47-55..

De acordo com Ana Frazão[7], a regulação jurídica verificada na LGPD deve servir como fio condutor para as diversas formas de regulação, como a autorregulação e o desenvolvimento do mercado, mecanismos que se somam aos princípios e direitos previstos na lei para combater imposições unilaterais de agentes de tratamento de dados como, por exemplo, o próprio Estado.

Nesse sentido, **a própria LGPD já prevê taxativamente a quais tratamentos ela não se aplica (art. 4º)**: o realizado por pessoa natural para fins exclusivamente particulares e não econômicos; o feito com finalidade jornalística e artística, acadêmica; para assegurar a segurança pública, a defesa nacional, a segurança do Estado, a investigação e a repressão de infrações penais; e o feito a partir de dados pessoais provenientes de fora do país e que não serão manejados no território nacional.

A regulação de tais atividades seguirão normas específicas, mas estão desde já vinculadas aos princípios da LGPD, conforme previsão do § 1º do art. 4º, da norma geral[8]. Além dessas matérias, os demais tratamentos de dados pessoais deverão respeitar a arquitetura regulatória proposta pela LGPD[9].

De acordo com esse entendimento, o Decreto 10.046/19, que dispõe sobre o compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão (CBC) e o Comitê Central de Governança de Dados (CCGD), também é regido pelos princípios basilares definidos pela LGPD, conquanto, em um primeiro momento, não se enquadre em nenhuma das situações excluídas da aplicação da LGPD. Mas, como mencionado, ainda que se enquadrasse em uma das matérias que não sofrem incidência da LGPD, os princípios base da lógica da norma geral deverão ser seguidos por todos os agentes de tratamento de dados pessoais.

---

[7] FRAZÃO, Ana. **Objetivos e alcances da Lei Geral de Proteção de Dados.** In: FRAZÃO, A. et. al. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. Pp. 125-126.

[8] Art. 4º, §1º, da LGPD: "O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei".

[9] MENEZES, J. et. al. **Quando a Lei Geral de Proteção de Dados não se aplica?** In: FRAZÃO, A. et. al. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. Pp. 171-172.

Em seu artigo 5º, o Decreto dispensa a celebração de instrumentos para a efetivação de compartilhamento de dados, mas prevê expressamente que essa dispensa está condicionada ao respeito à LGPD. Também nesse sentido, dispõe o **art. 3º, incisos I, V e VI**, do Decreto 10.046, sobre a necessidade de observância da LGPD para o tratamento de dados no âmbito do Poder Público Federal.

Ressalta-se que **a LGPD adotou um modelo *ex-ante* de proteção, em que o tratamento de dados só é possível com seu o enquadramento em uma das bases legais**, modelo semelhante ao europeu[10].

Essa escolha fica evidenciada a partir da leitura do *caput* do artigo 7º da LGPD, que assim dispõe: "o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses". Com isso, as hipóteses elencadas nos incisos do artigo 7º são situações taxativas nas quais o tratamento de dados deve se enquadrar para ocorrer. As hipóteses contam com previsões que destacam o papel do titular de dados, como o consentimento (inciso I), e outras que analisam o equilíbrio entre os interesses legítimos do controlador e do titular (inciso IX).

A mesma lógica é seguida ao longo da LGPD, que traz rol ainda mais limitante de bases legais para os casos de tratamento de dados sensíveis em seu artigo 11.

Em relação ao tratamento de dados pessoais realizado pelo Poder Público, a LGPD prevê, em seu Capítulo IV, regras gerais a serem respeitadas pelas entidades públicas. Esse tratamento deve se atentar aos princípios gerais trazidos pela lei, em especial ao da finalidade e o da transparência. Para garantir os direitos do titular, a norma geral utiliza inclusive de instrumentos já previstos em outras legislações esparsas, como a Lei nº 9.507/97 (Lei do *Habeas Data*) e a Lei nº 12.527/11 (Lei de Acesso à Informação)[11].

Respeitando a ideia de uma norma geral, a LGPD busca garantir que o tratamento de dados pessoais pelas entidades públicas seja feito de forma

[10] BIONI, B. R. et. al. **Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência.** In: FRAZÃO, A. et. al. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. Pp. 810-812.

[11] SOUSA, R. et. al. **Acesso à informação e ao tratamento de dados pessoais pelo Poder Público**. Inf. & Soc.: Est. João Pessoa, v. 29, n.1. 2019. Pp. 237-251.

interoperável e racional e para fundamentar a realização de políticas públicas[12], mas reforçando a ideia de respeito ao princípio da finalidade.

Essa construção reforça o modelo *ex-ante* de proteção, ao estipular que **o tratamento de dados pelo Estado deve ser feito desde que fundamentado em uma das hipóteses legais, tenha o interesse público como objetivo e apresente informações claras a respeito de para qual finalidade os dados serão tratados** (art. 23, I, LGPD). Vale ressaltar que a importância de o setor público cumprir com esses comandos se expressa principalmente ao se considerar a grande quantidade de dados que é tratada pelo Estado[13].

Por essa razão, a norma brasileira trouxe em seu art. 7º, inciso III, a possibilidade restrita de tratamento para a execução de políticas públicas e, ainda, em seu art. 23, uma base legal mais ampla para abranger os diversos serviços prestados pelo Estado:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> (...)
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> 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

[12] O art. 25 da LGPD dispõe sobre o tratamento de dados pelo Poder Público: "*Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral*."
[13] BLACK & STEVENS, Op. Cit., pp. 99-101.

> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

Ou seja, a própria LGPD possibilita que o tratamento de dados pessoais pelo Poder Público seja realizado, desde que observados os princípios que regem esse sistema, reforçando a ideia de que a norma geral deve servir como guia para garantir uma política de proteção de dados forte. A existência de um regime homogêneo entre os diferentes órgãos do Poder Público mitiga os riscos inerentes ao tratamento de dados pessoais, ao passo que a existência de diferentes microssistemas, com sistemas e classificações distintas, diminui a confiabilidade nas instituições públicas quando tratam dados[14].

Por conseguinte, a fim de preservar o princípio da legalidade e garantir o regime rígido de proteção de dados pessoais, **a aplicação e a interpretação do Decreto 10.046/19 devem respeitar o sistema de proteção estabelecido pela LGPD,** que, apesar de ainda não estar em vigor, já teve seus princípios reconhecidos como fundamentais para garantia do direito constitucional à proteção de dados. Nesse sentido, destaca-se a decisão da relatora, Ministra Rosa Weber, referendada pelo plenário, no julgamento da Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 688, 6389, 6390 e 6393:

> Nessa ordem de ideias, não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida. E tal dever competia ao Poder Executivo ao editá-la.
>
> Nessa linha, **ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.** Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva.
>
> (...)
>
> Essas considerações são corroboradas pela manifestação trazida aos autos pela Agência Nacional de Telecomunicações – ANATEL, que destacou necessária "a observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações". E recomendou a **adoção de medidas visando a adequar a medida à garantia dos princípios estabelecidos na**

[14] Ibid.

> **Constituição Federal, na Lei Geral das Telecomunicações e na Lei Geral de Proteção de Dados,** de modo a assegurar a proteção da privacidade, da intimidade e dos dados pessoais de usuários de serviços de telecomunicações (...) (Grifos aditados)

Considerando a relevância da observância à LGPD para a garantia do direito à proteção de dados, o provimento do pedido de realização de interpretação conforme à Constituição realizado na presente demanda é fundamental para garantir que a aplicação do Decreto 10.046/19 será submetida à LGPD e, portanto, respeite a privacidade e a proteção de dados dos titulares de dados.

Por outro lado, o papel da LGPD enquanto norma geral que o Decreto 10.046/2019 pretende regular conduz a outro ponto de extrema importância: a análise de se o Decreto se aplica ou não às hipóteses sobre as quais a LGPD não impera, o que inclui atividades de inteligência (art. 4º, III, c, LGPD). A próxima seção explora esse tema.

III. DA TAXATIVIDADE DO ROL DO ART. 1º DO DECRETO 10.046/19

Diante da sistemática trazida pela Lei Geral de Proteção de Dados, em especial em vista das disposições dos artigos 7º e 11, **o rol do art. 1º do Decreto 10.046/19 deve ser interpretado como taxativo**. Tal visão deriva de um argumento de ordem principiológica, envolvendo a aplicação dos princípios da adequação, necessidade e finalidade previstos no art. 6º da LGPD e da aplicação do princípio da legalidade na seara da proteção de dados pessoais.

A Lei Geral de Proteção de Dados, ao prever a aplicabilidade dos princípios da finalidade, adequação e necessidade nos incisos I a III, respectivamente, do artigo 6º da referida Lei, prevê um **modelo de tratamento de dados pessoais que visa restringir as possibilidades onde o tratamento pode ocorrer**.

Isto ocorre porque esses três princípios servem de linha-mestra interpretativa ao se realizar o tratamento de dados, inibindo condutas desproporcionais, visando garantir o respeito à autodeterminação informacional e à privacidade dos indivíduos, vide art. 2º da Lei Geral de Proteção de Dados.

A norma traz ainda, em seu Capítulo IV, regras específicas para o tratamento de dados pessoais pelo Poder Público. Enquanto o art. 23 limita o rol de hipóteses legais para o tratamento nesse contexto, o art. 26 as restringe ainda mais quando a operação de tratamento for o compartilhamento de dados.

Nesse sentido, **o artigo 26 da LGPD deixa claro que compartilhamento de dados entre a Administração Pública deve se ater às finalidade específicas de execução de políticas públicas e de cumprimento de obrigações legais,** restringindo o campo de hipóteses legais aplicáveis neste contexto.

Ademais, o art. 37 da Constituição Federal, ao estabelecer o **princípio da legalidade** como um dos princípios basilares da Administração Pública, **restringe a atuação do Estado a apenas aquilo que lhe é permitido por lei**[15]. Da leitura do princípio constitucional com o disposto na LGPD, conclui-se que as hipóteses para compartilhamento de dados pela Administração Pública devem estar

[15] FILHO, José dos Santos Carvalho. **Manual de Direito Administrativo.** 32ª ed. São Paulo: Atlas. 2018. P. 73.

embasadas em fundamentos legais que estabeleçam finalidades específicas para esse tipo de tratamento.

Isto mostra que há uma faixa de sobreposição no que tange aos princípios da finalidade e da legalidade no âmbito do tratamento de dados (e subsequentemente o compartilhamento) pela Administração Pública, que indicam que as finalidades que legitimam o Estado a fazer o compartilhamento de dados devem estar previstas na legislação de forma explícita.

Deste modo, a leitura do Decreto 10.046/19 deve ser balizada pelas regras estabelecidas na LGPD, e as hipóteses trazidas pelo artigo 1º do Decreto devem ser lidas como a explicitação das finalidades que o Estado elencou como legítimas para a realização do compartilhamento de dados pessoais entre órgãos da Administração Pública Federal. Isso indica que **não deve a autoridade pública ir além do que dispõem as hipóteses legais da LGPD, sob o risco de violar o princípio da legalidade da Administração Pública.**

É sobre esta ótica que se deve analisar o rol do artigo 1º do Decreto 10.046/19: **como Decreto, instrumento normativo infralegal, ele tem o condão de regulamentar as hipóteses em que o compartilhamento é possível, desde que restrito às limitações da lei sobre a qual se baseia, que é, no caso, a LGPD.** Uma leitura diversa importaria entender que a Administração Pública não está adstrita aos termos dos próprios atos normativos que ela edita.

Caso contrário, o artigo 1º do Decreto servirá como verdadeira carta em branco para a Administração Pública Federal (APF), permitindo-lhe compartilhar dados entre si sem qualquer tipo de controle. Tal tipo de postura poderá abrir brechas para que sejam violados os princípios da finalidade, adequação e necessidade.

Ademais, a LGPD, em seu art. 4º, III, c,[16] afirma que ela não se aplica ao tratamento de dados pessoais para fins de segurança do Estado, o que inclui atividades de inteligência. Uma vez fora do escopo da LGPD, portanto, tampouco pode esse tipo de atividade ser regulado pelo Decreto 10.046/19.

[16] "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
III - realizado para fins exclusivos de:
c) segurança do Estado;"

Essa conclusão também é tirada da própria análise do rol de objetivos previsto no art. 1º do Decreto. O dispositivo apresenta 5 finalidades que a Administração Pública Federal pode perseguir no compartilhamento de dados entre seus órgãos e entidades:

> I - simplificar a oferta de serviços públicos;
> II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;
> III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;
> IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e
> V - aumentar a qualidade e a eficiência das operações internas da administração pública federal.

Uma breve análise permite observar que o rol estabelecido visa promover o cumprimento do princípio da eficiência administrativa (CF, art. 37). Isso porque pretende aprimorar a máquina pública no que diz respeito à oferta de serviços públicos (inciso I), ao desenvolvimento de políticas públicas (inciso II), ao acesso e manutenção de benefícios sociais e fiscais (inciso III) e para assegurar maior qualidade e fidedignidade dos dados custodiados pela APF (inciso IV).

Todos esses objetivos se referem, portanto, a hipóteses previstas pela LGPD como passíveis de fundamentar tratamentos de dados pessoais, já que dizem respeito a obrigações legais e ao desenvolvimento de políticas públicas que não recaem sobre as exceções descritas no art. 4º, da LGPD.

Finalmente, no que diz respeito ao inciso V, identifica-se um objetivo específico de eficiência das operações da APF, o que inclui uma série de órgãos que vão além inclusive do escopo da LGPD. A ABIN é um deles: uma vez parte da Presidência da República, também pertence à Administração Pública Federal.

No entanto, considerando que as atividades-fim da ABIN não estão no escopo da LGPD e não podem ser consideradas como de políticas públicas, fica clara a sua dissonância com os incisos do art. 1º do Decreto, bem como com a própria LGPD, na qual se fundamenta.

Deste modo, a ABIN só estaria autorizada a se valer das regras de compartilhamento de dados do Decreto nº 10.046/2019 nas hipóteses em que atuasse em sua **atividade-meio**, de caráter administrativo, mas nunca quanto às suas atividades-fim, de serviços de inteligência. Isso se restringiria ao compartilhamento de dados de servidores da ABIN para realização de processos de recursos humanos, por exemplo, mas não para realização de atividades de segurança nacional.

Ainda assim, tal compartilhamento deveria ser feito com cautela, em observância ao **princípio da precaução**, previsto no art. 6º, inciso VIII, da LGPD.

O princípio da precaução prevê que é necessário que se adote todas as medidas possíveis para prevenir danos que poderão advir do tratamento de dados. Tal noção é emprestada do direito ambiental, onde significa que atos que possam causar grande degradação ambiental só podem ser realizados se existirem precauções adequadas para evitar o dano. Caso não existam, não será possível a realização do ato diante do risco de dano.[17] O cerne do princípio é uma análise de risco de dano que o ato poderá causar.

Quando aplicado à proteção de dados, o princípio implica na necessidade de analisar a possibilidade de um tratamento bem como as salvaguardas a serem postas em prática com base nos riscos de dano que ele poderá causar. Caso os riscos sejam altos demais para as salvaguardas disponíveis, o tratamento não poderá ser realizado.[18]

Há de se ter em mente que o compartilhamento de dados pessoais da Administração Pública com uma agência de inteligência, ainda que para o exercício de suas atividades-meio, deve ser feito com procedimentos especiais de proteção de dados e da privacidade, para evitar desvios de finalidade no tratamento dos dados.

No entanto, existiria ainda assim um alto risco em permitir o livre compartilhamentos de dados com serviços de inteligência. Afinal, a ABIN teria ampla margem para desvirtuar o uso desses dados ao eventualmente aplicá-los

[17] AMARO, Frederico. **Direito Ambiental Esquematizado.** 5ª ed. Rio de Janeiro: Forense. 2014. P. 86.
[18] GELLERT, Raphaël. Understanding Data Protection As Risk Regulation. **Journal of Internet Law**, vol. 18, 2015, n. 11, P. 23.

às suas atividades-fim, dado que teria grande facilidade em acessar dados pessoais em poder de outros órgãos e utilizá-los para fins de vigilância estatal.

Isso se agrava ao levar em consideração a falta de mecanismos existentes para garantir supervisão e transparência a respeito dos processos internos de acesso a esse tipo de informação. Vale lembrar que o Brasil não tem instituída sequer sua Autoridade Nacional de Proteção de Dados para atuar como supervisora desse tipo de compartilhamento.

Por isso, levando em conta o princípio da precaução, que prevê que tratamentos não poderão ser realizados caso os riscos envolvidos sejam altos demais para as salvaguardas disponíveis, **deve-se considerar incompatível com a LGPD o compartilhamento de dados com a ABIN nos termos trazidos pelo Decreto 10.046/2019, ainda que meramente para cumprimento de suas atividades-meio.**

Um outro ponto que merece atenção é o fato de que as atividades de inteligência não são regidas diretamente pela LGPD, uma vez que o art. 4º, inciso III, excluiu do escopo da legislação as atividades de segurança pública, investigação e repressão de infrações penais, que estão estritamente relacionadas com o serviço de inteligência.

Isto significa que, como a LGPD não se aplica às atividades finalísticas da ABIN, tampouco o Decreto 10.046/2019 poderá ser utilizado nesse contexto. Afinal, enquanto norma regulamentadora de lei cuja hierarquia é superior, o Decreto deve se ater a seu escopo de abrangência.

Voltando ao caso concreto, do compartilhamento de dados entre ABIN e Serpro, embora a Agência não tenha revelado para que finalidade ela desejava o compartilhamento das CNHs dos cidadãos brasileiros, deve-se presumir que o interesse era para sua atividade-fim já que as funções administrativas do órgão não necessitariam do compartilhamento desses documentos. Em vista do exposto acima, isso basta para levar à conclusão de que tal compartilhamento não pode ser feito com base no Decreto 10.046/2019.

Cumpre ainda ressaltar que, embora as atividades de inteligência estejam excluídas do escopo da LGPD, esta lei não deixou as operações de tratamento para tais finalidades fadadas ao vazio legislativo. Isto porque o § 1º do art. 4º

deixou claro que legislação específica deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, **observados o devido processo legal, os princípios gerais de proteção e os direitos do titular** previstos nesta Lei.

Ou seja, conquanto a LGPD não se aplique diretamente nos contextos das atividades do inciso III do art. 4º, o devido processo legal, os princípios gerais do art. 6º da LGPD, e os direitos previstos nesta lei deverão ser respeitados desde já. O mero fato de as atividades de inteligência não estarem no escopo da LGPD não exime a ABIN da necessidade de tomar todas as salvaguardas necessárias para a proteção dos dados pessoais dos indivíduos afetados, o que inclui o respeito aos direitos e princípios da Lei Geral de Proteção de Dados.

IV. DA INCOMPATIBILIDADE DE CONCEITOS

O Decreto 10.046/2019, ao pretender regulamentar o tratamento de dados no âmbito da administração pública federal, institui diretrizes para o seu compartilhamento entre órgãos públicos. No entanto, apesar de, em seu preâmbulo, referenciar a Lei Geral de Proteção de Dados, percebe-se uma **falta de compatibilidade entre os conceitos apresentados no Decreto**, como dados cadastrais e gestor de dados, **e conceitos-chave da LGPD e do o Marco Civil da Internet (MCI),** como dado pessoal, controlador e operador de dados.

a. Dados Pessoais

As primeiras divergências entre os instrumentos surgem no que diz respeito aos dados que são objeto do Decreto. Apesar de fazer referência, em seu art. 3º, V, à obrigação de que todo tratamento de dados pessoais deve observar a proteção de dados, **conceitos como "dados cadastrais", "atributos biográficos" e "atributos biométricos" são introduzidos sem a devida atenção ao que outras leis já haviam instituído sobre a natureza dessas informações.**

No que diz respeito ao conceito de **dados cadastrais**, por exemplo, o Marco Civil da Internet assinalava que esses dados equivaleriam à "qualificação pessoal, filiação e endereço" de um indivíduo (art. 10, §3º). Especificamente quanto ao conceito de qualificação pessoal, o Decreto 8.771/2016, que regulamenta o MCI, a descreve como "nome, prenome, estado civil e profissão do usuário".

Com isso, seriam dados cadastrais, de acordo com o MCI: (1) nome, prenome, estado civil e profissão do usuário; (2) filiação; e (3) endereço.

Contudo, o que se constata é que o Decreto 10.046/2019 vai de encontro à lógica estipulada no Marco Civil da Internet, já que inclui os dados descritos como cadastrais pelo MCI no conceito de **atributos biográficos** (art. 2º, I). Como se não fosse suficiente, cria outra categoria também chamada de **dados cadastrais** para incluir "informações identificadoras perante os cadastros de órgãos públicos" (art.

2º, III), como CPF, PIS, PASEP e NIS, bem como dados vinculados a pessoas jurídicas, como o CNPJ.

Com isso, o Decreto amplia a confusão conceitual no ordenamento jurídico, agravada pelo fato de **desrespeitar uma norma de hierarquia superior**.

Vale chamar atenção de que, apesar de quase todos os dados citados serem pessoais, não é especificada sua relação com o conceito de **dado pessoal**, descrito pela LGPD como "informação relacionada a pessoa natural identificada ou identificável". Essa específica falta de compatibilização se agrava considerando a confusão que existe no Brasil a respeito de como dados cadastrais se relacionam com a definição de dados pessoais, presente na LGPD.

Um exemplo dessa falta de compreensão pode ser extraído de um trecho de carta assinada por ex-presidentes do IBGE a respeito da Medida Provisória n. 954, que determinava o compartilhamento dos dados de nome, telefone e endereço de todos os clientes de telefonia no Brasil ao IBGE para realização de "estatísticas oficiais" e teve sua eficácia suspensa por esta Corte durante o julgamento da Ação Direta de Inconstitucionalidade nº 6.387. De acordo com os redatores da carta, "os dados [coletados pela MP] não incluem informações pessoais"[19], uma observação equivocada, se tomado como base o disposto na LGPD.

Além disso, dados considerados pela LGPD como **dados sensíveis**, que são qualquer "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" (art. 5º, II, LGPD), são diluídos no Decreto.

Um exemplo é, no contexto dos **atributos biográficos**, a inclusão de dados relativos a grupo familiar. A depender do contexto, esse tipo de informação pode indicar, por exemplo, aspectos sobre a vida sexual do titular de dados, como se é homossexual, por exemplo. Isso se enquadra no conceito de dado sensível, o que exige a adoção de mecanismos mais protetivos de segurança e privacidade.

[19] Simon's Site. **Precisamos das estatísticas do IBGE para ajudar a vencer o COVID-19. 20 abr. 2020**. Disponível em http://www.schwartzman.org.br/sitesimon/?p=6488. Acesso em 23 abr. 2020.

Demais exemplos de dados sensíveis citados pelo Decreto também são encontrados em **atributos biométricos**, tidos como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar". No entanto, não é explicitado qual seria a finalidade ou o grau de proteção e segurança adotado para uso desses dados, cuja natureza sensível ocorre justamente pela ampla margem que dão para fundamentarem atividades de vigilância estatal.

A esse respeito, o tratamento de dados genéticos para controlar cidadãos é o mais recente estágio da política de vigilância chinesa. O jornal New York Times tornou público um projeto do governo chinês para criar um banco de dados de seus mais de 700 milhões de cidadãos homens por meio de coletas de sangue que têm sido realizadas muitas vezes sem o consentimento de seus doadores.[20]

De acordo com a justificativa oficial, a política tem por intuito capturar criminosos. No entanto, a pesquisadora Maya Wang, da organização Human Rights Watch, afirma que "a habilidade das autoridades de descobrir quem é parente de quem, dado o contexto de punições a famílias inteiras como resultado do ativismo de uma só pessoa terá um efeito inibidor na sociedade como um todo".[21]

Considerando o exemplo chinês, é inevitável levantar dúvidas a respeito de o que o governo brasileiro pretende fazer com dados tão sensíveis como a forma de andar dos cidadãos. É difícil imaginar que qualquer política pública tenha uma necessidade tão grande de utilização desse tipo de dado. Vale lembrar que o uso de dados sensíveis, quando não obtidos via consentimento, só pode ser realizado se **indispensável** para determinada finalidade, de acordo com o art. 11, II, da LGPD [22].

---

[20] WEE, Sui-Lee. **China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment.** The New York Times. 17 jun. 2020. Disponível em https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html. Acesso em 2 jul 2020.

[21] *Idem*.

[22] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
II - sem fornecimento de consentimento do titular, **nas hipóteses em que for**

b. Gestor de dados

Outro conceito que não encontra paralelo com a LGPD é o de **gestor de dados,** definido no Decreto como o "órgão ou entidade responsável pela governança de determinado conjunto de dados" (art. 2, XIII). Ele é que será responsável por definir os critérios de compartilhamento dos dados (art. 4º, §1º), incluindo quem terá acesso a um conjunto de dados e quais as permissões necessárias para tal. O gestor de dados poderá determinar a total ausência de barreiras de acesso, ou seja, ampla disponibilização dos dados a qualquer um que o requisitar, até regras para compartilhamento específico.

O Decreto não deixa claro, no entanto, **como a figura do gestor de dados se relaciona à do controlador ou do operador de dados pessoais**, que são os entes a serem responsabilizados por violações à proteção de dados de indivíduos. Nos termos da LGPD, controlador é a quem competem as decisões referentes ao tratamento de dados pessoais, enquanto o operador é que, realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VI c/c VII, LGPD).

Definir como se enquadra o gestor de dados à luz da LGPD é de suma importância para permitir o exercício de direitos como o de acesso ou retificação de dados pelo titular (art. 18, LGPD), bem como para a definição do grau de responsabilidade de cada responsável pelo tratamento (art. 42 a 45, LGPD).

Os poderes reservados ao gestor de dados são delicados. Por eles, um gestor é capaz, por exemplo, de garantir amplo acesso a informações como com quem uma pessoa reside ao tornar público seu grupo familiar. Em última instância, o compartilhamento indevido desses dados pode levar à exposição de grupos vulneráveis,, como, por exemplo, ao tornar público que uma determinada pessoa reside com um companheiro do mesmo sexo.

Também não são especificados quaisquer meios pelos quais o gestor de dados se responsabilizará pelo tratamento que descumprir o disposto na LGPD, seja ele feito sob sua supervisão ou por outro agente que obtiver o dado com base na classificação estipulada pelo gestor.

---

indispensável para:"
(Grifos aditados)

Tendo em vista todos os problemas apresentados a respeito da figura do gestor de dados, a única forma de tornar a figura do gestor conforme à LGPD é a equiparando à do **controlador de dados**. Afinal, considerando que o gestor será o "órgão ou entidade responsável pela governança de determinado conjunto de dados" (art. 2º, XIII, Decreto 10.046/2019), bem como o responsável por determinar quais dados se referem a cada categoria de compartilhamento e consequentemente gerir os controles de acesso (art. 4º, §1º, c/c art. 7º, par. único, Decreto 10.046/2019), é de se concluir que é a ele que "competem as decisões referentes ao tratamento de dados pessoais", como ocorre exatamente com o controlador.

Foi pela confusão gerada a partir dessa miscelânea de conceituações e pelo apego à noção de categorias estanques para tratamento de dados pessoais que quase se permitiu que dados obtidos para regulação do sistema de trânsito fossem repassados massivamente para a ABIN, desvirtuando completamente a finalidade para a qual foram inicialmente coletados e o âmbito de incidência da LGPD e do Decreto. Por isso, **uma leitura constitucional que estenda os princípios da proteção de dados à aplicação do Decreto 10.046/2019 é essencial**, inclusive para garantir **proporcionalidade** no uso de dados pessoais pela administração pública.

V. DOS NÍVEIS DE COMPARTILHAMENTO DE DADOS PROPOSTOS PELO DECRETO 10.046/2019 E DOS PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

De modo a compreender como o Decreto 10.046/2019 já está produzindo efeitos em relação à proteção dos dados pessoais detidos pelo governo, vale examinar como outras entidades da administração pública federal têm sido instruídas a respeito de como operacionalizar suas regras de compartilhamento.

O Decreto 10.046/2019 determina, nos incisos de I a III, do art. 4º, que os dados serão compartilhados de acordo com três níveis de compartilhamento, que definem quem terá acesso a quais dados pessoais:

I. **"compartilhamento amplo**, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;

II. **"compartilhamento restrito**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e

III. **"compartilhamento específico**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados."

Para análise das categorias estipuladas, também tomaremos como parâmetro o conteúdo de documentos emitidos pelo Comitê Central de Governança de Dados (CCGD), como as **Regras para Compartilhamento de**

Dados - CCGD[23] (doravante referenciado "Regras"), de 4 de maio de 2020, e a **Apresentação das Regras de Compartilhamento**[24] (doravante referenciado "Apresentação").

Tais publicações estabelecem parâmetros para guiar o trabalho de categorização dos dados de acordo com os níveis de compartilhamento determinados pelo Decreto. No entanto, antes de passar ao exame de cada categoria individualmente, vale analisar o paradigma sobre o qual os níveis de compartilhamento foram estruturados.

DO CONTEXTO DOS DADOS

Da leitura dos incisos citados, observa-se que os níveis de compartilhamento trabalham com uma **categorização estanque dos dados pessoais**. Essa visão promove que dados específicos, **independentemente do contexto** em que foram coletados ou em que serão aplicados, observarão as mesmas regras de controle de acesso.

É o que se conclui ao analisar que determinados dados serão abertos ao público (inciso I), a qualquer órgão da administração pública federal (inciso II) ou a órgãos específicos (inciso III), **independentemente da observância da finalidade** visada pelo requerente dos dados. Para agravar a situação, a revisão das regras será feita apenas uma vez a cada cinco anos, ou quando for conveniente para a administração (art. 4º, §6º).

A disciplina da proteção de dados pela LGPD, assim como pelo regulamento europeu, se baseia em uma abordagem de risco para direcionar os esforços de controladores de dados a respeito de quais salvaguardas devem ser postas em prática para garantia da proteção de dados e da privacidade.[25] Isso

[23] CCGD. **Regras para Compartilhamento de Dados CCGD.** 4 mai 2020. Disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf. Acesso em 1º jun 2020.
[24] CCGD. **Apresentação das Regras de Compartilhamento**. Disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/apresentacao_categorizacao_2020-abril-02.pdf. Acesso em 1º jun 2020.
[25] Information Commissioner's Office (ICO). **Data protection by design and default**. Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/. Acesso em 30 de junho de 2020.

se reflete na obrigação do art. 46 da LGPD, que institui o *privacy-by-design* como medida fundamental para *compliance* com a norma, bem como na adoção de boas práticas de governança (art. 52, §1º, IX) como aspecto a ser sopesado na imposição de sanções pela Autoridade Nacional de Proteção de Dados.

Com isso, **o juízo sobre a sensibilidade dos dados** e, com ela, a exigência de mais ou menos medidas de segurança a serem implementadas, depende do risco que **envolve o contexto em que ocorre o tratamento de dados e as expectativas do titular em relação a como suas informações serão utilizadas**.

A teoria da **privacidade contextual** é uma importante referência para delimitar o âmbito de aplicação da proteção de dados no tratamento de informações de acordo com o contexto em que ocorrem. Um dos objetivos da teoria é de **superar a noção de que existem dados que *a priori* devem ou não ser protegidos.**[26]

Helen Nissenbaum, que cunhou o termo, afirma que todos os espaços que ocupamos em nossas vidas são dotados de regras para o fluxo de informações, o que chama de **normas informacionais** (*norms of information flows*).[27]

Essas normas seriam próprias para cada contexto social em que nos inserimos. Elas se dividem em **normas de conveniência** (*appropriateness*), que revelam quais informações são apropriadas para serem reveladas sobre um indivíduo em uma situação específica,[28] e **normas para distribuição de informação** (*distribution of information*), que se referem à distribuição de um dado pessoal de uma pessoa a outra.[29]

Normas de conveniência estipulam que, em condições normais, uma pessoa expresse sua visão política para um amigo mas não necessariamente para seu superior no trabalho.[30] Já um exemplo de norma de distribuição é o de que um delicado segredo contado para uma amiga não seja compartilhado com um terceiro.[31]

---

[26] NISSENBAUM, Helen. **Privacy as Contextual Integrity.** Washington Law Review, v. 79, 2004.
[27] *Idem,* p. 119.
[28] *Idem,* p. 120.
[29] *Idem*, p. 122.
[30] *Idem*, p. 121.
[31] *Idem*, p. 123.

Uma violação à privacidade pode ocorrer caso qualquer um desses dois tipos de normas seja violado.[32] Nesse sentido, Helen Nissenbaum afirma que o que mais preocupa as pessoas não é a mera restrição do fluxo de informações pessoais de que é titular, mas a garantia de que esse fluxo seja feito de forma apropriada.[33]

Ao permitir um fluxo indiscriminado de dados dentro da administração pública federal sem atentar à finalidade e ao contexto em que são tratados, o Decreto viola essas normas de fluxo informacional, mais especificamente as de normas de distribuição de informação descritas por Nissenbaum.

Nesse sentido, o Decreto, bem como as Regras que pretendem instruir sua aplicação, se atêm a uma noção ultrapassada de privacidade, que foca estritamente na categorização *a priori* de dados.

Descrita a visão sobre o porquê de todo dado dever ser protegido, cabe trazer à luz o **debate sobre a dicotomia entre dados pessoais e dados pessoais sensíveis**, cuja **fluidez** é maior do que se conclui de uma leitura superficial da LGPD.

A depender do contexto, dados inicialmente não listados como sensíveis pelo art. 5º, II, da LGPD, podem vir a ser considerados como tais graças a informações adicionais que permitem acessar. Um exemplo são os dados de **geolocalização**.

Apesar de não estarem descritos nem na LGPD nem na lei europeia como dados sensíveis, a importância de tratar a localização de um indivíduo como sensível[34] advém da possibilidade de revelar, por exemplo, que ele compareceu a um hospital, revelando um dado de saúde, ou frequentou determinado ambiente LGBTQ+, dado sobre sua vida sexual. Tanto dados de saúde quanto sobre a vida sexual são considerados sensíveis.

---

[32] *Idem*, p. 125.
[33] NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford University Press, Stanford, California. 2010, p. 2.
[34] Commission Européenne. **Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données.** 17 abr. 2020. Disponível em https://ec.europa.eu/info/sites/info/files/5_fr_act_part1_v3.pdf. Acesso em 1º jul. 2020.

O mesmo se aplica a um identificador como o **CPF**. A princípio, trata-se de dado não incluso no rol de dados sensíveis pela LGPD. No entanto, ao figurar em uma lista de filiados a determinado partido, por exemplo, o CPF se torna um dado capaz de revelar a opinião política do filiado, e passa a refletir um dado sensível.

DOS PRINCÍPIOS DE PROTEÇÃO DE DADOS

Intrinsecamente relacionado à noção de contexto e já citado de passagem acima, um importante princípio trazido pela LGPD é a **finalidade**. Saber o propósito para o qual um dado será tratado é indispensável identificar quais informações são de fato necessárias para alcançar determinado fim e, com isso, avaliar a própria conveniência de usar ou não um dado específico. O princípio da finalidade também é importante para identificar quais as medidas de segurança apropriadas, o que inclui controles de acesso e limitações temporais.

Dados tratados pelo poder público dificilmente utilizarão a base legal do consentimento como hipótese para tratamento. Por isso, avaliar a **necessidade** da informação para obtenção do fim almejado é fundamental.

Um juízo de **necessidade** pressupõe que dados só podem ser tratados se esse tratamento for proporcional e reduzido ao mínimo necessário para alcançar determinada finalidade. Na LGPD, esse princípio anda lado a lado com o da **adequação**, que estipula que a finalidade dos dados tratados deve ser compatível com aquela informada ao titular de acordo com o contexto do tratamento.[35]

O *Information Commissioner's Office* especifica que o tratamento de dados pessoais para cumprimento de funções públicas deve atentar a uma análise de necessidade, pela qual o tratamento deve ser direcionado e proporcional para atender um propósito definido. Nesse sentido, não seria

[35] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

permitido o tratamento se houvesse outra forma razoável e menos intrusiva de alcançar o mesmo resultado.[36]

A esse respeito, uma série de medidas podem ser aplicadas para garantir a integridade desse direito. Isso inclui **minimizar** a quantidade de dados processados, de modo a garantir que só aqueles adequados e necessários ao uso que se tem em vista. Ademais, aplicar técnicas como a pseudonimização e garantir **transparência** no uso dos dados são atitudes tidas como fundamentais para garantir o respeito à privacidade do titular.[37]

A importância da noção de contexto e sua relação com a finalidade encontram paralelo, por exemplo, nos dados tornados públicos por usuários de mídias sociais. Vários pesquisadores começaram a utilizar essas informações para buscar indicativos de depressão ou alcoolismo em determinado grupo social.[38]

A coleta de dados pessoais em redes sociais normalmente garante acesso em primeira mão aos comportamentos, pensamentos e sentimentos de uma determinada população, indicativos de seu bem-estar emocional.[39] No entanto, o uso desse tipo de dado pessoal para pesquisa tem implicações éticas que se referem à quebra das **expectativas do indivíduo** quanto ao uso de seus dados, que passa a ocorrer fora do contexto e da finalidade para os quais os forneceu. Remetendo novamente à teoria da privacidade contextual, isso provavelmente afetaria as normas de fluxo de distribuição.

Nesse sentido, ao contrário da lógica que permeia o Decreto, principalmente quanto aos níveis de compartilhamento amplo e restrito, não é simplesmente porque determinada informação é pública e disponível que qualquer uso ulterior pode ser considerado ético.[40] Usos de dados que podem ser

---

[36] Information Commissioner's Office. **Public Task**. Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/.
[37] Information Commissioner's Office, **Data protection by design and default**. Op. Cit.
[38] CONWAY, Mike & O'CONNOR, Daniel. **Social Media, Big Data, and Mental Health**: Current Advances and Ethical Implications. Current Opinion in Psychology Volume 9, Junho 2016, Pages 77-82. Disponível em https://www.sciencedirect.com/science/article/pii/S2352250X16000063?via%3Dihub. Acesso em 1º jul. 2020.
[39] *Idem*.
[40] *Ibidem*.

vistos como éticos para fins de pesquisa, por exemplo, podem não sê-lo quando realizados com intuitos comerciais.[41]

Por isso é que se chama especial atenção à falta de mecanismos que garantam o cumprimento dos princípios da **necessidade**, **adequação** e **finalidade** no texto do Decreto, especialmente no que diz respeito à estruturação dos níveis de compartilhamento proposta.

Não é meramente o dado em si, se é um número de CPF ou a informação de quem é o cônjuge de uma pessoa, que determinará **qual órgão da administração pública federal poderá ter acesso** sobre ele, mas **a finalidade e o contexto do tratamento**.

Uma vez realizada uma análise mais generalizante a respeito de como os níveis de compartilhamento descritos no Decreto se comportam face à LGPD, cabe proceder agora a uma exploração mais pormenorizada a respeito de cada nível, começando pelo de compartilhamento amplo.

i. Compartilhamento amplo

A categoria de **compartilhamento amplo** inclui dados que serão disponibilizados para que qualquer pessoa, seja ela servidora pública ou não, tenha acesso irrestrito. As "Regras" trazem ainda mais um elemento problemático: cairão nessa categoria todos os "dados não protegidos por norma, portanto públicos"[42].

Esses dados dispensarão autorização prévia pelo gestor de dados e seu compartilhamento será realizado pelos canais existentes para dados abertos e transparência ativa descritos (art. 11, Decreto). Para a categoria ampla, as únicas restrições apresentadas pelas "Regras" são em relação ao CPF, que deverá ser mascarado no formato ***.999.999-**.[43]

Vale dizer que não há qualquer explicação ao longo do documento sobre qual o motivo pelo qual se decidiu realizar o mascaramento do CPF dessa forma,

[41] VAYENA E, SALATHÉ M, MADOFF LC, BROWNSTEIN JS. **Ethical Challenges of Big Data in Public Health**. PLoS Comput Biol 11(2), 2015: e1003904. doi:10.1371/journal.pcbi.1003904
[42] CCGD. **Regras**, Op. Cit, p. 6.
[43] *Idem*, p. 8.

nem se esse tipo de encriptação do dado é de fato eficiente para impedir a identificação do indivíduo.

Considerando que a LGPD é justamente uma lei de **proteção** de dados, soa minimamente **contraditório** que informações como **diploma universitário**, que contém dados pessoais (nome do indivíduo, área de formação, local de graduação), seja considerado "desprotegido" e sirva de exemplo para um dado de categoria ampla, conforme pág. 15 das Regras.

O próprio CPF mascarado, que, se comprovada a efetividade desse procedimento, pode ser considerado dado pseudonimizado, é outra informação tida como de compartilhamento amplo pelas Regras e que chama muita atenção. Afinal, **dados pseudonimizados também constituem dado pessoal**, de acordo com a LGPD, considerando que continuam a ser informações relacionadas a pessoas naturais identificáveis[44].

Por isso é que **chama atenção outro dado definido pelas Regras como de compartilhamento amplo: informações sobre beneficiários de programas sociais, que podem revelar especificidades sobre a vida financeira de indivíduos.**

Dados financeiros são informações consideradas sensíveis pelo *Federal Trade Commission*[45], e tanto o são que **informações sobre cartão de crédito têm sido usadas por consultores políticos para criar perfis políticos de eleitores para melhor endereçarem campanhas de desinformação**. Vale ressaltar que informações que permitem extrair opiniões políticas de indivíduos são consideradas dados sensíveis pela LGPD.[46]

Identifica-se, pois, uma série de incongruências entre o que tem sido estipulado pelo CCGD e as regras da LGPD. Salta aos olhos a confusão entre o que são ou não dados pessoais, bem como sobre como protegê-los, especialmente

[44] Art. 13 §4° - Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
[45] Federal Trade Commission (FTC). **Protecting Consumer Privacy in an Era of Rapid Change**: Recommendations For Businesses and Policymakers. 2012, p. 59. Disponível em https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers. Acesso em 1º jul 2020.
[46] HOWARD, Philip. **Lie Machines.** Yale University Press, 1ª Ed., 2020.

pelo fato de que o Decreto e as Regras consideram que “dados públicos” devem ser disponibilizados sem qualquer discrição.

Nesse sentido é que Daniel Solove[47], já em 2001, chamava atenção para que o acesso aberto à informação fosse feito tendo em vista a revolução trazida pelo desenvolvimento das capacidades de processamento de computadores, que ampliaram exponencialmente a capacidade de coletar e processar informações.

O aumento exponencial da capacidade de processamento de dados faz com que o uso de dados pessoais, sejam eles quais forem, pode afetar a privacidade e a proteção de dados de seus titulares, o que inclui sua autonomia. Foi o que demonstrou o escândalo *Cambridge Analytica*, quando dados que não eram considerados sensíveis foram utilizados para manipular eleições.[48]

Isso mostra que dados pessoais, sensíveis ou não, devem ser protegidos conforme os parâmetros previstos na LGPD, o que determina inclusive a jurisprudência desta Suprema Corte no julgado da ADI 6387. Nesse sentido, os **requisitos especificados na categoria ampla deverão ser revistos**, de modo a garantir que um nível adequado de proteção de dados seja garantido na administração pública federal.

ii. Compartilhamento restrito

As preocupações se mantêm nas definições e exemplos de dados de compartilhamento restrito. O art. 4º, II, do Decreto 10.046/2019, estabelece que se concederá acesso desses dados “a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas”.

O documento de Regras traz mais detalhamento sobre o acesso aos dados restritos:

> *"São dados restritos aqueles que o órgão entende que podem ser acessados por todos os órgãos e entidades da*

[47] SOLOVE, Daniel J. **Privacy and Power**: Computer Databases and Metaphors for Information Privacy. Stanford Law Review, Vol. 53, 2001, pp. 1393-1462. Disponível em https://ssrn.com/abstract=248300. Acesso em 2 jul 2020.
[48] THE GUARDIAN. **What is the Cambridge Analytica scandal?** - video explainer. 19 mar 2018. https://www.theguardian.com/news/video/2018/mar/19/everything-you-need-to-know-about-the-cambridge-analytica-expose-video-explainer. Acesso em 24 abr 2020.

> *Administração Pública Federal (APF), sem a necessidade de analisar pedidos e emitir permissões para cada caso. Não emitir permissão não deve ser confundido com não ter controle sobre acessos, como a rastreabilidade destes acessos".*[49]

Tal explicação é uma contradição em si mesma. Conforme a RFC 4949 do Internet Engineering Task Force (IETF), organização internacional que cunhou o termo **controle de acesso,** este seria a "*proteção dos recursos de um sistema contra acesso não autorizado*", ou ainda, "*um processo pelo qual o uso dos recursos do sistema é regulamentado de acordo com uma política de segurança e é permitido somente por entidades (usuários, programas, processos ou outros sistemas) de acordo com a essa política*."[50]

Como demonstra o conceito da organização técnica, o controle de acesso não pode se resumir a uma mera rastreabilidade. A restrição dos dados deve estar **atrelada** a um controle de acesso, que inclui um **mecanismo de autorização** para acesso aos dados. Nada impede, contudo, que esse mecanismo seja automatizado pelo uso de hashes criptográficos que autentiquem o acesso a dados quando a necessidade foi comprovada em momento prévio (por exemplo, ao se firmar um convênio entre o órgão requerente e o responsável pela base central).

Com isso, demonstra-se que, apesar de o acesso a dados de compartilhamento restrito não mais englobar qualquer pessoa, mas todos os funcionários da administração pública federal, mais uma vez **nem o Decreto, nem os documentos do CCGD, estipulam salvaguardas suficientes a ponto de subsumir-se que os princípios da LGPD estejam sendo seguidos.**

Isso se aplica inclusive no que diz respeito à segurança dos dados pessoais, que, de acordo com o **art. 6º, VII, da LGPD**, obriga aos controladores a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de

---

[49] CCGD. **Regras**. Op. Cit., p. 9.

[50] "*Access control: 1. (I) Protection of system resources against unauthorized access. 2. (I) A process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy.*" *In* Internet Engineering Task Force (IETF). **Internet Security Glossary,** Version 2, 2007. https://tools.ietf.org/html/rfc4949. Acesso em 1º jul. 2020.

acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

Além disso, **as Regras impõem outra confusão conceitual, dessa vez com o Decreto, ao confundirem os conceitos de dados cadastrais com o de atributos biográficos** (p. 16). Isso se reflete onde chamam de cadastrais incluem nesse campo o que o Decreto chama de atributos biográficos, como nome, data de nascimento, situação civil, endereço, contatos (telefone, e-mail, etc.), filiação, nome social. Todos esses dados poderão ser acessados sem restrições dentro do poder público.

Também são exemplos de dados de compartilhamento restrito os dados sobre a situação de regularidade de pessoas físicas com a Administração Pública Federal. Isso inclui dados detalhados sobre alvarás, dívida ativa, certificados e certidões.

O fácil acesso a esses dados evidencia mais uma vulnerabilidade de segurança quanto a dados financeiros. Caso agentes maliciosos venham a acessá-los, seu uso indevido poderá repercutir no acesso a crédito de milhões de brasileiros, que terão suas informações financeiras sendo expostas no mercado clandestino de dados.

Cabe mencionar que instituições governamentais como Serpro e a base Infoseg são vítimas de grande parte dos vazamentos no setor público brasileiro,[51] informação que se soma às preocupações que advêm da ausência de salvaguardas suficientes para proteger os dados pessoais dos cidadãos previstas no Decreto.

Ademais, no caso de dados restritos, **bastará o cumprimento de um formulário descrevendo a razão do tratamento dos dados e da assinatura de um termo de sigilo e confidencialidade para que qualquer órgão da administração pública federal possa ter acesso a essas informações**.

Fora isso, não há previsão de salvaguardas para a concessão de permissão de acesso para que qualquer órgão da administração possa utilizar essas

[51] SOUZA, Renato. **Dados pessoais de brasileiros são negociados livremente na internet**. Correio Braziliense. 18 jul 2018. Disponível em https://www.correiobraziliense.com.br/app/noticia/brasil/2018/07/16/interna-brasil,695136/dados-pessoais-de-milhares-de-brasileiros-sao-negociados-na-internet.shtml

informações. Caso o gestor de dados considere que as informações fornecidas no formulário sejam consideradas insuficientes ou que os dados acessados sejam **desproporcionais à finalidade almejada**, o máximo que poderá fazer é advertir o requerente, mas nunca restringir seu acesso aos dados.[52]

Outro ponto delicado exposto nas Regras[53] é que dados considerados de compartilhamento restrito e específico só podem ser assim classificados com base em justificativa expressa. Tal obrigação poderá abrir espaço para que gestores classifiquem, por padrão, dados como de compartilhamento amplo, já que exige menos esforço. Ademais, dados de compartilhamento restrito só poderão ter seu acesso negado por determinado órgão se houver proibição expressa.

Ao assumir a lógica de que o acesso a dados é, *a priori*, livre dentro da administração pública federal, o Decreto viola o art. 7º da LGPD, que estipula que dados pessoais só podem ser tratados em situações específicas e previstas em lei.

Essas disposições do Decreto poderão representar uma abertura para possíveis violações em massa dos princípios da finalidade, necessidade e adequação e, com eles, da proteção de dados de milhões de indivíduos. Com essa massificação do acesso a dados pessoais, e que a única forma de controle prevista é a mera rastreablidade das informações, fica a dúvida: **quem exercerá o controle de se os tratamentos de dados estão de fato cumprindo os princípios da LGPD?**

Essa pergunta é deixada sem resposta pelo Decreto. Assim como a dúvida a respeito de como o titular de dados exercerá seus direitos de acesso, informação e correção. Isso será mais explorado adiante.

iii. Compartilhamento específico

A última categoria de compartilhamento do Decreto é o nível de compartilhamento específico, que promete maior nível de controle de acesso. É a única categoria que prevê ser necessária permissão do gestor de dados para

[52] CCGD. **Regras**. Op. Cit., p. 8.
[53] *Idem*.

liberação de acesso. De acordo com as Regras, "[c]ritérios para aprovar ou recusar acesso, bem como detalhes do processo, são de total responsabilidade do gestor dos dados."[54]

Nesse nível, **o documento das Regras foge completamente ao escopo do Decreto e da LGPD, por incluir dados para os quais esses instrumentos não se aplicam, conforme art. 4º, III, da LGPD: segurança pública, defesa do Estado, segurança nacional e atividades de investigação e repressão de infrações penais**.[55] Conforme descrito acima, na Seção III, o Decreto se limita a regular o que está sob o âmbito da LGPD.

Por fugirem completamente do escopo da LGPD, e pelo fato de o Decreto 10.046/2019 ser de natureza **regulamentar**, não podendo, pois, inovar sobre aspectos não regulados na lei sobre a qual se baliza, **as previsões a respeito do tratamento de dados relativos às exceções do art. 4º, III, da LGPD devem ser excluídas das previsões para tratamento sob o escopo do Decreto.** Isso inclui o impedimento de qualquer compartilhamento de dados para esses fins com base nas normas infralegais do Decreto.

[54] *Idem*, p. 12.
[55] *Idem,* p. 18.

VI. DA FALTA DE PREVISÕES PARA O EXERCÍCIO DOS DIREITOS PREVISTOS NA LGPD

Além da expressiva falta de conformidade com os princípios da LGPD, o Decreto falha ao não trazer nenhum dispositivo que permita o exercício, pelo titular de dados, dos direitos previstos na LGPD.

Primeiramente, o Decreto não prevê meios para que se **confirme a existência de tratamento de dados pessoais** de que um indivíduo é titular, conforme previsto no art. 18, I, da LGPD. O exercício do **direito de acesso aos dados** também não encontra nenhuma previsão no texto do Decreto, e tampouco é descrito qualquer mecanismo para o exercício do **direito à correção de dados incompletos, inexatos ou desatualizados** pelo titular (art. 18, III, da LGPD).

A administração pública toma decisões que afetam a vida dos brasileiros em modo que inclusive pode exacerbar ou transformar relações de poder na sociedade, e essas decisões são cada vez mais baseadas em análises de dados pessoais.[56] Por isso, é indispensável que uma regulação de dados preveja meios para que o titular saiba quais dados seus estejam sendo tratados, tenha acesso a eles e que garanta que as informações utilizadas estejam corretas.

Sem uma leitura apropriada do Decreto 10.046/2019, que seja centrada no titular de dados e nos direitos e princípios estipulados pela LGPD, seus efeitos se refletirão na **estruturação de uma máquina burocrática com mecanismos cada vez mais opacos** de acesso pelo indivíduo às informações detidas pelo Estado sobre ele, bem como quem tem acesso a elas e para quais propósitos. Ainda que o art. 7º, pár. único, especifique que gestores terão esse controle, não há previsão sobre como isso será revelado ao titular de dados.

Nesse sentido, **a leitura constitucional a ser feita sobre o Decreto deve garantir que sua interpretação supere a noção ultrapassada de que existem dados protegidos e dados desprotegidos**. Com o desenvolvimento tecnológico e o fato de que hoje permite que massas de dados sejam analisadas com grande velocidade de processamento para a criação de perfis com base em informações

[56] SOLOVE, 2001, Op. Cit., p. 1399.

as mais diversas possíveis, é necessário compreender que **o mau uso de qualquer dado pode representar uma violação à autodeterminação informativa.**

O Decreto deve ser interpretado de modo que os princípios e direitos estipulados na LGPD sejam devidamente seguidos, em atenção a seu art. 4º, §1º, que determina que o tratamento de dados pessoais, inclusive para fins não previstos na lei, deverá "**prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, **observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei**".

Vale ressaltar que o uso de dados para fins de políticas públicas pelo Estado não deve ser de forma alguma impedido ou obstaculizado a ponto de tornar impraticável a agenda de construção de medidas para o desenvolvimento do país. O que se pretende aqui é ressaltar que o tratamentos de dados para tais fins deve ser feito de forma a garantir que haja **proporcionalidade** em seu uso.

Isso inclui **impedir que qualquer tratamento de dados pessoais seja feito de forma ilimitada e sem garantir controle para o indivíduo**, levando a um cenário em que o titular perde totalmente a noção de quem tem acesso a seus dados e para qual finalidade.

Com isso, é necessário garantir que o Decreto fuja a essa visão ultrapassada de categorias estanques de compartilhamento de dados, de modo a prever que a interoperabilidade dentro da administração pública federal seja feita em concordância com os princípios da **necessidade**, **adequação** e **finalidade**. Isso garante que dados só sejam usados quando forem necessários para a finalidade buscada, e os controles de acesso, permissão, bem como a adoção de técnicas como anonimização e pseudonimização, devem atender a tais noções.

Outro princípio da LGPD que merece destaque no contexto de compartilhamento de dados é o da **transparência**, que será melhor explorado na seção seguinte.

VII. DO PRINCÍPIO DA TRANSPARÊNCIA E A LEI DE ACESSO À INFORMAÇÃO

O poder público possui a função precípua de atender à população, sendo o povo sua origem e sua finalidade. Para viabilizar o monitoramento de suas atividades e evitar o desvio de sua função, é dever do Estado guarnecer os cidadãos de informações suficientes para que estes possam exercer a função de controle popular da atividade pública.

Este dever de prestação de contas e informações aos administrados é consagrado na Constituição Federal em seu art. 5º, XIV, XXXIII, XXXIV, LXXII, bem como no art. 37, na forma do **direito fundamental à transparência**[57].

Este direito fundamental é concretizado no ordenamento jurídico infraconstitucional pelas normas integrantes do Sistema Brasileiro de Proteção e Acesso a Dados Pessoais[58], composto da Lei de Acesso à Informação (Lei 12.527/2011), do Marco Civil da Internet (Lei nº 12.965/2014) e da LGPD, todas referenciadas pelo Decreto em sua epígrafe.

A lei nº 12.527, de 2011, denominada **Lei de Acesso à Informação (LAI)**, reflete desde a data de sua entrada em vigor a concretização de uma demanda longeva por maior transparência do poder público quanto aos dados relativos à sua atuação.

A LAI prevê ao cidadão a garantia de uma gestão de dados e informações por parte do poder público de forma **transparente**. No entanto, a LAI garante que deve ser igualmente resguardada a **segurança dessa informação**, sua

[57] MEDEIROS, Simone Assis; MAGALHÃES, Roberto; PEREIRA, José Roberto. **Lei de Acesso à Informação**: em busca da transparência e do combate à corrupção. Informação & Informação, [S.l.], v. 19, n. 1, p. 55–75, dez. 2013. ISSN 1981-8920. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/view/13520/14207>. Acesso em: 01 jul. 2020.

[58] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais**: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasília : MPF, 2019. 85 p. – (Roteiro de Atuação ; v. 3)

disponibilidade, **autenticidade** e **integridade**, assim como a **proteção da informação sigilosa e da informação pessoal**[59].

Apesar de não ser o objeto principal da LAI, a proteção aos dados pessoais e à privacidade ganharam dispositivos próprios em seu corpo. Dentre estas previsões legais, a lei traz garantias de respeito à intimidade, vida privada, honra e imagem das pessoas em seu art. 31.

Uma vez que esteja em posse de dados pessoais, o poder público deve preconizar a privacidade dos titulares destes dados. **A norma prevê a limitação do acesso a informações pessoais, independente de determinações de sigilo**, assim como a **previsão da responsabilização do agente público** que dê uma finalidade indevida a essas informações.[60]

A LAI delimita uma série de deveres do agente público durante o manuseio destas informações. Dados pessoais somente podem ser compartilhados caso (i) haja consentimento expresso do titular, (ii) haja lei que autorize o compartilhamento ou (iii) esteja em alguma das exceções previstas em algum dos incisos de seu art. 31, §3º, quais leem-se:

> Art. 31. (...)
>
> § 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;

---

[59] Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

[60] 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:
I - **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
II - 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.**

> 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.

Além de estabelecer estas restrições à utilização de dados pessoais, o Decreto nº 7.724/2012, que regulamenta a LAI, define uma série de salvaguardas para garantir o uso correto dessas informações.

Em seu **art. 60**, ficam estabelecidos todos os requisitos necessários para que o agente, público ou privado, obtenha o acesso a esses dados pessoais[61]. Este mecanismo **visa garantir que o agente que pretenda obter acesso às informações pessoais possua uma finalidade legal**. Uma vez feita a requisição, esta passará por uma apreciação interna ao órgão em posse dos dados.

O art. 60 prevê que a apreciação levará em conta, inclusive, a existência de consentimento do titular de dados, que deverá ser expresso e via procuração. Também prevê a **necessidade de demonstração da necessidade do acesso à informação pessoal requerida (inciso IV), bem como comprovação de finalidade dessa requisição (inciso II),** obrigações que estão diretamente relacionadas aos já mencionados princípios da finalidade, adequação e necessidade, da LGPD.

Por fim, caso entenda ser cabível o compartilhamento desses dados pessoais, o art. 61 do Decreto regulador da LAI vincula o agente público à finalidade pretendida com esse compartilhamento. Essa disposição gera a

[61] Art. 60. O pedido de acesso a informações pessoais observará os procedimentos previstos no Capítulo IV e estará condicionado à comprovação da identidade do requerente.
Parágrafo único. O pedido de acesso a informações pessoais por terceiros deverá ainda estar acompanhado de:
I - **comprovação do consentimento expresso** de que trata o inciso II do **caput** do art. 55, por meio de procuração;
II - comprovação das hipóteses previstas no art. 58;
III - demonstração do interesse pela recuperação de fatos históricos de maior relevância, observados os procedimentos previstos no art. 59; ou
IV - **demonstração da necessidade do acesso à informação** requerida para a defesa dos direitos humanos ou para a proteção do interesse público e geral preponderante.

possibilidade de responsabilização do agente caso destine a informação a uma finalidade indevida, que vá além da que fora pretendida no momento do fornecimento das informações.[62]

A partir da leitura do Decreto 10.046/19, em conjunto com o Decreto 7.724/2012 e as leis em que se baseia, identifica-se evidente afronta à LAI. Apesar das "Regras"[63] destacarem como um benefício aos administrados uma maior transparência quanto ao manuseio de dados pessoais, isto não se reflete na prática.

Não há previsão de canais de acesso ao cidadão para o acompanhamento de quais dados estão em posse do poder público, assim como é lacunoso quanto a obrigações do agente público em prestar contas à população, não imputando-o deveres nos ditames da LGPD, como a delimitação da finalidade da coleta ou previsão legal do tratamento.

Quanto mais, no que tange ao **princípio da transparência**, quando aplicado ao titular de dados, este possui desdobramento na LGPD, mais especificamente em seu artigo 6º, VI, da LGPD. Esse dispositivo prevê que seja dada "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

Apesar da vocalização da LGPD a esse respeito, o Decreto parece ignorar a existência do titular de dados, tomando as informações pessoais de cidadãos que estão sob seu poder como se fossem suas. Isso se reflete no eloquente silêncio do Decreto em relação a qualquer obrigação de informação ao titular a respeito de como seus dados estão sendo utilizados.

---

[62] Art. 61. O acesso à informação pessoal por terceiros será condicionado à assinatura de um termo de responsabilidade, que disporá sobre a finalidade e a destinação que fundamentaram sua autorização, sobre as obrigações a que se submeterá o requerente.
§ 1º **A utilização de informação pessoal por terceiros vincula-se à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa.**
§ 2º Aquele que obtiver acesso às informações pessoais de terceiros será responsabilizado por seu uso indevido, na forma da lei.

[63] CCGD. **Regras**. Op. Cit., p. 3.

Afinal, **o Decreto não descreve meios pelos quais o indivíduo pode saber quais dados estão sendo compartilhados, de que forma, quem é o gestor de dados responsável por eles e como exercer direitos como acesso e correção**.

Ademais, a falta desse tipo de garantia é uma afronta à ideia de que a proteção de dados se reflete justamente na ideia de controle do titular sobre suas informações e de determinar como sua esfera privada deve ser construída,[64] expressa, na LGPD, nos art. 51 e 55-J, VII.

Além dos riscos associados à utilização das categorias previstas no decreto apresentados anteriormente[65], o enquadramento de dados pessoais como dados que podem ser livremente compartilhados na administração pública, sem a necessidade de análise de pedidos e emissão de permissões para cada caso[66], configura uma afronta diametral à Lei de Acesso à Informação.

Permitir a livre circulação desses dados com base em uma categorização *a priori,* que não leve em conta a hipótese legal que autorize seu compartilhamento e sem consentimento do titular, além de não levar em consideração o contexto que estes dados foram coletados, contraria o dispositivo legal contido na LAI.

Restando evidenciadas as afrontas e riscos ao princípio da transparência gerados pelo Decreto dada a sua desconformidade frente à Constituição Federal e às normas integrantes do Sistema Brasileiro de Proteção e Acesso a Dados Pessoais, cabe a esta E. Corte se posicionar para resguardar a defesa dos direitos dos administrados frente ingerências ilegais do Estado, devendo assim julgar provida a presente ação para interpretar o r. Decreto conforme a CRFB.

[64] RODOTÀ, S. Data Protection as a Fundamental Right. In: GUTWIRTH, S. et al. Reinventing Data Protection? 1 ed. Springer, EUA, p. 78.
[65] Vide seção “DOS PRINCÍPIOS DE PROTEÇÃO DE DADOS”.
[66] CCGD. **Regras**. Op. Cit., p. 9.

VIII. DA OMISSÃO DO EXECUTIVO QUANTO À IMPLEMENTAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Postos os paradigmas legais introduzidos pela LGPD e pela LAI para a execução de políticas públicas, ponto que deve igualmente ser considerado para a real concretização do direito à proteção de dados pessoais é a implementação da Autoridade Nacional de Proteção de Dados (ANPD), prevista no art. 55-A da LGPD[67].

Tendo origem na Convenção 108 da Comissão Europeia, de 1981, que, no seu artigo 13, previa a necessidade de indicação de uma autoridade independente para o auxílio durante a cooperação internacional para a apuração da correta aplicação dos dispositivos sobre proteção de dados presentes na Convenção[68], a figura da autoridade de proteção de dados adquiriu diversas atribuições ao longo do tempo.

O Regulamento Geral de Proteção de Dados (do inglês, GDPR) da União Europeia, por exemplo, define que as autoridades de proteção de dados do bloco devem ter as atribuições principalmente de ombudsman, de auditoria, consultiva, educadora, conselheira política, negociadora e executora[69]. A ANPD segue atribuições semelhantes, listadas no art. 55-J da LGPD.

---

[67] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

[68] Art. 13º - Cooperação entre as Partes
1- As Partes comprometem-se a prestar assistência mútua com vista à aplicação da presente Convenção.
2- Para esse efeito:
a) Cada Parte designará uma ou mais autoridades cujo nome e endereço serão comunicados ao Secretário-Geral do Conselho da Europa;
b) As Partes que tenham designado várias autoridades indicarão, na comunicação referida na alínea anterior, a competência de cada uma delas.
3- A autoridade designada por uma Parte deverá, a pedido da autoridade designada por outra Parte:
a) **Fornecer informações sobre o seu direito e a sua prática administrativa em matéria de protecção de dados**;
b) **Adoptar**, em conformidade com o seu direito interno e apenas para efeitos de protecção da vida privada, as medidas adequadas à prestação de informações factuais relativas a um determinado tratamento automatizado efectuado no seu território, à excepção, contudo, dos dados de carácter pessoal que sejam objecto desse tratamento.

[69] BENNETT, Colin J.; RAAB, Charles D. **The Governance of Privacy**: Policy Instruments in Global Perspective. [*S. l.*]: Routledge, 2017. 272 p.

O universo que envolve o tratamento de dados pessoais é complexo, sendo um constante estado de aprendizado e melhoria de todos os agentes envolvidos com este processo, essencial para que o regramento de proteção de dados esteja em conformidade com o desenvolvimento de novas tecnologias. Por isso, a existência de uma instituição especializada neste ramo é crucial para manter atualizado o racional de proteção de dados em determinado país ou região[70].

No caso brasileiro, a obrigação para instituir a ANPD é da Presidência da República e existe desde a aprovação da LGPD em 2018. Ao se manter inerte por dois anos e postergar indeterminadamente a instauração de uma autoridade brasileira de proteção de dados, **a Presidência está manifestamente obstando a fruição dos cidadãos dos direitos previstos na Constituição e na LGPD**.

Na ausência de uma autoridade especializada, resta ao Judiciário a tarefa de adequar atividades públicas e privadas às balizas legais da proteção de dados. Esse quadro sobrecarrega este poder com demandas, tanto dos titulares frente controladores que porventura atentem contra seus direitos quanto pelo próprio poder público contra atos da administração pública quando esta age em desconformidade com a lei.

Esse fenômeno se evidenciou perante esta Suprema Corte em especial durante a ADI 6.387, onde o poder público agiu contrariamente à lei, tendo que o poder judiciário intervir na situação antes que houvessem danos aos direitos dos titulares de dados. A figura se repete na presente demanda: sem uma autoridade para reger as relações de compartilhamento de dados entre órgãos públicos, excessos devem ser levados ao Judiciário, inflando este poder.

Para que haja uma alteração neste quadro de incerteza e excessos de demandas ao poder judiciário, resta imanente à presente causa a necessidade desta Corte se manifestar quanto à omissão do Poder Executivo em instaurar a ANPD.

Dado que a falta da ANPD afeta o exercício dos direitos fundamentais à privacidade e à autodeterminação informativa, faz-se necessária a **pronta intimação da União** para que se manifeste sobre as razões para essa omissão,

[70] INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, 28., 2006, Londres, Reino Unido. **Communicating Data Protection and Making It More Effective** [...]. [*S. l.*: *s. n.*], 2006.

dada a inércia em seu dever constitucional de adstrição à lei e consequente afronta expressa à LGPD e à Constituição. Em última instância, será inevitável declarar como omissa a União em cumprir seu dever constitucional.

Caso contrário, esse cenário de ilegalidade e inconstitucionalidade do Executivo Federal perdurará indefinidamente, abrindo espaço para outros abusos à proteção de dados pessoais pelo poder público, bem como o aumento das demandas judiciais sobre o tema, inflando ainda mais o Poder Judiciário.

IX. PEDIDOS

Face ao exposto, o Laboratório de Políticas Públicas e Internet - LAPIN:

1. Requer seja autorizada sua **sustentação oral** durante julgamento da matéria, diante do deferimento de sua participação como *amicus curiae* no presente feito, nos termos do artigo 138 do Código de Processo Civil e do artigo 131, §3º, do RISTF.
2. Recomenda que seja, no mérito, **julgada procedente a presente demanda**, no sentido de:
    - **a.** reconhecer a taxatividade do rol do art. 1º do Decreto 10.046/2019, de modo que o tratamento de dados pessoais que se der sob seu escopo seja feito apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, à luz do princípio da finalidade que norteia o direito à proteção de dados pessoais constitucionalmente reconhecida por esta Suprema Corte durante o julgamento da ADI 6387;
    - **b.** afastar da abrangência do referido Decreto a finalidade de atividade de inteligência, visto que não prevista em seu bojo nem na lei que rege o tratamento de dados pessoais no país, a Lei Geral de Proteção de Dados;
    - **c.** reconhecer expressamente, à luz do previsto nos incisos I, V e VI do art. 3 do referido Decreto, que qualquer tratamento de dados pessoais realizado por órgãos e entidades do setor público está expressamente sujeito e vinculado aos princípios que balizam a proteção de dados pessoais no Brasil, expressos no art. 6º da Lei nº 13.709, de 2018, especialmente quanto à **finalidade, adequação, necessidade e transparência**;
    - **d.** declarar expressamente, conforme determina o art. 4º, §1º, da LGPD, que qualquer tratamento de dados pessoais, inclusive quando realizado para fins de segurança nacional e para as outras exceções previstas no art. 4º, III, da LGPD, deve ser feito à luz dos princípios previstos em seu art. 6º;

e. intimar a União a se manifestar a respeito de sua omissão constitucional em instituir a Autoridade Nacional de Proteção de Dados (ANPD), com fulcro no art. 55-A, da LGPD; e

f. declarar a omissão constitucional e o descumprimento de preceito fundamental pela União ao não instituir a ANPD.

3. Seja a postulante intimada, por meio de seus procuradores, de todos os atos do processo.

Termos em que,

Pede deferimento.

Brasília, 30 de julho de 2020.

Henrique Bawden Silverio de Castro
OAB/DF n. 58.680

José Renato Laranjeira de Pereira
OAB/DF n. 59.985

Isabela Maria Rosal Santos
OAB/DF 63.395

Paulo Henrique Atta Sarmento
OAB/DF n. 63.259

Thiago Guimarães Moraes
CPF n. 014.667.361-19