2020 | MAIO

ANÁLISE
GUIA DE BOAS PRÁTICAS LGPD

COMENTÁRIOS AO GUIA DE BOAS PRÁTICAS PARA IMPLEMENTAÇÃO DA LGPD NA ADMINISTRAÇÃO PÚBLICA FEDERAL

LAPIN

Sobre esta contribuição

Com vistas a adequar a governança de dados no âmbito da Administração Pública Federal (APF) às disposições previstas na Lei nº 13.709/2018, foi editado, em abril de 2020, o "Guia de Boas Práticas para Implementação na Administração Pública Federal - Lei Geral de Proteção de Dados (LGPD)" (doravante denominado "Guia").

O documento tem como finalidade "**fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD**."

De modo a colaborar com seu aprimoramento, o Laboratório de Políticas Públicas e Internet (LAPIN) vem apresentar suas contribuições[1] ao Guia, com ênfase nos **capítulos 1 e 2** pela necessidade de urgência da análise. As observações trazidas serão apresentadas de acordo com a ordem estabelecida em seu texto.

Os trechos objeto das mudanças estão distribuídos em caixas azuis com o título "**Texto Guia**", seguidos da apresentação das contribuições ("**Contribuições LAPIN**") e de caixas verdes com sugestões de redação com o título "**Texto Sugerido**".

Quem somos nós

O **Laboratório de Políticas Públicas e Internet (LAPIN)** é um *think tank* com sede na capital federal brasileira, de composição multidisciplinar e cujo objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

[1] Participaram dessa contribuição: Henrique Bawden, José Renato Laranjeira de Pereira, Paulo Henrique Atta Sarmento e Thiago Guimarães Moraes.

Sumário

1. Direitos Fundamentais do Titular dos Dados

1.1 - Base Legal para Tratamento dos Dados Pessoais

Texto Guia (p. 8):

> *Cumpre destacar que o princípio da finalidade do tratamento de dados estabelecido na LGPD exige que os propósitos do tratamento sejam legítimos, específicos, explícitos e informados ao titular. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades (art. 6º, I). No caso do setor público, a finalidade relaciona-se com a execução de políticas públicas,devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador. O consentimento, quando exigido pelos órgãos públicos, será medida excepcional e deverá se referir a finalidades determinadas e comunicadas claramente ao titular do dado.*

Contribuições LAPIN

Como bem mencionado pelo próprio texto, a finalidade do tratamento de dados no caso do setor público se relaciona com o propósito de viabilizar o funcionamento de políticas públicas realizadas pelo Estado. Contudo, acerca do consentimento, é necessário que haja uma interpretação mais restritiva, levando em conta o modo como a proteção de dados pessoais é estruturada.

O consentimento possui um papel especial na sistemática prevista pela lei: é ele que possibilita que o tratamento garanta ao titular maior controle e autonomia sobre seus dados. A preocupação com o consentimento é algo central, vide as publicações recorrentes da União Europeia visando esclarecer como se deve interpretar este conceito[2].

Toda a lógica por trás do consentimento aponta para a necessidade de garantir a sua existência sempre que possível, levando em conta desequilíbrios de poder entre as partes, a finalidade, a possibilidade de retirada do consentimento, entre outros pontos.

Logo, a interpretação que deve ser feita não é de que o consentimento é uma medida excepcional, mas sim de que apenas quando não for possível obtê-lo é que se deve dispensá-lo e consequentemente basear-se em uma das

[2] Vide o "Guidelines on consent under Regulation 2016/679" e o recente "Guidelines 05/2020 on consent under Regulation 2016/679" acerca do consentimento na GDPR pela European Data Protection Board.

outras hipóteses legais. Nesse caso, uma boa prática a ser adotada é que o uso das bases legais de execução de políticas públicas e de obrigação legal ou regulatória pelo controlador sejam residuais, optando-se pelo consentimento sempre que possível, preferencialmente de modo para evitar a inexecução de políticas públicas, em respeito ao princípio da continuidade dos serviços públicos.

Texto Guia (p. 10):

> *Nesses casos, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados. É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência.*

Para esse trecho, sugere-se a seguinte redação:

Texto Sugerido:

> Nos casos de tratamento de dados em que a base legal não é o consentimento, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, **garantindo-lhes o exercício aos direitos previstos no art. 18 da LGPD, com destaque aos direitos de acesso, retificação, oposição, eliminação e informação das entidades públicas e privadas com as quais o controlador irá realizar o uso compartilhado de dados**. É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência. Além disso, é necessário que a cada tratamento de dados seja feita uma análise de se os princípios da necessidade e adequação também estão sendo cumpridos pelo controlador.
>
> Já nos casos de tratamento de dados feitos com base no consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, de dentro ou fora da administração pública federal.

Contribuições LAPIN

A nova redação é condizente com a ideia de que o uso de bases legais que não o consentimento deve ser residual. Ela ainda deixará claro, para o caso de tratamentos feitos sob outras hipóteses legais, o fato de que a mera notificação do usuário não é suficiente para cumprir a LGPD, mas que deve-se também garantir que outros direitos possam ser exercidos.

Além disso, o texto antigo impossibilitava que o titular dos dados exercesse tanto seu direito de revogação de consentimento, no caso de tratamentos de dados feitos com base nessa hipótese legal, bem como seu direito de oposição ao tratamento, quando houvesse violação à LGPD. Afinal, a comunicação ao titular, apesar de permitir-lhe maiores informações sobre o tratamento de seus dados, não garante o exercício de todos os direitos garantidos pela lei.

Texto Guia (p. 11):

> *O consentimento também pode ser tácito quando o titular do dado o torna manifestamente público previamente. Tal situação está prevista no §4° do Art. 7°: "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.*

Contribuições LAPIN

Outro ponto também relacionado ao consentimento é de que na **página 11,** ao tratar do consentimento manifestado pelo titular, o Guia dita que o art. 7°, §4° traria uma hipótese de consentimento tácito. No entanto, qualquer espécie de consentimento tácito, ou seja, que não seja obtido por meio de *manifestação inequívoca,* pela qual se identifica que o titular de dados expressou seu desejo de consentir através de clara ação afirmativa, será considerado **ilegítimo**.

Assim sendo, o silêncio e a inatividade, como por exemplo caixas de seleção automaticamente preenchidas no meio online, não devem ser considerados formas de consentimento, pois não deixam claro que o sujeito de dados concordou que seus dados fossem tratados para um devido fim. Nesse sentido é que, no contexto europeu, a Comissão Europeia de Proteção de Dados (EDPB) manifestou que o consentimento deve ser provido por meio de uma manifestação deliberada em consentir do titular de dados.[3]

Ademais, uma leitura correta do art. 7°, §4° mostra que, na verdade, dados tornados manifestamente públicos pelo titular se tratam de uma hipótese de dispensa de consentimento, não de expressão tácita. Isso implica que, conforme será demonstrado nos parágrafos seguintes, o consentimento poderá ainda ser pedido em alguns casos, como no inciso III do art. 7°.

Caso ainda mais restritivo é a hipótese do art. 11, I, que exige que o consentimento obtido para o tratamento de dados sensíveis seja **destacado**. Na

[3] European Data Protection Board (EDPB). **Guidelines 05/2020 on consent under Regulation 2016/679**. 4 mai 2020. Disponível em https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt. Acesso em 18 mai 2020, Paras 77 a 79.

versão europeia, a expressão equivalente é o "*explicit*" (explícito).[4] Mais uma vez, o Comitê Europeu de Proteção de Dados apresenta orientações de como distinguir esse termo da manifestação inequívoca "regular".[5] Aqui, o controle é ainda mais rígido, e o consentimento deve ser expresso pelo titular de dados mediante uma declaração. Exemplos trazidos são o uso de assinatura (física ou digital), responder um email declarando o consentimento do tratamento para um determinado fim, ou a gravação de uma conversa em que o titular de dados expressa que concorda com o tratamento.[6]

Na **página 12**, ao elencar os incisos do art. 7º, o Guia faz uma relação de cada inciso com a necessidade ou não de consentimento. Aqui, cabe realizar uma interpretação restrita do referido artigo, em especial dos incisos II e III.

Em uma primeira leitura do texto do Guia, parece que há uma sobreposição entre os casos previstos pelos dois dispositivos, considerando que ambos acabam por se referir a obrigações legais. No entanto, uma análise mais atenta demonstra que o inciso II se refere aos casos em que existe uma obrigação legal imposta ao controlador mas que acaba por afetar o titular de dados, determinando que ele realize o compartilhamento de suas informações.

Exemplo disto é o caso dos dados relativos ao patrimônio que são compartilhados com a Receita Federal para fins de lançamento tributário. Nessa situação, há uma obrigação do Estado de realizar a coleta dos tributos, que, para ser cumprida, exige do indivíduo informações específicas, conforme o tipo de declaração exigido pelo tributo.

Já quanto ao inciso III, que versa sobre o tratamento de dados pessoais no contexto de execução de políticas públicas, sua leitura deve ser feita com **especial atenção ao termo "necessário"** existente no texto legal. Deve-se interpretar esse termo de modo que apenas nos casos em que conseguir o consentimento do titular dos dados torne impraticável a execução da política pública ocorra a dispensa do consentimento do titular. Caso contrário, há uma abertura demasiadamente grande para o poder público pedir dados com base em documentos infralegais.

[4] GDPR, art. 9 (2) (a).
[5] European Data Protection Board (EDPB). Op cit 3, para 93.
[6] Ibid, para 94.

1.2 - Direitos do Titular

Contribuições LAPIN

Objetivando uma maior clareza e capacidade informativa do Guia, consideramos que **as tabelas da seção 1.2, "Direitos do Titular", deveriam ser substituídas por uma seção que explique cada um dos princípios** previstos no art. 6º da LGPD.

Tal explicação funcionaria como um guia para o administrador público, para que ele entendesse qual é a lógica que permeia todo o sistema de proteção de dados.

Da forma como a tabela está no guia, ela acaba por induzir o administrador público ao entendimento de que há um rol taxativo de direitos da LGPD que seriam diretamente deduzíveis de cada princípio. Não consideramos esse um caminho adequado. **Os princípios regem uma série de relações e obrigações** necessárias ao funcionamento adequado da proteção de dados do país, **e não é possível extrair automaticamente um direito de cada um deles.**

Também é necessário mencionar o fato de que há uma omissão do guia no que tange a certos princípios, como o da segurança (art. 6º, inciso VI) ou da prevenção (art. 6º, inciso VIII). Eles são centrais nos processos de tratamento de dados pessoais, ditando como se deve dar a atuação do controlador. Uma explicação do seu significado terá maior utilidade no caso concreto que a mera relação de um direito com um princípio, tal como consta na tabela da seção 1.2.

A fim de evitar tal situação, recomendamos que se faça uma exposição explicativa de cada princípio e de cada direito, para que o leitor tenha uma visão sistêmica da Lei Geral de Proteção de Dados e consiga realizar suas operações com maior independência e confiabilidade.

1.3 - Exercício dos Direitos dos Titulares perante a Administração

Texto Guia, p. 18:

> *O titular do dado tem o direito, mediante requerimento expresso seu ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:*
>
> *a. correção de dados incompletos, inexatos ou desatualizados (art. 18, III);*

b. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);

c. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e

d. revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

Contribuições LAPIN

Falta ao trecho trazer o direito de acesso do usuário aos dados de que é titular e que são objeto de tratamento, previsto no art. 18, II, da LGPD. Esse dispositivo é essencial para que o titular tenha noção de quais dados seus são tratados pelo poder público, de modo a possuir maior controle sobre o uso de suas informações.

Por isso, sugerimos a inclusão de tópico referente a esse direito, possivelmente com a seguinte redação:

Texto Sugerido:

a. acesso aos dados pessoais de que é titular e que são objeto de tratamento pela Administração Pública Federal (art. 18, II);

1.4 - Tipologia de Dados Pessoais

Contribuições LAPIN

Na seção 1.4, "Tipologia de Dados Pessoais", ao passo que o Guia está correto em dizer que não há uma correlação direta entre dados pessoais e os conceitos do Decreto nº 10.046/2019, consideramos **necessária a apresentação de uma definição de o que seriam dados cadastrais e como eles se relacionam com o conceito de dados pessoais**.

É possível perceber a existência de certa confusão 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".

Em carta aberta, ex-presidentes do IBGE se manifestaram a respeito dos protestos feitos por especialistas de que a MP não estaria protegendo os dados de brasileiros. De acordo com os redatores da carta, a "preocupação não se justifica, porque os dados não incluem informações pessoais"[7]. A MP foi posteriormente suspensa pelo Plenário do STF, por não garantir o direito à proteção de dados da população brasileira.

No entanto, foi possível perceber que o conceito de dados pessoais não foi bem compreendido pelos citados ex-presidentes, e é possível que a mesma dúvida ronde outras áreas da administração pública.

Por isso, achamos **necessário que o Guia especifique melhor de que forma o conceito de dados cadastrais se relaciona com o de dados pessoais.** Dados que usualmente são chamados de cadastrais, como nome, CPF, NIS, título eleitoral, data de nascimento, situação civil, endereço, contatos (telefone, e-mail, etc.), filiação, nome social **são dados pessoais**.

É importante afirmar que tais dados são dados pessoais, e que recaem sobre eles as regras e princípios expressos na LGPD. Isso porque, conforme o art. 5º, I, da LGPD, dado pessoal é qualquer "informação relacionada a pessoa natural identificada ou identificável". O ideal é que este conceito seja descrito com detalhe no Manual de modo a evitar dúvidas, e trazemos a seguinte tabela como sugestão:

Por que informações como CPF e endereço são dados pessoais?
Conforme a LGPD, art. 5º, I, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Este conceito é composto por quatro elementos:[8]

[7] 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.

[8] Esses elementos são apresentados a partir do conceito legal da LGPD e as referências do Grupo de Trabalho do Artigo 29, Comitê Europeu que regulou matérias de proteção de dados. Para mais informações, checar: Article 29 Working Party, Opinion 4/2007 on the concept of personal data Brussels, 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acesso em: 23 abr. 2020.

Elementos do dado pessoal	**Informação**	Pode ter natureza objetiva (ex. idade) ou subjetiva (ex. o devedor X é confiável).
	Relacionada a	Um dado pode ser considerado relacionado a um indivíduo se ele diz respeito a um dos seguintes critérios: (i) se relaciona a um **conteúdo** sobre o indivíduo; (ii) tem a **finalidade** de avaliar um indivíduo ou seu comportamento; ou (iii) tem um **impacto** sobre interesses ou direitos do indivíduo.
	Pessoa Natural	Para ser pessoal, a informação deve estar relacionada a um indivíduo humano.
	Identificada ou identificável	"Identificada" significa que a ligação ao indivíduo é feita de forma direta, como pelo tratamento de seu nome completo ou sua foto. Como "identificável", a ligação é indireta, e um processo de cruzamento de dados pode ser necessário para a identificação. Isto contudo não elimina a caracterização do dado como dado pessoal. É o caso de identificadores como o RG, CPF, o endereço e o telefone de uma pessoa natural.

Texto Guia, p. 19:

Primeiramente, cabe destacar que todos os tipos de atributos constituem informações pessoais, pois são relativos a titular pessoa física identificado ou identificável.

Atributos genéticos e biométricos, por definição legal, constituem dados pessoais sensíveis. Atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor são o que se denomina de dados cadastrais.

Por sua vez, a depender do seu conteúdo, atributos biográficos poderão ou não ser considerados sensíveis. Nos termos da Lei, serão considerados sensíveis aqueles atributos biográficos que digam respeito à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

Assim, via de regra, o tratamento de atributos biométricos e genéticos se dará com base no regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos será feito de acordo com o seu conteúdo, o qual definirá a tipologia do dado à luz da LGPD.

No que tange aos **dados cadastrais** citados na página 19, vale ressaltar que, **dependendo do contexto**, **podem ser considerados dados sensíveis**.

Para ilustrar a importância de analisar a natureza de um dado conforme seu contexto, trazemos uma situação em que o CPF seria considerado um dado pessoal sensível. Imagine o caso de uma base de dados estatal em que fossem relacionados portadores de HIV que recebessem assistência estatal para comprar medicamentos. Nessa tabela, as pessoas não são identificadas por seu nome, mas por seu CPF, um dado altamente capaz de identificação por existir sempre somente um para cada cidadão brasileiro.

Nesse caso, o conhecimento do CPF já possibilitaria saber qual o estado de saúde do cidadão, permitindo sua individualização de modo praticamente automático. Com isso, pelo contexto em que está inserido, o CPF se tornaria por si só um dado sensível, pelo fato de ele permitir relacionar o indivíduo ao dado de saúde.

Texto Sugerido:

Primeiramente, cabe destacar que todos os tipos de atributos constituem informações pessoais, pois são relativos a titular pessoa física identificado ou identificável.

Atributos genéticos e biométricos, por definição legal, constituem dados pessoais sensíveis. Atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor são o que se denomina de dados cadastrais, que são, à luz da LGPD, dados pessoais.

Isso porque, se qualquer dado, inclusive o cadastral, trouxer informação relacionada a pessoa natural identificada ou identificável, será considerado um dado pessoal. Para maiores detalhes, favor checar o quadro **“Por que informações como CPF e endereço são dados pessoais?”**.[9]

[9] Aqui sugerimos referência ao quadro "Por que informações como CPF e endereço são dados pessoais?"

Por sua vez, a depender do seu conteúdo, atributos biográficos poderão ou não ser considerados sensíveis. Nos termos da Lei, serão considerados sensíveis aqueles atributos biográficos que digam respeito à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político. **Os números de cadastro em si também podem ser considerados sensíveis quando estiverem relacionados a dados pessoais sensíveis.**

Assim, via de regra, o tratamento de atributos biométricos e genéticos se dará com base no regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos será feito de acordo com o seu conteúdo, o qual definirá a tipologia do dado à luz da LGPD.

2. Como Realizar o Tratamento dos Dados Pessoais

2.1. Hipóteses de Tratamento

Texto Guia (p. 20-21)

A tabela a seguir elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD.

Contribuições LAPIN

A definição das bases legais que serão adotadas pela autoridade pública para o tratamento de dados é essencial para que seja atendido o princípio da transparência, contido no art. 6º, VI, da LGPD. O cidadão que tiver seus dados utilizados pela Administração tem o direito de possuir informações claras, precisas e facilmente acessíveis sobre a realização do tratamento.

A partir da leitura da tabela 3, denominada "Hipóteses de Tratamento de Dados Pessoais", identifica-se uma utilização errônea das bases legais previstas na LGPD, condição que pode ser facilmente sanada.

Primeiramente, a coluna com o título "Requer Consentimento do Titular?" traz a impressão que o consentimento seria meramente um acessório das demais bases legais previstas na Lei. Contudo, o consentimento, base prevista no art. 7º, I, quando utilizado para o tratamento de dados pessoais, e art. 11, I, quando para o tratamento de dados pessoais sensíveis, é autônomo, não devendo ser confundido com as demais bases.

Utilizar o consentimento como base "suplementar" fere a importância desta base legal. Esta previsão legal reflete a conquista do titular dos dados do protagonismo sobre a determinação de sua informações[10]. Tanto é que, quando utilizada, esta base pode ser retirada a qualquer momento pelo titular.

Quanto mais, a tabela ora analisada somente elabora as bases legais cabíveis para o tratamento de dados pessoais, não enumerando as bases legais disponíveis para o tratamento de dados pessoais sensíveis, contidas no art. 11 da LGPD..

[10] BIONI, Bruno. **Proteção de Dados Pessoais:** A Função e os Limites do Consentimento. Rio de Janeiro: Forense. 2019. p. 188.

Cremos que, para melhor compreensão do tema, poderiam as bases legais, tanto utilizáveis para dados pessoais quanto para dados pessoais sensíveis, serem dispostas em tabelas distintas. Afinal, mesmo que aparentemente estas categorias de dados possuam bases legais em comum, a aplicação prática desses institutos são distintas, devendo estas bases serem tratadas de maneira igualmente distinta.

<u>Texto Sugerido</u> - Tabela "Hipóteses de Tratamento de dados pessoais"

Hipótese de Tratamento	Dispositivo legal para o tratamento de dados pessoais	Dispositivo legal para o tratamento de dados pessoais sensíveis
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I - "mediante o fornecimento de consentimento pelo titular".	LGPD, art. 11, I - "quando o titular ou seu responsável legal consentir, **de forma específica e destacada, para finalidades específicas."**
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II - "para o cumprimento de obrigação legal ou regulatória pelo controlador."	LGPD, art. 11, II, "a" - "cumprimento de obrigação legal ou regulatória pelo controlador."
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, 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**"	LGPD, art. 11, II, "b". "tratamento compartilhado de dados necessários à execução, pela administração. pública, de políticas públicas previstas em leis ou regulamentos"
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, IV - "para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais"	LGPD, art. 11, II, "c" - "realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais **sensíveis.**
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, V - "quando necessário para a execução de contrato ou de procedimentos	Não há

	preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados".	
Hipótese 6: Para o exercício de direitos em processo judicial administrativo arbitral	LGPD, art. 7º, VI - "para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996"	LGPD, art. 11, II, "d" - "exercício regular de direitos, **inclusive em contrato** e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro:	LGPD, art. 7º, VII - "para a proteção da vida ou da incolumidade física do titular ou de terceiro"	LGPD, art. 11, II, "e" - "proteção da vida ou da incolumidade física do titular ou de terceiro"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, VIII - "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária"	LGPD, art. 11, II, "f" - "tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, IX - "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"	Não há
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, X - "para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente"	Não há
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não há	LGPD, art. 11, II, "g" - "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º

		desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

Contribuições LAPIN

Posteriormente, o guia enumera as bases legais previstas na LGPD, trazendo maior profundidade aos institutos, nas **páginas 22 a 25**.

Contudo, uma das bases legais cabíveis para o tratamento de dados pessoais sensíveis não foi detalhada nos mesmos moldes das demais bases legais, que é a de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistema eletrônico, contido no art. 11°, II, "g", da LGPD.

Texto sugerido:

HIPÓTESE 11: Tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

Essa hipótese é aplicável para o tratamento de dados para assegurar a identificação e autenticação do titular dos dados, visando à prevenção de fraudes e garantir a segurança do titular.

Para enquadramento nessa hipótese, deve-se garantir:

1. Que não haja outro meio para a identificação do titular sem a necessidade do tratamento de dados sensíveis.

2. Que o titular do dado seja comunicado sobre o tratamento de dados e da forma como será realizado.

3. Que sejam adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador.

4. Que medidas de segurança adequadas sejam aplicadas para proteção dos dados.

5. A elaboração de Relatório de Impacto de Proteção de Dados.

2.3. Anonimização e Pseudonimização

Texto Guia (p. 29):

> *Segundo a LGPD,* ***dado anonimizado é o dado relativo a titular que não possa ser identificado****. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta.*

Contribuições LAPIN:

A conceituação de dados anonimizados deve ser muito bem definida, em especial em conteúdos voltados à administração pública, uma vez que serviços prestados tradicionalmente pelo Estado, como realização de pesquisas populacionais ou de saúde, deverão, sempre que possível, realizar um processo de anonimização dos dados.

O enfoque da definição de dados anonimizados deve ser não nos dados propriamente ditos, mas sim no processo realizado para a impossibilitar a identificação de seu titulares. Desde que o processo tenha sido feito empregando meios técnicos razoáveis e disponíveis no momento do tratamento para impedir essa re-identificação, estes dados serão considerados anônimos.

Afinal, como definem Finck e Palas, a anonimização de dados nunca é perfeita, e sempre é possível a re-identificação de seu titular. Seu objetivo é, na realidade, fazer com que essa re-identificação seja o mais onerosa e trabalhosa possível.[11]

Sobre o tema, vale trazer a definição apresentada por Bruno Bioni sobre dado anonimizado:

> Ao invés de considerar anonimização como algo cujo resultado (output) é infalível, foca-se em uma abordagem que considera a aplicação sistemática de técnicas de anonimização com o objetivo de agregar consistência ao processo como um todo. Por essa razão, a análise acerca de se um dado deve ser, de fato, considerado como anonimizado é eminentemente circunstancial.[12]

[11] Sobre esse tema, vale a leitura de: FINCK, Michèle; PALLAS, Frank. **They who must not be identified—distinguishing personal from non-personal data under the GDPR**. International Data Privacy Law, Oxford, pp. 1-26, 10 mar. 2020. Disponível em: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. Acesso em: 9 abr. 2020.

[12] BIONI, Bruno. **Compreendendo o conceito de anonimização e dado anonimizado.** Cadernos Jurídicos da Escola Paulista da Magistratura, São Paulo, SP, ano 21, n. 53, p. 191-201, 2020.

Desta forma, cremos que seja mais adequado definir o dado anonimizado quanto a seu processo, considerando que a definição quanto a seu conteúdo é passível de interpretações dúbias.

Texto Sugerido:

Segundo a LGPD, **dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo**. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta.

Texto Guia, p. 29:

É importante ressaltar que, ainda que o dado esteja anonimizado, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, este processo deixa de ser assim considerado e passa a ser considerado **pseudonimização**. Esses processos, de acordo com a legislação em vigor, devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis na ocasião do tratamento dos dados.

Aqui existe uma clara confusão envolvendo os conceitos de anonimização e pseudonimização. Como ressaltado acima, anonimização é o processo pelo qual um dado perde a possibilidade de associação, direta ou indireta, a seu titular, levando em conta os meios técnicos razoáveis no momento de tal tratamento e considerando o estágio de desenvolvimento tecnológico corrente.

Pseudonimização, por sua vez, de acordo com o art. 13, §4º, 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.

Essa característica específica da informação adicional é chave para o conceito de pseudonimização. Como o próprio nome já diz, esse processo se refere à criação de um pseudônimo para substituir a referência ao dado em si.

Esse pseudônimo pode ser criado por meio de técnicas como *hashes* ou por outros sistemas criptográficos, por exemplo, que se utilizem de chaves privadas mantidas em separado pelo controlador ou pelo titular dos dados, que

funcionariam como meio para acesso à informação criptografada e pseudonimizada.

É ai que reside a diferença entre anonimização e pseudonimização. Dados anonimizados pretendem eliminar toda informação adicional que possa servir para identificar seu titular, uma vez que não há nenhum interesse do controlador em re-identificá-lo no futuro. Já no caso da pseudonimização, a informação adicional é mantida e guardada em ambiente controlado e seguro, com o intuito de posterior re-identificação.

Por isso, deve-se deixar claro que os dois não são etapas distintas de um mesmo processo, como o texto do Guia parece sugerir, mas processos bem diferentes entre si.

2.5 Relatório de Impacto de Proteção de Dados

Texto Guia (p. 32):

Esta etapa consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art 5º da LGPD). Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração do RIPD.

Art. 5º Para os fins desta Lei, considera-se:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

A conclusão desta etapa envolve registrar o e-mail e o telefone de contato do encarregado, já que ele é o canal de comunicação entre o controlador, titulares dos dados e ANPD.

Contribuições LAPIN:

Estes parágrafos tratam de alguns dos aspectos de maior confusão dentro da regulação do tratamento de dados na Administração Pública: a distinção entre

controladores e operadores em uma relação de tratamento de dados, principalmente em situações complexas onde há a possibilidade de atuação conjunta de controladores. Esta conceituação é essencial, uma vez que as obrigações e responsabilidades desses agentes são distintas e devem ser bem delimitadas.

Apesar da leitura do texto legal ser essencial para a compreensão dos institutos, cremos que situações práticas seriam de extrema valia para melhor exemplificar quais agentes públicos se enquadram nesses papeis, da seguinte forma:

Exemplo 1:

O órgão público X decide terceirizar a vigilância de suas instalações a uma companhia externa CE. A empresa terceirizada CE gerencia o pessoal envolvido no serviço, e o órgão X lhe exige somente que um número definido de seguranças esteja presente em pontos específicos.

São ambas as partes controladoras para o tratamento dos dados pessoais dos seguranças para a administração de recursos humanos pela empresa terceirizada, como para fins de avaliação de desempenho? A situação se alteraria se o órgão também delegasse à empresa o registro de visitantes às instalações?

É evidente que tanto o propósito quanto os meios para o tratamento dos dados dos seguranças não são determinados conjuntamente pelas partes envolvidas, sendo estes definidos autonomamente pela empresa terceirizada. Sendo assim, as partes não serão consideradas controladoras em relação ao tratamento de dados para fins de recursos humanos.

Entretanto, quando tratar os dados pessoais de visitante do órgão X, a empresa terceirizada estaria agindo sob as ordens do órgão público. Em outras palavras, a empresa CE deveria dar garantias da implementação de meios técnicos e organizacionais, com base nas requisições do controlador, o órgão público X, e agiria assim como operadora de tratamento dos dados.

Contudo, para as operações de tratamento de dados de seus empregados para fins trabalhistas, a empresa CE continua sendo controladora de dados.[13]

Exemplo 2:

Em um órgão público, o setor STI é responsável pelo desenvolvimento e administração técnica de uma ferramenta de tecnologia da informação que o setor de recursos humanos SRH utiliza. O setor SRH, que utiliza a ferramenta, define as

[13] *ibidem*

configurações e funcionalidades desta ferramenta. Qual seria o papel do setor STI, que desenvolveu o sistema?

O setor STI, por desenvolver, processar ou manter uma ferramenta de TI para o setor SRH, exerce o papel de operador dos dados tratados por esta ferramenta. Este setor não define o propósito ou os elementos essenciais dos meios do tratamento (p. ex.: o período de armazenamento, o acesso aos dados e o recipiente dos dados). Contudo, isto não obsta o setor STI a sugerir meios técnicos ao controlador dos dados, o setor SRH, a quem caberá decidir sobre estes meios.[14]

Exemplo 3:

Com base em poderes de investigação garantidos legalmente, o Ministério Público (MP) decide iniciar a investigação de uma suposta fraude em licitação noórgão da administração pública X, requerendo em juízo que haja busca e apreensão de informações junto a este órgão (que comumente possuem dados pessoais). O pedido é acatado pelo Judiciário.

O órgão X é compelido a agir, mas questiona se, neste caso, seria considerado como controlador do tratamento de dados para a investigação para fins da LGPD, ou se este é o próprio MP.

O que deve ser levado em consideração em uma relação de controladores conjuntos é quanto à definição conjunta da finalidade e dos meios para o tratamento.

Se as partes envolvidas não determinam conjuntamente o mesmo objetivo geral ou meios de tratamento, sua relação parece apontar para uma situação de "controladores separados".

Neste caso em específico, é evidente que as duas instituições não determinam conjuntamente o propósito da operação de tratamento. O órgão trata dados pessoais para um propósito específico, sendo este o procedimento de licitação.

Esta finalidade não coincide com a do Ministério Público, sendo esta de investigação da suspeita fraude. Quanto mais, cada uma das partes envolvidas tratam dados pessoais independentemente dos meios usados pelo outro controlador. Portanto, essa situação aponta que o órgão e o MP seriam controladores distintos.[15]

Estes exemplos visam demonstrar como a definição dos agentes envolvidos em uma relação de tratamento de dados pode ser complexa. Quanto

[14] *ibidem*

[15] Inspirado em EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725**. [*S. l.*], 7 nov. 2019, p. 10. Disponível em: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf. Acesso em: 10 maio 2020.

mais, a relação de critérios, na forma de *checklist* como o sugerido abaixo, poderia auxiliar na definição desses papéis.

Caso a maioria das respostas dadas pelo órgão para as perguntas feitas no *checklist* sejam "Sim", este provavelmente será o controlador do tratamento analisado, o mesmo se aplicando para a *checklist* referente ao operador.

***Checklist* - controlador:**

	Sim	Não
Você determinou o tratamento de dados pessoais ou determinou que outra entidade o realizasse?		
Você decidiu o propósito ou resultado que o tratamento precisa alcançar?		
Você decidiu os elementos essenciais do tratamento (p. ex.: quais dados pessoais devem ser coletados, sobre quais indivíduos, o período de retenção dos dados, quem tem acesso a esses dados, recipiente, etc.)?		
Você tem uma relação direta com os titulares?		
Você possui autonomia e independência (dentro das funções atribuídas a você por uma instituição pública) quanto o tratamento dos dados pessoais?		
Você apontou um operador para executar o tratamento em seu nome, mesmo que esta entidade determine os		

meios técnicos e organizacionais (elementos não-essenciais)?		

***Checklist* - operador:**

	Sim	Não
Você segue instruções de outra parte quanto o tratamento dos dados pessoais?		
Você possui autoridade quanto a determinação da coleta de dados pessoais?		
Você decide a base legal para a coleta e uso desses dados?		
Você decide o propósito ou propósitos quais os dados pessoais são usados?		
Você decide se ou para quem esses dados podem são divulgados?		
Você decide o período de retenção dos dados?		
Você toma certas decisões sobre como os dados são tratados, porém implementa essas decisões sob um contrato, outro instrumento legal ou convênio com o controlador?		
Você está interessado no resultado final do tratamento?		

Por fim, cabe aqui ressaltar a importância de que o Guia estabeleça uma ponte mais sólida entre a LGPD e o Decreto n. 10.046 no que diz respeito ao conceito de **gestor de dados**, presente no Decreto. O gestor será o controlador, operador ou o encarregado de dados? Ou nenhum deles, apenas um funcionário da pessoa jurídica controladora ou operadora? A definição desse conceito é primordial para uma compreensão mais ampla de como será a governança de dados dentro da Administração Pública Federal.

Texto Guia (p. 32-33):

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

- *Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);*
- *Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e*
- *A qualquer momento sob determinação da ANPD (art. 38).*

*Quando for necessária a elaboração do **RIPD**, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do **RIPD**.*

*A elaboração de um único **RIPD** para todas as operações de tratamento de dados pessoais ou de um **RIPD** para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um **RIPD** único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único **RIPD** não seja a opção mais indicada, optando por elaborar **RIPDs** segregados por ser mais adequado à sua realidade.*

*O **Relatório de Impacto** é elaborado ou atualizado sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:*

- *uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;*
- *rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);*
- *tratamento de 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" (LGPD, art. 5º, II);

- *processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);*
- *tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);*
- *tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);*
- *tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);*
- *tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);*
- *alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e*
- *reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.*

*Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o **RIPD** ser elaborado ou atualizado pela instituição.*

Contribuições LAPIN:

Nesse trecho, foram descritos todos fatores que devem ser considerados antes da feitura de um Relatório de Impacto de Proteção de Dados, de acordo com os elementos trazidos pela LGPD. Caso algum desses elementos seja constatado no caso concreto, a realização de RIPD será essencial.

Contudo, a maneira como esse texto trouxe as circunstâncias que devem ser consideradas para a realização de um RIPD, dividindo-as em duas listas distintas e desenvolvendo-as em longos parágrafos, pode trazer certa confusão para o leitor do guia, não havendo razão aparente para a discriminação das primeiras hipóteses das demais.

Nesse sentido, sugerimos que seja feita uma síntese das duas listas em uma só relação que descreva as hipóteses para realização de RIPD.

Texto guia (p. 34):

*A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal.*

(...)

*O **escopo** representa a abrangência do tratamento de dados.*

Contribuições LAPIN:

A conceituação da natureza e do escopo do tratamento de dados é essencial para a definição da necessidade da realização de um relatório de impacto de proteção de dados, em conjunto com o contexto e propósito deste tratamento.

A definição trazida no texto original do Guia pode trazer certa confusão ao leitor, uma vez que estes termos são definidos não só no Guia, mas também em outros instrumentos internacionais, de maneira demasiadamente abrangente, de difícil delimitação.

Sendo assim, a aplicação dos elementos que devem ser aferidos para a realização de um RIPD em um caso concreto seria crucial para a plena compreensão desses quesitos. A tabela abaixo busca elucidar uma possível forma de descrição desses critérios:

Exemplos	Natureza	Escopo
Instalação de câmeras para a realização de monitoramento em local de grande circulação	Dados serão coletados diretamente com titulares com finalidade "F" e serão transferidos para autoridade policial. Será utilizado algoritmo de reconhecimento facial.	Serão coletados dados biométricos sensíveis (art. 5º, II, LGPD) de tais pessoas em tal lugar por tanto tempo. Serão coletados "x" pontos da face dos titulares para identificação de maneira contínua. Os dados serão armazenados até o envio para autoridades. Somente afetará titulares que transitem pelo local de monitoramento.
Coleta de dados pessoais para levantamento de pessoas com problemas de saúde em determinada região.	Coleta realizada junto aos titulares por tal órgão com a finalidade "F", armazenada em base de dados estruturada de tal órgão e eliminados após	Serão coletados dados sensíveis de saúde (art. 5º, II, LGPD). Serão coletadas informações sobre a existência de doenças pré-existentes. O levantamento será

	período “P”. Os dados não serão compartilhados.	anual, sendo armazenado durante este período. Serão afetados “x” habitantes do bairro “B”

Texto Guia (p. 35):

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos. Especial atenção deve ser dedicada ao tratamento de dados pessoais realizado com base exclusivamente no consentimento do titular, que pode ocorrer excepcionalmente no caso dos órgãos e entidades públicas. Em ocorrendo, a ***finalidade*** *deve ser precisamente detalhada. Nesse caso, é importante:*

- *Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.*
- *Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.*

Contribuições LAPIN

Cremos ser descabida que a indicação das finalidades, dos resultados e benefícios pretendidos com o tratamento seja feita somente para as hipóteses onde haja o tratamento com base no consentimento. Tal postura pode dar a falsa impressão de que o princípio da finalidade só se aplique aos tratamentos feitos com suporte apenas nessa hipótese legal.

Todo serviço público deve, a princípio, possuir um objetivo pré-definido por lei e satisfazer as necessidade coletivas[16]. Além disso, o juízo de finalidade, necessidade e adequação no tratamento de dados deve ser feito em qualquer hipótese de tratamento. Sendo este realizado para a satisfação ou execução de um serviço público, independentemente da base legal adotada, deverá ser aferível a finalidade legal e interesse coletivo almejado.

[16] PIETRO, Maria Sylvia Zanella Di. **Direito Administrativo**. 31ª. ed. Rio de Janeiro: Forense, 2018. p. 177.

Conclusão

Por concentrar uma larga quantidade de informações de cidadãos para fundamentar o cumprimento de obrigações legais e a construção de políticas públicas, a Administração Pública Federal é uma controladora de dados de extrema relevância para o ambiente digital brasileiro. Por isso, a definição de uma estratégia sólida de governança de dados é fundamental para garantir o exercício de direitos de privacidade e proteção de dados à população.

O **Guia de Boas Práticas para Implementação na Administração Pública Federal - Lei Geral de Proteção de Dados (LGPD)** exerce um importante papel nesse contexto, ao iluminar conceitos chave da LGPD de forma didática para que o gestor público possa tomar decisões fundamentadas e protetivas a respeito dos dados que estão sob seu controle.

Nesse contexto, os comentários que apresentamos ao documento pretendem contribuir com o aprimoramento constante deste Guia, e se relacionam diretamente com o encaminhamento que o governo brasileiro tem feito para sua maior abertura à sociedade.

Isto posto, o **Laboratório de Políticas Públicas e Internet - LAPIN** se põe à disposição deste **Comitê Central de Governança de Dados**, cujo papel é fundamental para o ambiente de governança de dados no aparato estatal, para apoiá-lo com esta e demais iniciativas que visem aprimorar o sistema regulatório de proteção de dados brasileiro.