REVISTA SEMESTRAL DE DIREITO EMPRESARIAL

Nº 25

Publicação do Departamento de Direito Comercial e do Trabalho
da Faculdade de Direito da Universidade do Estado do Rio de Janeiro

Rio de Janeiro
Julho / Dezembro de 2019

REVISTA SEMESTRAL DE DIREITO EMPRESARIAL

Nº 25 Julho/Dezembro de 2019

Publicação do Departamento de Direito Comercial e do Trabalho da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (Prof. Alexandre Ferreira de Assumpção Alves, Prof. Eduardo Henrique Raymundo Von Adamovich, Prof. Enzo Baiocchi, Prof. Ivan Garcia, Prof. João Batista Berthier Leite Soares, Prof. José Carlos Vaz e Dias, Prof. José Gabriel Assis de Almeida, Prof. Leonardo da Silva Sant'Anna, Prof. Marcelo Leonardo Tavares, Prof. Mauricio Moreira Menezes, Prof. Rodrigo Lychowski e Prof. Sérgio Campinho).

ISSN 1983-5264

CIP-Brasil. Catalogação-na-fonte
Sindicato Nacional dos Editores de Livros, RJ.

Revista semestral de direito empresarial. — nº 25 (julho/dezembro 2019)
. — Rio de Janeiro: Renovar, 2007-.
v.

UERJ
Campinho Advogados
Moreira Menezes, Martins Advogados

Semestral
1. Direito — Periódicos brasileiros e estrangeiros.

94-1416. CDU — 236(104)

* Publicado no segundo semestre de 2021.

O CONCEITO DE 'AGENTES DE TRATAMENTO' NA LGPD: UM OLHAR SOBRE SUA INTERPRETAÇÃO INICIAL NO BRASIL[1]

THE CONCEPT OF PERSONAL DATA 'PROCESSING AGENTS' IN BRAZILIAN GENERAL DATA PROTECTION LAW: A GLANCE AT INITIAL INTERPRETATION IN BRAZIL

Leonardo Figueiredo Barbosa

Resumo: O presente artigo examina o conceito de agentes de tratamento de dados pessoais trazido pela Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018). Considerando algumas interpretações que têm sido dadas na definição de controladores e operadores – mormente no setor público, mas que podem vir a ser incorporadas pela iniciativa privada – é fundamental problematizar tais interpretações diante de uma visão mais sistemática da LGPD, bem como cotejar essas novas figuras jurídicas em nosso ordenamento com as definições oriundas do contexto europeu que as inspirou.

Palavras-chaves: Dados pessoais. Agentes de tratamento. Controlador. Operador. LGPD.

Abstract: This article examines the concept of personal data processing agents brought by the Brazilian General Personal Data Protection Law (LGPD - Law 13.709/2018). Considering some interpretations about definition of controllers and processors that have been given by public sector entities in Brazil, it is important to problematize such interpretations in the context of a more systematic view of LGPD, as well as to compare these new legal figures in Brazilian order with the definitions coming from the European context.

---

1 Artigo recebido em 26.07.2021 e aceito em 16.08.2021.

Keywords: Personal data. Personal data processing agents. Controller. Processor. Brazilian General Data Protection Law (LGPD).

Introdução.

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/18), apesar de não ter inaugurado a preocupação com o tema da proteção de dados pessoais na legislação brasileira[2] como, inadequadamente, tem sido propagado por alguns, trouxe realmente diversas inovações significativas para a matéria. Dentre elas, a especificação de novas figuras jurídicas, como a de *agentes de tratamento* de

2 Apenas exemplificativamente, (e para não repetir os já combalidos exemplos acerca das previsões pontuais no Código de Defesa do Consumidor e no Marco Civil da Internet) a Lei de Acesso à Informação (Lei 12.527/2011) já trazia, há quase 10 anos, diversas previsões acerca do tratamento de informações pessoais: conceituação de 'informação pessoal' e de 'tratamento' de forma similar à LGPD; preocupação com a segurança da informação pessoal e restrição de acesso; responsabilização por uso indevido, tanto institucional como das pessoas naturais envolvidas; dentre outras.

dados pessoais, gênero do qual são espécies os *controladores* e os *operadores*.

O objetivo desse artigo é analisar a adequada conceituação jurídica desses personagens, o que será feito a partir da análise não só da LGPD e de documentos recentemente divulgados pelo Governo Federal,[3] mas também pelo seu cotejamento em relação aos documentos europeus que tratam do tema, considerando ser essa nossa maior fonte de inspiração na área de proteção de dados.

O tema é relevante em função de sua atualidade e do impacto, seja econômico ou cultural, que já está ocasionando tanto no setor público como na iniciativa privada. Isto porque diversos deveres e responsabilidades são direcionados, pela LGPD, aos agentes de tratamento e tanto a concretização dos direitos dos titulares quanto a própria construção de uma cultura de proteção de dados pessoais em nosso país dependem, em grande medida, da correta compreensão desses conceitos. Todavia, a lei deixa em aberto muitos aspectos, fazendo com que diversos pontos dependam de interpretação e esclarecimentos que ainda estão sendo construídos, ao menos do ponto de vista administrativo ou judicial.

Isso tudo foi agravado pelo contexto específico relacionado ao processo de entrada em vigor da LGPD, considerando que não obstante aprovada e publicada desde 14 de agosto de 2018, sua completa vigência foi adiada algumas vezes. Com isso, a efetiva atuação da Autoridade Nacional de Proteção de Dados (ANPD), que poderia/deveria ter sido criada há cerca de dois anos, também foi postergada. Somente nos últimos dias a autoridade começou a minimizar as divergências na interpretação da lei, concretizando algumas de suas

---

3 Desde setembro de 2020 o Governo Federal criou uma página denominada "Guias Operacionais para adequação à LGPD" na qual vem, sistematicamente, publicando orientações para a implementação da LGPD na esfera do Poder Executivo Federal. Mais recentemente – em maio de 2021 – após a finalização da primeira versão deste artigo, a própria ANPD publicou o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", confirmando a visão defendida no presente trabalho.

atribuições legais, quais sejam a promoção do conhecimento das normas e das políticas públicas sobre proteção de dados; a elaboração de estudos sobre as práticas nacionais e internacionais relacionadas ao tema; bem como a interpretação da lei em caráter terminativo na esfera administrativa (art. 55-J, VI, VII e XX).

Mas, antes da divulgação de tais esclarecimentos – durante a ausência efetiva de uma autoridade administrativa capaz de esclarecer certas dúvidas – tanto o setor público quanto a iniciativa privada vinham buscando cumprir as determinações do novo texto normativo da forma como entendem mais adequada. Porém, todo o cenário exposto acima causou uma cacofonia interpretativa sobre a lei, sendo que, umas das mais expressivas, foi aquela relativa à conceituação dos agentes de tratamento.

1. O conceito de 'agentes de tratamento' na LGPD.

Como já indicado acima, a Lei Geral de Proteção de Dados Pessoais cria o conceito de agentes de tratamento, definindo-o como "o controlador e o operador" (art.5º, IX) e, quanto a estes últimos, especifica:

> 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; (grifo nosso)

No que concerne a definição e esclarecimentos sobre os conceitos, é tão somente isso que dispõe o texto legal. Importante enfatizar que, apesar da lei brasileira se inspirar claramente na tradição

normativa europeia sobre proteção de dados,[4] não se adotou no Brasil a mesma metodologia da atual regra europeia – o GDPR – que, além dos artigos, parágrafos e incisos comuns às normas legais, também incorporou 173 notas explicativas (*recitals* ou considerandos) sobre os principais pontos da lei, buscando esclarecer, aprofundar e orientar sua adequada compreensão e aplicação. Obviamente, isso se justifica pela história europeia, em que alguns países debatem o tema da proteção de dados pessoais há, pelo menos, 50 anos, sendo certo que o Brasil não compartilha dessa tradição.

2. A interpretação inicial dos conceitos no Brasil.

Diante da efetiva entrada em vigor da LGPD (com exceção da seção das sanções administrativas, adiada para agosto de 2021), as instituições iniciaram um movimento mais robusto de adequação ao texto normativo.

O Conselho Nacional de Justiça (CNJ), por exemplo, atento ao papel que o judiciário exercerá no tema de proteção de dados, editou alguns documentos dentre os quais a Recomendação 73/2020[5] indicando aos órgãos do Poder Judiciário brasileiro que adotem medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases, dentre as quais:

> Art. 1º [...]
> II – disponibilizar, nos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários:
> a) informações básicas sobre a aplicação da Lei

4 O *General Data Protection Regulation* (*GDPR*) ou *Regulation* (*EU*) 2016/679 é a principal norma a regulamentar o tema na União Europeia (além de Irlanda, Noruega e Liechtenstein). Aprovada em 27 de abril de 2016, entrou em vigor em 25 de maio de 2018, substituindo a *Diretive 95/46/EC* que regulamentava o tema desde 1995. Disponível em: «https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679». Acesso em: 08 dez. 2020.

5 Disponível em: «https://atos.cnj.jus.br/atos/detalhar/3432». Acesso em: 08 dez. 2020.

> Geral de Proteção de Dados aos tribunais, incluindo os requisitos para o tratamento legítimo de dados, as *obrigações dos controladores* e os direitos dos titulares; (grifo nosso)

Os órgãos de Poder Judiciário começaram a criar documentos internos especificando quem seriam os controladores (e os operadores), no que foram acompanhados por diversas instituições públicas. Não obstante seja importante reconhecer esforço dessas instituições na busca pela adequação à lei e na promoção de uma cultura de privacidade e proteção dos dados pessoais, entende-se necessário problematizar algumas colocações que (embora sejam compreensíveis diante da inovação da matéria, da ausência de definições normativas mais aprofundadas e da falta de orientações pela ANPD até aquele momento), podem direcionar a compreensão de toda nossa sociedade, dificultando a apropriada operacionalização da lei.

O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), por exemplo, criou a 'Política de Privacidade dos Dados das Pessoas Físicas' (PPD),[6] que "estabelece princípios e normas que devem nortear o tratamento de dados pessoais, físicos e digitais, no Tribunal, a fim de garantir a proteção da privacidade de seus titulares, bem como define papéis e diretrizes iniciais para obtenção da gradual conformidade" do Tribunal à LGPD.O documento estabelece que *controlador* é "pessoa jurídica *de direito público* a quem compete definir todas as ações relativas ao tratamento dos dados pessoais" (art. 3º, XVIII) e que *operador* é "pessoa *física* que realiza o tratamento em nome do controlador, em todas as instâncias da instituição ou no âmbito de contratos ou instrumentos congêneres firmados com ele", mas, paradoxalmente, afirma que

> Art. 5º No Tribunal, o *Controlador* e os *Operadores* são *respectivamente* o *Presidente do Tribunal*,

6 Resolução 9/2020. Disponível em: «https://www.tjdft.jus.br/institucional/imprensa/noticias/arquivos/resolucao-9-2020-1.pdf». Acesso em: 10 nov. 2020.

> assessorado pelo Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais - CGSI, e os *servidores e colaboradores* que exerçam atividade de tratamento de dados pessoais na instituição *ou terceiros*, em contratos e instrumentos congêneres firmados com o Tribunal. (grifo nosso)

Além disso, cria a figura de *controlador conjunto*, a ser exercida pelos Vice-Presidentes e pelo Corregedor da Justiça (art. 5º, § 1º).

Sem adentrar aspectos específicos da LGPD, pode-se apontar o problema em afirmar que controlador é "pessoa jurídica de direito *público*", mas será o presidente do tribunal. Além disso, também se indica que operador é "pessoa *física*", mas pode ser terceiro com quem o tribunal estabeleça contratos ou congêneres o que, na maior parte dos casos, ocorrerá por meio de pessoa jurídica.

O Ministério Público do Rio Grande do Sul também é um exemplo interessante dessas primeiras tentativas de adequação a lei. Por meio do Provimento 68/2020 PGJ,[7] traz definições de *controlador* e operador muito similares as do TJDFT.[8] Todavia, é interessante observar que, diferentemente do que foi estabelecido pelo tribunal, o artigo 5º desse documento estipula que o "Ministério Público do Estado do Rio Grande do Sul é o *controlador* dos dados pessoais a sua disposição e a ele compete decidir sobre o tratamento destes dados".

Ou seja, enquanto na primeira situação há indicação da pessoa física que ocupa o cargo de presidente da organização como controlador, na segunda é a própria instituição – como ente responsável

---

7 Disponível em: «https://www.mprs.mp.br/legislacao/provimentos/14204/». Acesso em: 20 set. 2020.

8 O documento do MP-RS é anterior ao do TJDFT. O artigo 2º, VII indica que controlador é "pessoa jurídica de direito *público* a quem competem as decisões referentes ao tratamento dos dados pessoais" e o inciso VII define operador como "pessoa *natural* que realiza o tratamento de dados pessoais em nome do controlador".

para tomar as decisões sobre o tratamento – que é apontada como agente de tratamento. É bem verdade que a LGPD permite que tanto pessoas físicas como jurídicas sejam agentes de tratamento, mas veremos nas seções seguintes os problemas que podem advir da divergência acima aventada.

Já no que concerne aos *operadores*, o provimento do MP-RS indica "os membros, servidores e estagiários da Instituição" (art. 6º).

Os exemplos do TJDFT e do MP-RS, desconsideradas as inconsistências internas já indicadas, não contrariam o texto expresso do artigo 5º da LGPD que conceitua os agentes de tratamento. Entretanto, não estão de acordo com o entendimento consolidado na tradição europeia que nos inspirou, motivo pelo qual foram alvo de críticas no meio especializado.[9]

3. Controlador (*controller*) e operador (*processor*) no contexto da União Europeia.

A compreensão dos conceitos de "controlador" e "operador" é fundamental para a adequada concretização da LGPD. Todavia, podem existir divergências já que a lei fornece apenas conceitos demasiadamente amplos e a ANPD ainda não se posicionou.

---

9 Tal debate gerou questionamento expressivo, mormente nas mídias especializadas. Apenas exemplificativamente, o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) dedicou um de seus encontros da série 'Varandas ITS' (atividades periódicas organizadas para promover conversas informais sobre temas relevantes ligados à tecnologia, política, cultura, sociedade e democracia) para debater sobre "LGPD no setor público: a controvérsia de servidores-operadores". O evento contou com a participação de Danilo Doneda, Marcos Lindemeyer (CGU - da equipe de elaboração do Guia de Boas Práticas: Lei Geral de Proteção de Dados), Nathalie Lanaret (*Centre for Information Policy Leadership/CIPL* – especialista da União Europeia e redatora dos comentários para as Diretrizes sobre os Conceitos de Controlador e Operador do EDPB) e Newton Moraes (MP-RS – da equipe de redação do ato supracitado). Disponível em: «https://itsrio.org/pt/varandas/lgpd-no-setor-publico-a-controversia-de-servidores-operadores/». Acesso em: 30 out. 2020.

Diante de tais dissensos e considerando ser inegável que a legislação europeia é a maior inspiração da LGPD (ainda que existam diferenças relevantes)[10] pode ser importante compreender como o GDPR (enquanto norma que, atualmente, consolida boa parte da tradição de proteção de dados pessoais daquela cultura) interpreta tais conceitos. Além disso, existem outros documentos relevantes que podem colaborar para essa compreensão, conforme será apresentado adiante.

Iniciando pelos dispositivos do GDPR, percebe-se que os conceitos de *controller* (controlador) e *processor* (operador) são muito similares aos adotados pela LGPD, ainda que com sutis diferenças, conforme indicados no *article* 4:

> (7) '*controller*' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determinesthe purposes and means* of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
> (8) '*processor*' means a natural or legal person, public authority, agency or other body which processes personal data *on behalf of* the controller; (grifo nosso)

Fazendo uma analogia entre LGPD e GDPR, os documentos do TJDFT e do MP-RS parecem – com base apenas na leitura do texto do artigo 4º – não contrariar suas disposições. Porém, além desses

10 Para uma análise comparativa entre GDPR e LGPD ver, entre outros, PARENTONI, Leonardo; LIMA, Henrique. Proteção de dados pessoais no Brasil: antinomias internas e aspectos internacionais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA, Cíntia; MACIEL, Renata Mota (Coords.). *Direito & Internet IV*: Sistema de Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019, p. 483-511.

conceitos, é importante analisar orientações e documentos divulgados pelos organismos e autoridades europeus relacionados ao tema da proteção de dados.

Um dos mais recentes é a *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*,[11] de 02 de setembro deste ano, produzido pelo Comitê Europeu para a Proteção de Dados.[12] O documento dedica quase 50 páginas para esclarecer, problematizar e dar exemplos práticos, acerca dos conceitos de controlador e operador, das consequências dessa atribuição de papéis e da responsabilização decorrente dessas relações.

Nesse documento, o EDPB, preliminarmente, enfatiza a necessidade de compreender que se trata de conceitos autônomos e funcionais. São *autônomos* porque devem ser interpretados considerando primordialmente a legislação de proteção de dados europeia e não com base em influências advindas de outras áreas do direito. São *funcionais* porque têm como objetivo "distribuir responsabilidades de acordo com os papéis reais" que as partes têm nas atividades de tratamento. Isto significa que, baseado no princípio da *accoun-*

---

11 Disponível em: «https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf». Acesso em: 20 out. 2020. Importante destacar que esse não é o primeiro documento de organizações da União Europeia visando esclarecer tais conceitos. Em 2010, ainda sob vigência da *Diretive 95/46/EC*, o *Article 29 Working Party* (grupo de trabalho europeu independente, também conhecido por WP29, criado por determinação do artigo 29 daquela diretiva) publicou o *Opinion 1/2010 on the concepts of "controller" and "processor"* no qual diversas orientações, indicadas agora, já estavam presentes. Portanto, a relevância dessa distribuição e diferenciação de papeis e responsabilidades no contexto da proteção de dados da UE não surgem com a GDPR, mas sim com a diretiva de 1995. Todavia, diante da promulgação do regulamento europeu e de algumas inovações trazidas pela norma, entendeu-se necessário revisitar as orientações e prover mais esclarecimentos.

12 O *European Data Protection Board* (*EDPB*) organismo europeu independente – composto pela Autoridade Europeia para a Proteção de Dados e por representantes das respectivas autoridades nacionais para a proteção de dados – que promove a cooperação entre tais autoridades e contribui para interpretação e a aplicação coerente de regras sobre proteção de dados na União Europeia.

tability, esses conceitos identificam papéis que caracterizam *quem é responsável* pelo cumprimento de diferentes regras de proteção de dados pessoais, além do modo como os titulares dos dados podem exercer os seus direitos na prática, isto é, seu objetivo é justamente o de buscar garantir uma proteção abrangente para os dados pessoais por meio da responsabilização adequada dos agentes de tratamento.[13] Portanto, a distinção entre controlador e operador, acarreta consequências expressivas, desde a obrigatoriedade de adoção de medidas aptas a promover essa proteção de forma contextualizada aos riscos de cada tratamento, passando pela demonstração da efetividade de tais medidas e, consequentemente, chegando ao dever de compensar os titulares por eventuais danos advindos do tratamento inadequado.[14]

3.1. *Controller*.

No que concerne ao *controller* (controlador), o documento afirma que a definição é composta por cinco elementos: (*i*) pessoa natural ou jurídica, autoridade pública, agência ou outro organismo; (*ii*) que determina; (*iii*) individualmente ou em conjunto com outros; (*iv*) as finalidades e os meios; (*v*) do tratamento de dados pessoais.[15]

(i) Sobre o tipo de entidade que pode ser caracterizada como controlador, o documento é incisivo ao esclarecer que embora não exista, a princípio, limitação sobre quem pode ocupar esse papel, em regra é a organização que é classificada como controlador, e não um indivíduo que a integra.

---

13 EDPB, op. cit., p. 7-9.

14 No mesmo sentido, MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*. São Paulo: Ed. RT, nov./dez. 2018. v. 120,p. 469-483.

15 EDPB, op. cit., p. 9-16.

Isso está intrinsecamente relacionado com o próximo elemento do conceito.

(ii) Determinar' significa exercer o poder de decisão, sendo o controlador quem determina elementos essenciais do tratamento. Essa ideia pode, nesse caso, ser traduzida nas seguintes perguntas: "Por que um tratamento específico está ocorrendo?" e "Quem decidiu que o tratamento deve ocorrer para um propósito específico?"

Este controle sobre o tratamento de dados pessoais pode decorrer de previsões legais ou da influência decisória factual sobre o tratamento. Na primeira hipótese, é comum que diferentes normas estabeleçam tarefas ou deveres que só podem ser efetivamente concretizados a partir do tratamento de dados pessoais. É exatamente o caso de órgãos ou instituições públicas que, para concretizarem suas atribuições, precisam analisar, usar, armazenar ou de qualquer outra forma tratar os dados de seus cidadãos. Sendo assim, conforme afirma o EDPB, "essas entidades normalmente seriam consideradas como controladores no que diz respeito ao processamento necessário para o cumprimento dessa obrigação". Quanto à segunda hipótese, na ausência de determinações legais claras, a identificação do controlador precisa ser estabelecida com base na avaliação das circunstâncias factuais de cada tratamento, visando apurar quem realmente exerce influência decisiva sobre as finalidades e os meios para atingi-las. Tal poder decisório específico pode derivar de diversas circunstâncias: porque decorre das diligências típicas de uma atividade ou modelo de negócios, porque existe previsão contratual (obviamente, em consonância com a realidade dos fatos) ou, simplesmente, porque o contexto factual específico indica quem exerce o efetivo controle.[16]

16 Ibidem, p. 9-11. O documento traz alguns exemplos interessantes desse controle decorrente

(iii) 'Individualmente ou em conjunto com outros' indica que o exercício do poder de decisão acerca do tratamento de dados pessoais pode ser efetivado por uma única instituição ou por diferentes entidades. Neste último caso significa que essas diferentes instituições agem, simultaneamente, como controladoras no que concerne aquele tratamento específico.

Essa possibilidade é prevista expressamente no artigo 4 (7) do GDPR, já indicado acima, no trecho que afirma "'*controller*' means the natural or legal person, public authority, agency or other body which, *alone or jointly with others*, determines the purposes and means of the processing of personal data [...]".

Portanto, uma entidade ou organização pode ser caracterizada como controladora, mesmo que não tome todas as decisões quanto aos propósitos e meios relacionados ao tratamento de dados pessoais.[17]

(iv) As *finalidades* e os *meios* representam, respectivamente, o propósito ou objetivo que se pretende alcançar com o tratamento dos dados pessoais (o "por quê?" do tratamento) e o modo ou maneira por meio da qual se pretende atingir aquele objetivo (o "como?" do tratamento), sendo certo que o controlador deve decidir tanto as finalidades como os meios.

Obviamente, isso não significa que não exista alguma mar-

---

de influência factual: o empregador em relação ao tratamento de dados pessoais de seus funcionários; o editor que trata dados de seus assinantes; a associação que lida com dados de seus membros ou apoiadores; bem como escritórios de advocacia em relação aos dados, inclusive de terceiros, repassados por seus clientes para que possam atuar em processos administrativos, judiciais ou de arbitragem.

17 Ibidem, p. 12-13.

gem de manobra para que os operadores tomem certas decisões sobre *como* realizar o tratamento. Em função disso, é importante diferenciar os meios *essenciais* dos *não essenciais*. Aqueles estão intimamente ligados à finalidade e ao escopo do tratamento, portanto, inerentemente reservados ao controlador (a escolha das categorias de titulares e dos dados específicos a serem tratados, a duração do tratamento e a definição sobre quem pode ter acesso são exemplos de meios essenciais). Já os "meios não essenciais" se relacionam a aspectos mais práticos de implementação (definição sobre um tipo particular de *hardware* ou *software* ou os detalhes acerca das medidas de segurança) podendo ser definidos pelos operadores. Todavia, o controlador deve, mesmo em relação aos meios não essenciais, estipular algumas orientações, ainda que gerais (como, por exemplo, definir que as medidas de segurança estejam de acordo com determinada *guideline*) até mesmo porque o controlador continua, em qualquer situação, responsável pela implementação das medidas técnicas e organizacionais apropriadas, bem como pela demonstração de que os tratamentos seguiram as determinações legais, sendo aconselhável que estipule tais especificações em contrato, de modo a tentar demonstrar a busca de conformidade das operações.[18]

(v) As finalidades e meios que são determinadas pelo(s) controlador(es) devem, evidentemente, relacionar-se com 'o tratamento de dados pessoais' caracterizado qualquer operação ou conjunto de operações – realizadas ou não por meio automatizado – efetuadas com dados pessoais ou

18 Ibidem, p. 13-14. Portanto, enfatize-se, as decisões sobre os objetivos ou finalidades são sempre dos controladores.

> conjuntos de dados pessoais. Aqui é relevante enfatizar que a definição do *controlador* (como a de *operador*) pode se relacionar à totalidade dos processamentos de dados feitos por uma entidade, bem como a operações específicas ou, até mesmo, a um estágio específico do tratamento.[19]

Também é relevante ressaltar que, para a caracterização como controlador, não é necessário que o agente de tratamento tenha acesso aos dados pessoais que estão sendo processados. É o exemplo de uma entidade que terceiriza o tratamento de dados pessoais: mesmo que na prática não efetue o acesso real aos dados, o que deve ser considerado é a real capacidade de exercer poder decisório acerca das finalidades e meios (essenciais) do tratamento.[20]

Após essas explicações, pode-se retornar aos exemplos do MP-RS e do TJDFT para uma análise crítica: será adequado imaginar que os dados pessoais que são coletados por um Tribunal de Justiça, bem como os tratamentos subsequentes decorrem da decisão de seu Presidente (ou dos Vice-Presidentes ou do Corregedor da Justiça)? É ele que determina tanto as *finalidades* como os *meios* para alcançar os objetivos de todos os tratamentos de dados pessoais realizados no tribunal? Ou a escolha do Ministério Público de indicar a própria instituição como controlador parece mais adequada às orientações do EDPB?

A *guideline* parece indicar uma resposta correlata:

> Algumas vezes, empresas e órgãos públicos nomeiam uma *pessoa específica* como responsável pela implementação das operações de tratamento. Mesmo se uma pessoa física específica for no-

19 Ibidem, p. 15-16.

20 Ibidem, p. 16.

> meada para garantir o *compliance* em relação às regras de proteção de dados, esta pessoa *não será o controlador*, mas *agirá representando a pessoa jurídica* (empresa ou órgão público) que *será o responsável final em caso de violação das regras* em sua capacidade de *controlador*.[21] (grifo e tradução livre nossa)

Portanto, ao menos na visão europeia, a figura do controlador não se confunde com a da pessoa física que age em nome do órgão, sendo a própria entidade que responderá em eventuais casos de violação das regras de proteção de dados pessoais. Isso porque, frise-se, o objetivo central da definição da figura jurídica de controlador está relacionado com a responsabilização e prestação de contas que busca, primeiramente, garantir o pleno efeito da legislação de proteção de dados, fomentando uma proteção efetiva e abrangente e evitando ou, pelo menos, minimizando, os danos que podem advir do tratamento e, posteriormente, assegurar a responsabilidade pelo ressarcimento desses danos. Portanto, a identificação da figura do controlador (assim como a do operador, como se verá a seguir) independe de indicação, nomeação ou previsão contratual, mas, antes, pressupõe a análise efetiva das circunstâncias que envolvem as atividades de tratamentos de dados pessoais.

3.2. *Processor*.

No que concerne ao *processor* (operador), conforme já citado no início da seção 3, a leitura do artigo 4(8) do GDPR parece não limitar o tipo de entidade passível de exercer tal papel. Apesar disso, as orientações do EDPB afirmam que há duas condições essenciais

21 Ibidem, p. 11.

para sua identificação: (i) que seja uma *entidade separada* do controlador e (ii) que realize o tratamento dos dados pessoais "em nome do controlador" (*on the controller's behalf*).[22]

"Entidade separada" significa que o controlador decide delegar atividades de tratamento de dados pessoais, no todo ou em parte, para um ente externo que, portanto, não se confunde com ele. Já o termo "em nome do controlador" indica que aquela entidade externa realiza o tratamento para o benefício do controlador, implementando as orientações por ele dadas, porém sem que isso ocorra de uma forma subordinada ao controle direto do controlador.

Tais afirmações parecem encontrar respaldo em uma leitura mais atenta e de interpretação sistemática do GDPR, em função de um conceito previsto no artigo 4 (10) e que não foi incorporado formalmente pela lei brasileira, qual seja, o conceito de *terceiro*:

> (10) 'third party' means a natural or legal person, public authority, agency or body other than the *data subject*, *controller*, *processor* and persons who, under the direct authority of the controller or processor, are authorised to process personal data; (grifo nosso)

Conforme se pode perceber, além de diferenciar os conceitos de 'terceiro', 'titular', 'controlador' e 'operador', o dispositivo também enfatiza (e esse é o destaque) que não se pode confundir o conceito de operador (*processor*) com as pessoas que, *sob a autoridade direta*

---

22 Ibidem, p. 24. Tais argumentos, em alguma medida, já estavam indicados na *Opinion 1/2010 on the concepts of "controller" and "processor"* do WP29. Ver ZANATTA, Rafael A. F. Agentes de tratamento de dados, atribuições e diálogo com o Código de Defesa do Consumidor. In: SOUZA, Carlos Affonso et al. (Coord.). *Caderno Especial*: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019, p. 183-198.

do controlador ou do operador, estão autorizadas a tratar dados pessoais.[23]

Sendo assim, seja em função das orientações do EDPB ou a partir do próprio texto do regulamento europeu, há distinção entre aqueles que tratam dados pessoais "em nome do controlador" (os operadores), e aqueles que estão autorizados a tratar tais dados "sob a autoridade direta" seja do controlador seja do operador.

> Se o controlador decidir tratar os dados por conta própria, *usando seus próprios recursos dentro de sua organização*, por exemplo, por meio de *sua própria equipe, isso não caracteriza o papel de operador*. Funcionários e outras pessoas que estão agindo sob a *autoridade direta do controlador* [...] não devem ser vistos como operadores, uma vez que irão tratar dados pessoais enquanto parte da instituição controladora.[24] (grifo e tradução livre nossa)

Conclui-se que, ao menos no contexto da União Europeia, não se pode tratar empregados, estagiários, demais colaboradores ou quaisquer integrantes de uma organização (seja ela pública ou privada) que atuem em uma relação de subordinação, como se fossem 'operadores' no sentido dado pelo GDPR.

---

23 Diferenciação similar ocorre em normas de boa prática que tratam sobre o tema. É o caso da ABNT NBR ISO/IEC 29100 aprovada em março de 2020 (que pretende ser uma tradução idêntica da ISO/IEC 29100:2011). O item 2.25 define "terceiro" como "parte interessada na privacidade que não o titular de dados pessoais (DP), o controlador de DP e o operador de DP, e as pessoas naturais que são autorizadas a tratar os dados sob direta autoridade do controlador de DP ou do operador de DP".

24 EDPB, op. cit., p. 24.

3.3. O caso da divulgação de conceito pelo professor austríaco.[25]

Um recente exemplo, que ilustra as explicações apresentadas acima, refere-se a uma reclamação de uma estudante contra professor que disponibilizou as 'notas' de suas avaliações para terceiros – prática que também não é incomum no Brasil.

O docente havia conversado com estudantes e representantes de turma sobre os conceitos avaliativos, bem como demais informações que detalhavam como esses teriam sido estipulados. Tendo em vista que a discente indicada estava ausente no dia em que isso ocorreu presencialmente, os representantes, por sua vez, fizeram a divulgação dos resultados da avaliação por intermédio de um grupo de WhatsApp dos estudantes, de forma que todos os integrantes do grupo puderam ter acesso aos conceitos que ela obteve.

Diante disso, a aluna fez uma reclamação junto a autoridade nacional de proteção de dados austríaca, especificamente contra o professor, sob alegação de que o procedimento iniciado por ele violaria seu direito a confidencialidade, pois os graus seriam dados pessoais e, portanto, seu tratamento deveria respeitar as previsões tanto do GDPR quanto do *Austrian Data Protection Act*.[26]

O relevante para o tema específico desse artigo é que, após a autoridade de proteção de dados ter concordado com o pedido da estudante, o docente recorreu da decisão por meio de apelação a *Federal Administrative Court* (*Bundesverwaltungsgericht - BVwG)*. Dentre as principais alegações, o professor afirmava que ele não deveria ser considerado controlador (*controller*) e, portanto, não pode-

---

25 Disponível em: «https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20200930_W274_2225135_1_00/BVWGT_20200930_W274_2225135_1_00.html». Acesso em: 21 out. 2020.

26 Lei austríaca que contêm disposições complementares ao GDPR. Disponível em: «https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1000159». Acesso em: 21 out. 2020.

ria ser responsabilizado pela situação nos termos do GDPR, pois apenas estaria cumprindo suas obrigações como docente nos termos das leis e demais regulamentos educacionais.

Nesse sentido, a corte entendeu que a análise do caso depende da compreensão sobre quem pode ser responsabilizado, no que concerne à proteção de dados, considerando as normas educacionais específicas que regulam as atividades educacionais e avaliativas no país. Conforme tal legislação, apesar do docente ter certa margem de autonomia na realização de suas funções, ele as realiza sob a supervisão direta da organização. Apenas exemplificativamente, a legislação austríaca determina que cabe ao diretor da escola – em nome da instituição educacional – a verificação de cumprimento das leis federais, regulamentos ou de quaisquer instruções das autoridades educacionais, salvo se houver indicação normativa de outra entidade ou autoridade competente. O diretor também é o superior direto de todos os professores que trabalham na escola.[27]

Com base nesse e em outros argumentos, a corte afirmou que o conceito do *controlador* está relacionado a pessoas ou organizações que podem influenciar significativamente o cumprimento das normas de proteção de dados e que as responsabilidades devem ser delegadas àqueles que efetivamente têm o poder de decisão.

Nesse sentido, ainda que se compreenda que a função de docente tem alguma margem de autonomia, o professor desempenha todas as tarefas na escola e sob a supervisão do diretor. Além disso, definir medidas e procedimentos para assegurar que o tratamento de dados pessoais esteja de acordo com normas legais e regulamentares (como são processados os dados, a quem são transmitidos, onde são

27 Não faz parte do escopo deste trabalho fazer uma análise dos pontos específicos da legislação educacional austríaca, mas tão somente apresentar a decisão, no mesmo sentido das orientações supracitadas da EDPB, que distingue a figura do *controller* ou do *processor* daqueles que atuam dentro dessas organizações, de forma subordinada, ainda que exista alguma margem de autonomia em sua esfera de atuação.

armazenados, como e quando devem ser eliminados), não é algo que caiba ao professor individualmente considerado.

Em conclusão, a corte austríaca decidiu: em última análise, tendo em conta todos os aspectos descritos, o responsável (seja como controlador ou, eventualmente, como operador) pelas ações relacionadas ao caso em análise, é a organização escolar e não o professor individualmente considerado.

4. Uma análise sistemática acerca dos agentes de tratamento na LGPD.

Embora as explicações acima evidenciem a visão europeia sobre o tema, o Brasil não tem obrigação jurídica de seguir a mesma interpretação. Mesmo considerando a expressiva influência do GDPR na criação da legislação nacional, inclusive na importação dos conceitos de controlador e operador criados por aquela tradição, – o que pode gerar um ônus argumentativo maior para justificar uma compreensão divergente dos conceitos internalizados – a soberania nacional possibilita que trilhemos outro caminho.

Diante disso, cabe analisar nossa própria lei e identificar se ela oferece guias sobre a adequada compreensão dos conceitos de controlador e operador. Neste artigo, dar-se-á especial atenção a algumas responsabilidades e deveres que a LGPD estabelece para os agentes de tratamento – ao longo das 62 e 13 vezes em que os termos controlado(es) e operador(es) são, respectivamente, citados – no intuito de avaliar se os exemplos do TJDFT e MP-RS são compatíveis com tais atribuições.

4.1. Controlador.

É ao controlador que LGPD – tal como no GDPR – atribui a maior parte dos deveres relacionados à proteção de dados pessoais,

bem como a maior possibilidade de responsabilização em caso de danos decorrentes do tratamento inadequado. E isso ocorre por uma questão lógica: é a ele que, nos termos da própria lei, compete "as decisões referentes ao tratamento de dados pessoais". Sendo certo que esse dever de *responsabilização e prestação de contas* (art. 6º, X) vale para pessoas físicas, jurídicas, públicas e privadas.[28]

Uma primeira problematização se refere a uma das hipóteses de tratamento (prevista tanto no artigo 7º, II quanto no 11, II, 'a'), qual seja, o "cumprimento de obrigação legal ou regulatória pelo controlador". Cabem algumas reflexões: (i) tais obrigações, ao menos em regra, são destinadas às pessoas jurídicas (seja de direito público ou de direito privado) ou a seus representantes legais? (ii) A identificação do controlador na figura do presidente/diretor/administrador (ao invés da própria PJ) impactaria na interpretação desse dispositivo? (iii) Quando dados são tratados para o cumprimento de atribuições legais da Administração Pública,[29] confundem-se as obrigações desta com as das pessoas físicas que as representam?

---

28 Excetuadas as hipóteses estabelecidas no art. 4º. Sobre o tema, há autores que defendem que a LGPD só incide, no caso de tratamentos realizados por pessoa natural, se houver finalidade econômica (KREMER, Bianca. Os agentes de tratamento de dados pessoais. In: MULHOLLAND, Caitlin (Org.) *A LGPD e o novo marco normativo no Brasil*. Porto Alegre: Arquipélago, 2020. p. 291). Respeitosamente discordamos, posto que a LGPD indica sua exclusão no caso de tratamentos "realizados por pessoa *natural* para fins *exclusivamente particulares E não econômicos*" (art. 4º, I, grifo nosso), i.e., a conjunção "E", reforçado pelo adverbio "exclusivamente", exigem ambas as características para excluir a aplicação da lei. Exemplo desse entendimento é a recente multa de 1.500 Euros aplicada pela autoridade espanhola à cidadão que equipou seu carro com equipamento de gravação de vídeo na parte traseira de seu veículo. Por estar direcionada para fora do automóvel, portanto, podendo obter imagens do espaço público, sem motivo justificado, a autoridade entendeu que a ação violava o GDPR. Ou seja, mesmo sem qualquer motivação econômica, o fato de a ação ser direcionada a espaço público implica na necessidade de cumprimento das previsões do regulamento europeu, dentre os quais os princípios da finalidade e da transparência, bem como da minimização dos dados pessoais. (AEPD. *Procedimiento* Nº: PS/00108/2020. Disponível em: «https://egida.es/wp-content/uploads/2020/10/ps-00108-2020.pdf». Acesso em: 20 out. 2020.)

29 No caso específico da Administração Pública, embora alguns autores indiquem que os tratamentos de dados pessoais relacionados à execução de competências legais ou ao cumprimento de atribuições legais do serviço público esteja embasado no artigo 23 da LGPD (MEN-

Questionamentos análogos podem ser feitos em relação à hipótese de "interesse legítimo do controlador". No primeiro caso, não parece adequado confundir os sujeitos a quem tais obrigações são direcionadas. No segundo caso, afigura-se mais grave ainda confundir as partes cujos interesses caracterizariam uma base legal que justifica o tratamento de dados pessoais sem a necessidade de consentimento, sob o argumento de que esses interesses já contemplariam as legítimas expectativas dos próprios titulares. Basta imaginar a elaboração de um *teste de legítimo interesse* – em um contexto organizacional – considerando finalidades legítimas e atividades do controlador que, em regra, pela interpretação dada pelo TJDFT, seria uma pessoa física da organização e não a própria instituição.

Outras questões são evidenciadas pelas atribuições operacionais que a LGPD determina aos controladores e que não parecem se compatibilizar com – ou terão muita dificuldade de serem efetivadas por – pessoas físicas que já possuem diversas outras atribuições institucionais. Dentre essas, apenas exemplificativamente, destacam-se: (i) atender aos direitos dos titulares (confirmação, acesso, correção, oposição, anonimização, bloqueio ou eliminação, portabilidade, informação sobre compartilhamento, revogação de consentimento) de forma imediata ou a justificativa de sua impossibilidade,[30] sendo que os titulares podem fazer tais solicitações a qualquer momento e, a princípio, sem limitações temporais ou quantitativas (arts. 9º, 18); (ii) realizar processo de gerenciamento de consentimento (com todos os cuidados acerca de sua manifestação livre, informada e inequívoca), com especial atenção, no caso de dados de crianças, à realização de todos os esforços razoáveis para verificar se houve consentimento

---

DES, Laura Schertel; DONEDA, Danilo, op. cit., p. 473), filiamo-nos àqueles que defendem se tratar de hipóteses relacionadas aos artigos supramencionados, posto que a atuação da Administração Pública decorreria de uma determinação legal (TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *civilistica.com*, v. 9, n. 1, p. 1-38, 9 mai. 2020).

30 Devendo, quando não for controlador no caso específico, sempre que possível, indicar o verdadeiro agente de tratamento.

efetivamente dado por um dos responsáveis, sendo que, independentemente do caso, cabe a ele o ônus da prova sobre tal obtenção (arts. 5º, XII; 7º, 11, 14, entre outros); (iii) informar de modo claro e adequado, sempre que solicitados, os critérios e procedimentos utilizados em decisões automatizadas (art. 20, § 1º); (iv) elaborar relatórios de impacto à proteção de dados pessoais (arts. 10, 3º; 32; 38); (v) verificar se todos os operadores estão realizando os tratamentos, realizados em seu nome, seguindo suas orientações e as normas aplicáveis sobre proteção de dados pessoais (art. 39); (vi) comunicar, em prazo razoável,[31] à ANPD e ao titular, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante, sendo que tal comunicação deverá conter, no mínimo: descrição da natureza dos dados afetados e informações sobre os riscos e os titulares envolvidos; indicação das medidas técnicas e de segurança utilizadas; riscos relacionados ao incidente; medidas adotadas para minimizar os danos e; se for o caso, razões da comunicação não ter sido efetuada imediatamente (art. 48); (vii) visando proteger efetivamente os dados pessoais, bem como minimizar eventuais sanções e multas,implementar programa de governança em privacidade (art.50, § 2º); dentre outros.

Como se pode verificar, a partir desse rol meramente exemplificativo, é muito difícil imaginar que todas essas atividades poderão ser compatibilizadas por uma pessoa natural (ou mesmo um grupo de pessoas) que ocupe posição de direção em uma entidade. Na verdade, a especificação dessas atividades parece ser direcionada – em um contexto organizacional – à própria instituição.

O texto da LGPD também parece distinguir claramente, em alguns momentos em que trata do controlador, pessoas jurídicas de pessoas naturais que nela atuam. É o caso do artigo 16, IV que, ao indicar a necessidade de exclusão dos dados após o término do trata-

31 Esse prazo deverá ser definido pela ANPD, mas, apenas como referência, o GDPR (art. 33 (1)) prevê que a autoridade seja comunicada sem atrasos injustificados, sempre que possível, em até 72 horas.

mento, autoriza sua conservação para "uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados".[32] Seria, no mínimo, inadequado que dados pessoais tratados por uma instituição, ao final do tratamento, pudessem ser mantidos para uso exclusivo de alguém que integra a entidade, mas não pela própria organização.

Outra situação que indica essa inconsistência, caracterizada pela confusão entre pessoa jurídica e pessoa física que a integra, pode ser vista no §7º do artigo 53: "os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo". Basta imaginar, nesses tempos em que os incidentes de segurança ocorrem a cada momento, que o diretor ou presidente de uma organização seja, não apenas o *responsável* por todas as tentativas de conciliação, mas também o indivíduo a ser *responsabilizado*, conforme as sanções do artigo 52, caso essas não alcancem bom termo.

Há ainda um argumento de autoridade (ainda que não seja da ANPD). O Comitê Central de Governança de Dados (CCGD)[33] do Go-

---

32 Reconhece-se, entretanto, a redação inadequada desse dispositivo considerando que a LGPD não incide sobre dados realmente anonimizados.

33 Instituído pelo Decreto 10.046, de 9 de outubro de 2019, o CCGD (composto por representantes do Ministério da Economia - um da Secretaria Especial de Desburocratização, Gestão e Governo Digital e um da Secretaria Especial da Receita Federal –; da Casa Civil da Presidência da República; da Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União; da Secretaria Especial de Modernização do Estado da Secretaria-Geral da residência da República; da Advocacia-Geral da União e do Instituto Nacional do Seguro Social) pode orientar o governo em questões relativas a políticas e diretrizes de governança de dados para a administração pública e tem competência para deliberar, entre outros assuntos, sobre: (i) as propostas para viabilizar, econômica e financeiramente, o Cadastro Base do Cidadão do setor público; (ii) orientações e diretrizes para a categorização de compartilhamento amplo, restrito específico, bem como a forma de publicação dessa categorização, observada a legislação referente à proteção de dados pessoais; (iii) regras e parâmetros para esse compartilhamento, incluídos os padrões relativos à preservação do sigilo e da segurança".

verno Federal criou o 'Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD)'. Esse documento afirma que "no âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei", sendo relevante, para sua distinção dos operadores, "que a identificação dos Controladores depende necessariamente, em cada situação, da existência da capacidade de decidir sobre os meios e a finalidade do tratamento de dados".[34]

4.2. Operador.

Embora o peso da responsabilização e prestação de contas previsto pela LGPD para o operador seja um pouco menor quando comparado ao controlador, isso não significa que não seja substancial. Algumas das obrigações mais expressivas, compartilhadas com o controlador são: (i) observação (e respectiva comprovação desta) dos princípios gerais do artigo 6º; (ii) elaboração e manutenção de registro das operações de tratamento de dados pessoais (art. 37); (iii) adoção de medidas de segurança, técnicas e administrativas, planejadas desde a concepção do produto/serviço, capazes de proteger os dados pessoais de qualquer forma de tratamento inadequado ou ilícito (art. 46).

Além disso, o artigo 50 possibilita que os agentes de tratamento – individualmente ou por meio de associações e desde que considerem a natureza, o escopo, a finalidade, a probabilidade e a gravi-

---

34 BRASIL. Comitê Central de Governança de Dados. *Guia de Boas Práticas* - Lei Geral de Proteção de Dados (LGPD), agosto de 2020, p. 10. Disponível em: «https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf». Acesso em: 07 set. 2020. Todavia, é importante reconhecer que o mesmo documento apresenta algumas informações questionáveis (o que é compreensível considerando a novidade do tema), dentre as quais a definição de *Operador* (ponto que será tratado na próxima seção) na qual indica que este é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII), *aí incluídos agentes públicos no sentido amplo que exerçam tal função*, bem como pessoas jurídicas diversas daquela representada pelo Controlador", sendo certo que o presente artigo defende que a parte destacada está equivocada.

dade dos riscos e dos benefícios decorrentes de tratamento de dados pessoais – formular regras de boas práticas e de governança que:

> estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Com todo respeito aos posicionamentos divergentes, é claro que tais obrigações – quando se pensa em uma estrutura organizacional, com o volume e complexidade de tratamento de dados que estas podem demandar – não são passíveis de serem realizadas adequadamente pelos indivíduos que integram a instituição, mas, antes, demandam o comprometimento de toda a organização, de forma sistemática e coesa. Basta imaginar cada funcionário (ou estagiário) de uma grande instituição (pública ou privada) formulando suas regras de boas práticas e de governança específicas, obviamente só depois de fazer, também individualmente, uma análise de riscos de todos os dados pessoais que trata. Ou, ainda, tendo que demonstrar que as medidas de segurança, adotadas por ele, são eficazes.

Por derradeiro, mas não menos relevante, há que se analisar as consequências, em termos de responsabilidade civil e de sanções, da indicação de funcionários e afins como operadores. O artigo 42 afirma que, não apenas operadores, mas também controladores, deverão reparar os danos decorrentes do tratamento de dados pessoais, sendo que o operador responderá solidariamente quando descumprir as obrigações da lei (lembrando que, conforme art. 44, basta que o tratamento não forneça "a segurança que o titular dele pode esperar" para ser caracterizado como irregular) ou não tiver seguido as instruções lícitas do controlador, havendo inclusive a possibilidade de inversão do ônus da prova.

Com base nesses dispositivos e tendo em mente os exemplos iniciais do TJDFT e MP-RS, questiona-se: pode a vítima do dano ingressar com uma ação judicial diretamente contra o funcionário, servidor ou estagiário (ou contra o presidente do tribunal ou empresa) sem obrigatoriedade de indicar a instituição, que tratava efetivamente seus dados, no polo passivo? Responderão judicialmente estes diretamente às vítimas (inclusive em ações coletivas), com seu próprio patrimônio? Em caso de dano decorrente de tratamento feito pela Administração Pública (ou em relação de consumo), a responsabilidade de "controladores" (presidente, vice-presidente, ouvidor ou outros indicados pela instituição pública ou privada) e "operadores" (membros, servidores e estagiários ou quaisquer outros integrantes indicados) será objetiva?

5. Boas Práticas e Padrões.

A LGPD seria prolixa – não fosse a relevância do tema – no que concerne a ressaltar a necessidade da utilização de padrões e de "boas práticas" no tratamento de dados pessoais. Tais indicações ocorrem expressamente nos artigos 12, 13, 32, 33, 35, 40, 46, 49, 50, 51 (sendo que esses dois últimos artigos integram uma seção denominada "Das Boas Práticas e da Governança") e 55-J.

Existem diversas instituições internacionalmente reconhecidas que podem servir como referência nessa área. Neste artigo, analisaremos algumas normas criadas pela *International Organization for Standardization*, as chamadas ISOs. A escolha se deve à longa história da organização, que atua desde 1946, bem como à sua representatividade que conta com a participação de instituições de 165 países diferentes (no Brasil, é representada pela Associação Brasileira de Normas Técnicas-ABNT, criada em 1940).

Relevante indicar que normas dessa entidade foram recomendadas pelo próprio Governo Federal do Brasil por meio do 'Guia de

Boas Práticas: Lei Geral de Proteção de Dados (LGPD)' – já mencionado acima – em que afirma, na página 49:

> Recomenda-se a utilização de algum framework, boa prática ou norma técnica aplicável como a ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls e ISO/IEC 29134 - Guidelines for privacy impact assessment.

A NBR ISO/IEC 29151 (elaborada pela Comissão de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade da ABNT para ser "uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 29151:2017" e aprovada em novembro de 2020) indica, em seu item 1, que ela se aplica às "organizações que atuam como controladores de DP", sendo tal conceito "estabelecido na ABNT NBR ISO/IEC 29100". Esta última traz conceito de controlador cuja ideia é muito similar à LGPD[35] e, também, no item 2.25, o conceito de "*terceiro*", nos mesmos moldes adotados pelo GDPR:

> parte interessada na privacidade que *não* o *titular* de dados pessoais (DP), o *controlador* de DP

35 O item 2.8 indica "parte(s) interessada(s) na privacidade que *determina(m) os objetivos e os meios* para o tratamento dos dados pessoais (DP) e que não é(são) pessoa(s) natural(is) que usa(m) os dados para objetivos pessoais" (grifo nosso).

> e o *operador* de DP, e as *pessoas naturais* que são autorizadas a tratar os dados *sob direta autoridade* do controlador de DP ou do operador de DP. (grifo nosso)

Portanto, reitera-se aqui a diferenciação entre controladores, operadores e pessoas naturais que atuam diretamente subordinadas a qualquer um desses, conforme já indicado na seção 3.

Além disso, as ISOs também indicam procedimentos que devem ser adotados por controladores e por operadores visando colaborar para a construção tanto de uma estrutura adequada de privacidade quanto de uma prática eficiente de proteção de dados pessoais.

Apenas exemplificativamente, a NBR ISO/IEC 27701 – que é uma extensão (portanto, deve ser aplicada conjuntamente) da NBR ISO/IEC 27001 e da NBR ISO/IEC 27002 para gestão da privacidade da informação – indica controles de privacidade[36] *específicos e diferenciados para controladores* e *operadores*. Como se poderá perceber, são medidas a serem adotadas, em sua totalidade, tipicamente por uma organização e não por pessoa(s) natural(is) que fazem parte da instituição.

5.1. Controles de privacidade específicos para controladores (ISO 27701).

A norma em comento sugere, em seu Anexo A, 31 (trinta e um) controles de privacidade[37] *que devem ser implementados especificamente por aqueles que atuam como controladores* dos tratamentos de dados pessoais.

---

36 Conforme definido no item 2.12 da NBR ISO/IEC 29100, são "medidas que tratam os riscos de privacidade por meio da redução de sua probabilidade ou de suas consequências".

37 Conforme definido no item 2.12 da NBR ISO/IEC 29100, são "medidas que tratam os riscos de privacidade por meio da redução de sua probabilidade ou de suas consequências".

Oito desses controles se referem as condições para a coleta e demais formas de tratamento de dados pessoais e tem como objetivo expresso determinar ações no intuito de garantir e evidenciar que o tratamento é lícito e que os propósitos são legítimos e claramente estabelecidos:

a) A.7.2.1 - A organização deve identificar e documentar os propósitos específicos pelos quais os dados pessoais serão tratados.

b) A.7.2.2 - A organização deve determinar, documentar e estar em *compliance* com a base legal pertinente para o tratamento de dados pessoais para os propósitos identificados.

c) A.7.2.3 - A organização deve determinar e documentar um processo pelo qual ela possa demonstrar se, quando e como o consentimento para o tratamento de dados pessoais foi obtido dos titulares.

d) A.7.2.4 - A organização deve obter e registrar o consentimento dos titulares de acordo com os processos documentados.

e) A.7.2.5 - A organização deve avaliar a necessidade para, e implementar onde apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de dados pessoais ou mudanças ao tratamento existente forem planejados.

f) A.7.2.6 - A organização deve ter um contrato por escrito com qualquer operador de dados pessoais que ela utilize, e deve assegurar que os seus contratos com os operadores contemplem a implementação de controles apropriados, conforme descrito no Anexo B da ISO 27701.

g) A.7.2.7 - A organização deve determinar as responsabilidades e respectivos papéis para o tratamento de dados pes-

soais (incluindo a proteção e os requisitos de segurança) com qualquer controlador conjunto.

h) A.7.2.8 - A organização deve determinar e manter de forma segura os registros necessários ao suporte às suas obrigações para o tratamento dos dados pessoais.

O maior conjunto de controles demonstra a preocupação da norma com o cumprimento das obrigações para com os titulares, mormente no que concerne as informações que devem ser fornecidas a eles e aos procedimentos adotados institucionalmente para garantir sua efetivação:

a) A.7.3.1 - A organização deve determinar e documentar suas obrigações regulatórias, legais e de negócios para os titulares, relativas ao tratamento de seus dados pessoais e fornecer meios para atender a estas obrigações.

b) A.7.3.2 - A organização deve determinar e documentar a informação a ser fornecida aos titulares, relativa ao tratamento de seus dados pessoais, e o tempo de tal disponibilização.

c) A.7.3.3 - A organização deve fornecer aos titulares, de forma clara e facilmente acessível, informações que identifiquem o controlador e descrevam o tratamento de seus dados pessoais.

d) A.7.3.4 - A organização deve fornecer mecanismos para os titulares para modificar ou cancelar os seus consentimentos.

e) A.7.3.5 - A organização deve fornecer mecanismos para os titulares para negar o consentimento ao tratamento de seus dados pessoais.

f) A.7.3.6 - A organização deve implementar políticas, procedimentos e/ou mecanismos para atender às suas obrigações para os titulares acessarem, corrigirem e/ou excluírem os seus dados pessoais.

g) A.7.3.7 - A organização deve informar aos terceiros com quem o dado pessoal foi compartilhado sobre qualquer modificação, cancelamento ou desaprovação pertinente, e implementar políticas e procedimentos apropriados e/ou mecanismos para fazê-lo.

h) A.7.3.8 - A organização deve ser capaz de fornecer uma cópia do dado pessoal que é tratado, quando requerido pelo titular.

i) A.7.3.9 - A organização deve definir e documentar políticas e procedimentos para tratamento e respostas, a solicitações legítimas dos titulares.

j) A.7.3.10 - A organização deve identificar e considerar as obrigações, incluindo obrigações legais, para os titulares, como resultado das decisões feitas pela organização que estejam relacionadas ao titular, baseadas unicamente no tratamento automatizado de dados pessoais.

Há também um grupo de controles com especial direcionamento às ideias de *privacy by design* e *privacy by default*, visando assegurar que processos e sistemas sejam projetados de modo a limitar os tratamentos de dados pessoais ao mínimo necessário ao propósito identificado:

a) A.7.4.1 - A organização deve limitar a coleta de dados pessoais a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.

b) A.7.4.2 - A organização deve limitar o tratamento de dados pessoais de tal forma que seja adequado, relevante e necessário para os propósitos identificados.

c) A.7.4.3 - A organização deve assegurar e documentar que o dado pessoal é preciso, completo e atualizado, como é necessário para os propósitos aos quais ele é tratado, por meio do ciclo de vida do dado pessoal.

d) A.7.4.4 - A organização deve definir e documentar os objetivos da minimização dos dados e quais mecanismos (como a anonimização) são usados para atender àqueles objetivos.

e) A.7.4.5 - A organização deve excluir dados pessoais ou entregá-los na forma que não permita a identificação ou reidentificação dos titulares, uma vez que o dado pessoal original não é mais necessário para os propósitos identificados.

f) A.7.4.6 - A organização deve assegurar que os arquivos temporários criados como um resultado de tratamento de dados pessoais sejam descartados (por exemplo, apagados ou destruídos) seguindo procedimentos documentados dentro de um período documentado, especificado.

g) A.7.4.7 - A organização não pode reter o dado pessoal por um tempo maior do que é necessário para os propósitos para os quais o tratamento é realizado.

h) A.7.4.8 - A organização deve ter políticas, procedimentos e/ou mecanismos documentados para o descarte de dados pessoais.

i) A.7.4.9 - A organização deve tratar dado pessoal transmitido (por exemplo, enviado para outra organização) que trafe-

gue por uma rede de transmissão de dados, com controles apropriados concebidos para assegurar que os dados alcancem seus destinos pretendidos.

Com o intuito de identificar se – e documentar quando – os dados pessoais são compartilhados ou transferidos para outras jurisdições ou com terceiros de forma a garantir as obrigações aplicáveis:

a) A.7.5.1 - A organização deve identificar e documentar as bases relevantes para a transferência de dados pessoais entre jurisdições.

b) A.7.5.2 - A organização deve especificar e documentar os países e as organizações internacionais para os quais os dados pessoais possam possivelmente ser transferidos.

c) A.7.5.3 - A organização deve registrar a transferência de dados pessoais para ou de terceiros e assegurar a cooperação com essas partes para apoiar futuras solicitações relativas às obrigações para os titulares.

d) A.7.5.4 - A organização deve registrar a divulgação de dados pessoais para terceiros, incluindo quais foram divulgados, para quem e quando.

Tais medidas devem ser implementadas ou, ao menos, sua exclusão deve adequadamente justificada de modo a explicar por que alguns controles não são considerados necessários, por exemplo, de acordo com a avaliação de riscos feita pela organização ou porque desnecessário de acordo com a legislação e/ou regulamentação incidente, sempre levando em consideração os contextos específicos da organização. Sendo assim, é perceptível que a adoção desses controles ou mesmo a avaliação e posterior justificativa de sua não implementação demandam um esforço institucional (portanto, do controla-

dor a quem a norma se aplica) que não pode ser corretamente atendido pelo representante institucional.

5.2. Controles de privacidade específicos para operadores (ISO 27701).

A ISO 27701, em seu Anexo B, indica ainda 18 (dezoito) controles de privacidade específicos para aqueles que atuam como operadores nos tratamentos de dados pessoais. Tais controles também são divididos em quatro grupos que, de forma geral, seguem modelo similar ao já comentado para os controladores:

a) B.8.2.1 - A organização deve assegurar, onde pertinente, que o contrato para tratar dados pessoais considera os papéis da organização em fornecer assistência com as obrigações do cliente (considerando a natureza do tratamento e a informação disponível para a organização).

b) B.8.2.2 - A organização deve assegurar que os dados pessoais, tratados em nome do cliente, o sejam apenas para o propósito expresso nas instruções documentadas do cliente.

c) B.8.2.3 - A organização não pode utilizar os dados pessoais tratados sob um contrato para o propósito de marketing e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular. A organização não pode fornecer esse consentimento como uma condição para o recebimento do serviço.

d) B.8.2.4 - A organização deve informar ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.

e) B.8.2.5 - A organização deve fornecer ao cliente informações apropriadas de tal modo que o cliente possa demonstrar *compliance* com suas obrigações.

f) B.8.2.6 - A organização deve determinar e manter os registros necessários para apoiar a demonstração do *compliance* com suas obrigações (como especificado no contrato aplicável) para tratamento de dados pessoais realizado em nome do cliente.

g) B.8.3.1 - A organização deve fornecer ao cliente meios para estar em *compliance* com suas obrigações relativas aos titulares.

h) B.8.4.1 - A organização deve assegurar que os arquivos temporários criados como um resultado do tratamento de dados pessoais sejam descartados (por exemplo, apagados ou destruídos) seguindo os procedimentos documentados, dentro de um período especificado e documentado.

i) B.8.4.2 - A organização deve fornecer a capacidade de retornar, transferir e/ou descartar dados pessoais de uma maneira segura. Deve também tornar sua política disponível para o cliente.

j) B.8.4.3 - A organização deve sujeitar dados pessoais transmitidos sobre uma rede de transmissão de dados a controles apropriados projetados, para assegurar que os dados alcancem seus destinos pretendidos.

k) B.8.5.1 - A organização deve informar ao cliente em um tempo hábil sobre as bases para a transferência de dados pessoais entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.

l) B.8.5.2 - A organização deve especificar e documentar os países e as organizações internacionais para os quais dados pessoais possam ser transferidos.

m) B.8.5.3 - A organização deve registrar a divulgação de dados pessoais para terceiros, incluindo quais foram divulgados, para quem e quando.

n) B.8.5.4 - A organização deve notificar ao cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de dados pessoais.

o) B.8.5.5 - A organização deve rejeitar quaisquer solicitações para a divulgação de dados pessoais que não sejam legalmente obrigatórias, consultar o cliente em questão antes de realizar quaisquer divulgações e aceitar quaisquer solicitações contratualmente acordadas para a divulgação, que sejam autorizadas pelo respectivo cliente.

p) B.8.5.6 - A organização deve divulgar para o cliente qualquer uso de subcontratados para tratar dados pessoais, antes do uso.

q) B.8.5.7 - A organização deve somente contratar um subcontratado para tratar dados pessoais com base no contrato do cliente.

r) B.8.5.8 - A organização deve, no caso de ter uma autorização geral por escrito, informar o cliente de quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados no tratamento de dados pessoais, dando assim ao cliente a oportunidade de se opor a essas alterações.

No que concerne aos controles específicos para os operadores fica ainda mais claro o equívoco de se confundir esse agente de tra-

tamento com os colaboradores/servidores/estagiários e correlatos que atuam em uma organização. Obviamente, a maioria expressiva de tais medidas são impossíveis de serem adotadas por essas pessoas físicas, seja por empecilhos técnicos, jurídicos, econômicos, operacionais ou até pela extrema dificuldade em negar determinadas ordens que provém de um superior hierárquico.

Basta pensar, apenas exemplificativamente, sobre a (im)possibilidade de um funcionário contratar um "subcontratado" para repassar parte de suas atribuições, ainda mais se tal contratação depender de um contrato (inexistente) com seu superior hierárquico ou mesmo com a instituição na qual atua. Ou, ainda, sobre a (im)possibilidade de qualquer 'colaborador' fornecer a capacidade de retornar, transferir e/ou descartar dados pessoais de uma maneira segura, tornando sua política disponível para seu empregador.

6. As recentes manifestações da ANPD.

Todos os argumentos acima delineados foram escritos diante da, até então, completa ausência de manifestação oficial da ANPD sobre o tema. Todavia, recentemente, a Autoridade produziu seu primeiro documento oficial, sendo o tópico inicial deste exatamente sobre a temática aqui abordada – o que ressalta a relevância do tema.[38]

---

38 ANPD. *Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Disponível em: «https://www.gov.br/anpd/pt-br/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf». Acesso em: 29 mai. 2021. O documento foi divulgado em 28 de maio de 2021, sendo certo que a notícia destaca que "a atual versão é a primeira edição do guia, que está sujeita a comentários e contribuições pela sociedade civil. As contribuições podem ser enviadas para o e-mail normatizacao@anpd.gov.br. O recebimento de sugestões de aprimoramento do guia é contínuo e o presente guia será atualizado à medida que novas regulamentações e entendimentos forem publicados e estabelecidos pela ANPD" «https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-orientativo-sobre-agentes-de-tratamento-e-encarregado». Portanto, defende-se que, mesmo diante do posicionamento do órgão, o presente trabalho continua sendo relevante para consolidar as opiniões emitidas pela ANPD.

Resumidamente, o documento reforça as conclusões aqui apresentadas, asseverando que "os agentes de tratamento devem ser definidos a partir de seu caráter institucional", sendo assim, não devem ser "considerados controladores [...] ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento".[39]

Obviamente, como já indicado, pessoas físicas podem ser consideradas *controladores* quando "atuarem de acordo com os próprios interesses, com poder de decisão sobre as finalidades e os elementos essenciais de tratamento", isto é, quando agirem de forma independente e em nome próprio – não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta – é o que ocorre com empresários individuais, profissionais liberais ou responsáveis pelas serventias extrajudiciais.[40]

Também podem ser consideradas *operadores* quando "atuarem de acordo com os interesses do controlador, sendo-lhes facultada apenas a definição de elementos não essenciais à finalidade do tratamento".[41] Isso pode ocorrer, por exemplo, quando uma pessoa natural é contratada como prestadora de serviços para uma finalidade específica. Todavia, tal situação é distinta da atuação de funcionários que simplesmente representam uma pessoa jurídica:

> empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como

39 Ibidem, p. 5.

40 Ibidem, p. 10.

41 Ibidem, p. 5.

> profissional subordinado a este ou como membro de seus órgãos.[42]

Portanto, em regra, no "contexto de uma pessoa jurídica, a organização é o agente de tratamento para os fins da LGPD, já que é esta que estabelece as regras para o tratamento de dados pessoais, a serem executadas por seus representantes ou prepostos".[43] Sendo certo que os conceitos de controlador e operador não devem ser entendidos como norma de distribuição interna de competências e responsabilidades.[44]

Considerações finais.

Não obstante seja importante reconhecer esforço das instituições públicas e privadas em seus primeiros passos em direção à conformidade com a proteção de dados pessoais – mormente diante de novas figuras jurídicas, princípios e práticas desconhecidas da grande maioria, somadas a, até então, ausência de orientações da ANPD, que ainda estava sendo efetivamente estruturada – buscou-se demonstrara inadequação de algumas interpretações que estavam sendo dadas aos conceitos de controlador e operador especificados na Lei Geral de Proteção de Dados Pessoais (LGPD).

Considerando-se a origem desses conceitos, relacionada a tradição europeia de proteção de dados ou mesmo por meio de uma compreensão sistemática da LGPD – em especial no que concerne aos papéis, obrigações e responsabilidades direcionados aos agentes de tratamento – não é adequado, em contextos organizacionais, confundir a pessoa jurídica (tanto de direito público como de direito privado) com as pessoas naturais que integram seus quadros.

---

42 Ibidem, p. 17.

43 Ibidem, p. 6.

44 Ibidem, p. 8.

Buscou-se argumentar que o objetivo central da definição das novas figuras jurídicas de controlador e operador está intimamente relacionado com o princípio da responsabilização e prestação de contas. O estabelecimento desses novos papeis tem o intuito, primeiramente, de garantir o pleno efeito da legislação de proteção de dados, fomentando a garantia efetiva e abrangente dessas informações, evitando ou, pelo menos, minimizando, os danos que podem advir do tratamento. Isso é ainda mais necessário ao se pensar – como já ocorre na União Europeia e, aparentemente, delineia-se entendimento similar no Brasil – a proteção de dados pessoais como inclusa no rol de direitos e garantias fundamentais.

Ademais, para além dessa tentativa de garantir tal proteção (e assegurar a responsabilidade pelo ressarcimento de eventuais danos), a adequada compreensão dos conceitos de controlador e operador está diretamente relacionada à qualidade da estrutura geral de governança das organizações – sejam elas públicas ou privadas –, inclusive aumentando a segurança jurídica ao identificar claramente os papéis, deveres e responsabilidades de cada agente de tratamento.

Sendo assim, o princípio da responsabilização e da prestação de contas, por si só, já indica que – em contextos organizacionais – é a própria instituição que deve atuar e ser reconhecida, seja como controlador seja como operador. Isso não significa, obviamente, que os integrantes das instituições não serão responsabilizados por eventuais condutas inadequadas – não faltam exemplos de previsões legais para garantir essa última possibilidade, seja na Constituição (art. 37, §6º), no Código Civil (art. 934), na Lei de Acesso à Informação (art. 31, § 2º e 32, II), na Lei 8.112/90 (art. 122) e na própria LGPD (art. 47), dentre outros.

Portanto, a adequada compreensão dos conceitos relacionados à proteção de dados – dentre eles o de controlador e operador – mormente diante da falta de vivência nacional com as especificidades do tema, não pode ser feita com os olhos voltados apenas para o texto da LGPD, nem mesmo centrada exclusivamente na experiência

brasileira. Sem olvidar nossa soberania e a liberdade na construção de nosso próprio caminho, a análise cuidadosa das experiências internacionais, mormente de sociedades que têm maior experiência com esse tema – dentre as quais a europeia – é fundamental para tais reflexões e para a construção de uma verdadeira cultura de proteção de dados pessoais que todos desejamos no Brasil.