

— ANÁLISE COMPARADA — LGPD E GDPR

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

FELIPE ROCHA DA SILVA

TAYNÁ FROTA DE ARAÚJO

ISABELA MARIA ROSAL

PAULO RICARDO SANTANA

EDUARDA COSTA

ELIS BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA
UNIVERSIDADE DE BRASÍLIA

VOLUME 1

Universidade de Brasília
Faculdade de Direito

**Anuário do Observatório da LGPD da
Universidade de Brasília**
Análise comparada entre elementos da LGPD e do
GDPR

Volume 1
Brasília-DF
2023



Anuário do Observatório da LGPD da Universidade de Brasília: Análise comparada entre elementos da LGPD e do GDPR © 2023 by Observatório da LGPD/Unb is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Anuário do Observatório da LGPD da Universidade de Brasília: Análise comparada entre elementos da LGPD e do GDPR.

A responsabilidade pelos direitos autorais de textos e imagens desta obra é do Observatório da LGPD/Unb.

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 1

Organização

Coordenação Geral: prof.^a Laura Schertel Mendes;

Coordenação Adjunta: Giovanna Milanese;

Coordenação de Pesquisa: Felipe Rocha e Tayná Frota de Araújo;

Revisão e Organização: Eduarda Costa Almeida, Elis Bandeira A. Brayner, Isabela Maria Rosal e Paulo Ricardo da Silva Santana.

Informações

Observatório da LGPD/Unb

Faculdade de Direito

Universidade de Brasília

Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília - BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes ... [et al.]. - Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

Ana Júlia Prezotti Duarte

Andressa Carvalho Pereira

Angélica Opata Vettorazzi

Gabriel de Araújo Oliveira

Gabriel Cabral Furtado

Eduarda Costa Almeida

Fernanda Passos Oppermann Ilzuka

Isabela de Araújo Santos

Júlia Carvalho Soub

Shana Schlottfeldt

Sofia de Medeiros Vergara

Paulo Ricardo da Silva Santana

Rafael Luís Müller Santos

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Ana Luísa Vogado de Oliveira

Angelo Prata de Carvalho

Davi Ory

Gabriel Fonseca

Isabela Maria Rosal Santos

Maria Cristine Lindoso

Matheus Vinicius Aguiar

Paula Baqueiro

Tainá Aguiar Junquilha

Thiago Guimarães Moraes

SUMÁRIO

APRESENTAÇÃO.....	6
<i>Felipe Rocha, Giovanna Milanese e Tayná Frota de Araújo</i>	
OS LIMITES DO EXERCÍCIO DO PRINCÍPIO DA FINALIDADE NA LGPD E NO RGPD	8
<i>Gabriel de Araújo Oliveira</i>	
O PRINCÍPIO DA NECESSIDADE NO ÂMBITO DA LGPD E DOA RGPD: TEORIA E PRÁTICA	23
<i>Gabriel Cabral Furtado</i>	
ANONIMIZAÇÃO DE DADOS PESSOAIS: UM ESTUDO À LUZ DA LGPD E DO RGPD	38
<i>Ana Júlia Prezotti Duarte</i>	
ANÁLISE COMPARATIVA ENTRE O ESCOPO MATERIAL DA LGPD E DO RGPD ...	56
<i>Eduarda Costa Almeida</i>	
O CONSENTIMENTO VÁLIDO NA INTERPRETAÇÃO DO RGPD E DA LGPD: UMA ANÁLISE ENTRE AS SIMILITUDES E DISPARIDADES ENTRE AMBAS AS LEGISLAÇÕES	73
<i>Isabela de Araújo Santos</i>	
USO DE DADOS POR ÓRGÃOS DE PESQUISA: UMA ÓTICA COMPARATIVA ENTRE A LGPD E O RGPD	89
<i>Fernanda Passos Oppermann Ilzuka</i>	
O LEGÍTIMO INTERESSE SOB AS LENTES BRASILEIRA E EUROPEIA	100
<i>Angélica Opata Vettorazzi</i>	
REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING	114
<i>Shana Schlottfeldt</i>	
OBRIGAÇÕES DOS AGENTES DE TRATAMENTO DE DADOS: INTERFACES ENTRE A REGULAÇÃO BRASILEIRA E EUROPEIA	137
<i>Sofia de Medeiros Vergara</i>	
SEGURANÇA DA INFORMAÇÃO NO TRATAMENTO DE DADOS PESSOAIS	155
<i>Paulo Ricardo da Silva Santana</i>	
ENCARREGADO DE PROTEÇÃO DE DADOS & DATA PROTECTION OFFICER (DPO): UM ESTUDO À LUZ DAS (PRÉ) CONCEPÇÕES BRASILEIRAS E CONCEPÇÕES EUROPEIAS	169

Rafael Luís Müller Santos

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS COMO INSTRUMENTO ÚTIL DE ADEQUAÇÃO E GOVERNANÇA CONFORME A LGPD E O RGPD..... 185

Wanessa Larissa Silva de Araújo

LIMITES AO COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE OS ENTES DO PODER PÚBLICO 204

Júlia Carvalho Soub

A PROTEÇÃO DE DADOS NO BRASIL E NA UNIÃO EUROPEIA: PERSPECTIVA COMPARADA ENTRE A INDEPENDÊNCIA E AUTONOMIA DAS AUTORIDADES DE FISCALIZAÇÃO 221

Andressa Carvalho Pereira

O PRINCÍPIO DA NECESSIDADE NO ÂMBITO DA LGPD E DOA RGPD: TEORIA E PRÁTICA

Gabriel Cabral Furtado¹

Dispositivos da LGPD	Dispositivos do RGPD
<p>Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:</p> <p>III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;</p>	<p>Art. 5 - Princípios relativos ao tratamento de dados pessoais</p> <p>1. Os dados pessoais são:</p> <p>c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (‘minimização dos dados’).</p>

Introdução

É inegável a relevância dos princípios jurídicos para a interpretação e para a aplicação do direito. São os princípios, nas importantes palavras de Humberto Ávila (2019), espécie de normas jurídicas de caráter finalístico que prescrevem conteúdos relacionados à conduta humana. Desse modo, atuam fundamentalmente no estabelecimento das principais balizas para a aplicação das demais normas, cuja interpretação é concretizada a cada caso.

No âmbito da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que foi elaborada tendo por base o imprescindível equilíbrio entre a crescente necessidade de proteção dos titulares de dados pessoais e o desenvolvimento econômico-inovador, os princípios estão descritos em seu artigo 6º e possuem incidência horizontal a todos os seus dispositivos. Por seu turno, na esfera do Regulamento Geral sobre a Proteção de Dados (RGPD), que objetiva sobretudo reforçar e unificar a proteção de dados pessoais na União Europeia, os princípios norteadores constam no artigo 5º.

Nesse contexto, o presente artigo se propõe a analisar, sob os vértices teórico e prático, o princípio da necessidade ou minimização (*data minimisation*), expressamente previsto no inciso III do art. 6º da normativa brasileira e na alínea “c” do item 1 do art. 5º da normativa

¹ Bacharel em Direito na Universidade de Brasília (UnB). Integrante do grupo de pesquisa Observatório da LGPD.

européia. Buscar-se-á, nesse caminho, (i) tecer comentários doutrinários acerca do princípio supramencionado, abrangendo-se a jurisdição nacional e a europeia; e, posteriormente, (ii) examinar um caso nacional – a Ação Direta de Inconstitucionalidade n° 6.387 – e outro estrangeiro – “TK” vs. *Associação dos condôminos do edifício M5A* –, a fim de compreender como o princípio da necessidade vem sendo aplicado na prática jurídica em âmbito territorial e internacional.

1. Comentários

Os princípios da LGPD constituem verdadeira condição de legitimidade para o tratamento de dados, de modo a refletir a essência do diploma e propriamente justificar a coleta, o compartilhamento e o processamento de dados. Servem, nesse caminho, como barreira legal de modulação à conduta do agente de tratamento de dados, inserido em um modelo *ex ante* de proteção.

De modo mais atido ao escopo deste artigo, o princípio da necessidade, alçado no parágrafo III do artigo 6° da LGPD, consiste em uma limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Portanto, o intento é de justamente tratar o mínimo possível de dados, em uma concepção que objetiva, sobretudo, controlar e eventualmente bloquear o uso incondicional de dados pessoais.

Nessa esteira, é notório que o princípio da necessidade manifestamente se conecta a outros princípios. Primeiramente, cumpre pontuar que ele limita o princípio da eficiência², vez que coletar mais dados que o estritamente necessário é um obstáculo à obtenção de resultados rápidos e precisos buscados pela Administração Pública, de sorte a gerar prejuízo ao titular dos dados e aos demais afetados. Além disso, está ligado ao princípio da finalidade³, haja vista que a sua coleta só pode ocorrer tendo em conta, rigorosamente, a finalidade por ela pretendida, rejeitando a captação excessiva.

² Alçado no art. 37 da Constituição Federal de 1988, cuida-se de um dos princípios constitucionais regentes do Direito Administrativo, segundo o qual a administração pública deve, na atuação de suas atividades, racionalizar os meios para atingir os fins. *In verbis*: Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e **eficiência** e, também, ao seguinte (...). (grifos nossos).

³ Previsto no art. 6°, I da LGPD. Veja: Art. 6°. (...): I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Ademais de expressamente previsto no artigo 6º, III da LGPD, releva pontuar que o princípio da necessidade está também contemplado no artigo 18, IV do mesmo diploma, que evidencia o direito do titular em requisitar a “anonimização, bloqueio ou eliminação de **dados desnecessários, excessivos ou tratados em desconformidade**”. Sob outro vértice, o mesmo princípio baliza uma das formas de tratamento de dados sensíveis que dispensa o consentimento do titular, qual seja o compartilhamento de dados necessários à execução de políticas públicas, consoante previsto na alínea b do inciso II do art. 11, *in verbis*:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

No assunto, a doutrina propõe relevante divisão na compreensão do princípio da necessidade. Nesse rumo, diz-se que a minimização se divide em sentido estrito – o qual diz respeito ao tratamento da menor quantidade de dados possível para uma finalidade específica –, e sentido *lato* – que se relaciona à articulação de medidas de salvaguardas⁴ que ambicionam mitigar os riscos para os direitos fundamentais dos titulares. Nesse sentido, há um dever de cuidado duplo, que provoca dois juízos diferentes: um em torno da menor intrusividade do tratamento de dados, outro acerca da menor lesividade (BIONI; RIELLI; KITYAMA, 2021).

A vertente da menor intrusividade, em palavras gerais, envolve a verificação de outros tipos de dados menos intrusivos, disponíveis ao controlador, os quais poderiam ser eventualmente utilizados para atingir as mesmas finalidades pretendidas. Sobre o assunto, o *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation* (2017) acuradamente ressalta que o adjetivo “necessário” não é sinônimo de “indispensável”, mas também não se traduz na ideia de “útil”, “razoável” ou “desejável”.

⁴ No âmbito da legislação europeia de tratamento de dados, releva mencionar o disposto no Artigo 89, nº1 do RGPD, segundo o qual os controladores e processadores devem implementar medidas técnicas – a saber, garantir a proteção do acesso mediante senha; e da transferência de dados, mediante criptografia – e organizacionais – como o registro de atividades, o treinamento do pessoal, etc. – apropriadas para proteger os direitos e a liberdade dos titulares de dados cujos dados pessoais são coletados e processados para fins de arquivo de interesse público, de investigação científica ou histórica, ou, ainda, estatísticos.

Assim, de forma relacionada à aplicação do legítimo interesse, o modo mais simples de se identificar a necessidade é questionar se existe outra forma de atingir o interesse pretendido, com menor ofensividade sobre os dados pessoais. Se não há ou se há outra forma que, todavia, exija um esforço desproporcional, então pode-se dizer que o processo é necessário. Doutro lado, se houver várias maneiras de atingir o objetivo, é recomendável a realização de um Relatório de Impacto à Proteção de Dados (RIPD)⁵ com o propósito de identificar a conduta menos invasiva.

A vertente do possível impacto do tratamento de dados sobre os direitos e liberdades fundamentais dos titulares, sob outro vértice, presta-se a analisar o potencial lesivo do tratamento, para o qual devem ser ajuntadas medidas mitigatórias de riscos, a saber a anonimização e a pseudonimização.⁶ Nesse caminho, Bioni, Rielli e Kityama (2021) lecionam que:

Essa faceta da minimização é extraída do próprio art. 10, inciso II, na medida em que ele condiciona a fundamentação do tratamento no legítimo interesse à, dentre outros elementos, “proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas [...] os direitos e liberdades fundamentais, nos termos desta Lei”. Medidas de promoção e proteção dos direitos e liberdades dos titulares, que se enquadram nessa categoria são, por exemplo, a anonimização ou pseudonimização, já que são aptas a mitigar os potenciais impactos negativos de um tratamento de dados pessoais.

De forma semelhante, na normativa europeia (RGPD), o princípio da necessidade equivale ao “princípio da minimização dos dados” e “limitação da conservação”, de modo que os dados pessoais deverão ser adequados (suficientes para cumprir adequadamente o seu propósito declarado), pertinentes (racionalmente ligados ao propósito) e limitados ao necessário para os propósitos do tratamento. Segundo esse princípio, os dados pessoais apenas devem ser

⁵ Previsto no art. 5º, XVII, da LGPD, cuida-se de uma documentação do agente de tratamento a quem competem as decisões referentes ao tratamento de dados pessoais. *In verbis*: Art. 5º Para os fins desta Lei, considera-se: **XVII - relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; (grifos nossos)

⁶ A LGPD define, no inciso XI do artigo 5º, que a anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". A definição para os dados pseudonimizados, por seu turno, está no artigo 13, §4º do diploma, sendo 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”.

tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.

Assim, caso se verifique que foram solicitados dados em excesso, o tratamento passará a ser ilícito. Cuida-se, nessa hipótese, de contraordenação muito grave, a qual está prevista e sancionada nos termos da alínea “a” do n.º 5 do artigo 83.º do RGPD, senão veja:

Art. 83.º (...) 5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20000000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:

b) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5, 6º, 7º e 9º;(…)

É precisamente por isso que o controlador precisa assegurar que o prazo de armazenamento do dado pessoal também seja limitado ao mínimo necessário. Isto é, os dados pessoais precisam ser descartados assim que terminado o tratamento, considerada a oferta do produto ou do serviço⁷. Isso se afirma, pois não é possível, à luz do princípio da necessidade, a coleta massiva de dados pessoais para só depois se pensar nos possíveis usos e destinos dos dados. Nesses casos, ainda, há de se reconhecer a evidente relação proporcional entre a quantidade de dados tratada e a responsabilidade, notadamente em casos de vazamentos e incidentes de segurança.

Nesse contexto, as empresas controladoras e operadoras de dados pessoais efetivamente precisam adotar medidas para se adequarem ao princípio da necessidade – a saber, providenciando o levantamento de todos os dados coletados e tratados (e a varredura dos dados pessoais armazenados e suas respectivas naturezas); a revisão das políticas das referidas coletas; e até o treinamento dos contratados para evitar a coleta desnecessária – e, portanto, ilegal – de dados pessoais. Os responsáveis pelo tratamento, ainda, devem divulgar as categorias de dados pessoais envolvidos no tratamento, de sorte a vinculá-las adequadamente à específica finalidade

⁷ Relaciona-se a esse ponto o artigo 17 do RGPD, que explicitamente dispõe acerca do direito ao esquecimento, uma salvaguarda de suma importância para a aplicação dos princípios de proteção de dados, destacadamente o princípio de minimização de dados. *In verbis*: “**Artigo 17º - 1.** O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito sem demora injustificada e o responsável pelo tratamento tem a obrigação de apagar os dados pessoais sem demora injustificada quando se aplique um dos seguintes motivos: **(a)** os dados pessoais não são mais necessários em relação aos fins para os quais foram coletados ou processados de outra forma (...)”.

pretendida, nos termos do art. 15º, nº 1, alínea ‘b’ do RGPD, sob pena de violação aos princípios da minimização de dados e da transparência.

No que concerne à utilização de dados pela Administração Pública, no mesmo caminho, é preferível a adoção de um meio que seja, concomitantemente, menos gravoso para o indivíduo e para o interesse público, ante a evidente inserção na temática de intervenção na privacidade e liberdade individuais. Sobre o tema, dispõe o seguinte trecho do Considerando 156 do RGPD:

As condições e garantias em causa podem implicar procedimentos específicos para o exercício desses direitos por parte do titular de dados, se tal for adequado à luz dos fins visados pelo tratamento específico a par de medidas técnicas e organizativas destinadas a reduzir o tratamento de dados pessoais de acordo com os princípios da proporcionalidade e da necessidade.

Por outro lado, é notório que uma conduta conforme leva, em muitos casos, a uma redução de despesas com segurança de dados. Afinal, apesar de não expressamente prevista nos princípios elencados no art. 6º da LGPD, a proporcionalidade da segurança, como antecipado, também é uma diretriz norteadora do regulamento. Logo, a revisão da estrutura de armazenamento e da segurança de informação – para que sejam adequadas ao tamanho da operação – contribuem duplamente (i) à adequação principiológica; e (ii) à redução de despesas.

2. Estudos de Caso

2.1. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387/ DISTRITO FEDERAL

Em âmbito nacional, a temática principiológica da LGPD foi tratada pela Corte Suprema em sede do julgamento da medida cautelar pleiteada na Ação Direta de Inconstitucionalidade nº 6387/DF⁸. Cuida-se, mais especificamente, de ação ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) contra o inteiro teor da Medida Provisória nº 954, de 17 de abril de 2020, que dispunha sobre “o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística”. O compartilhamento tinha por finalidade suportar a produção estatística oficial durante a situação crítica de saúde

⁸ As ações diretas de inconstitucionalidade nº 6388, 6389, 6390 e 6393, por igualmente impugnarem a validade constitucional da Medida Provisória nº 954/2020, tramitaram em conjunto com o feito em comento.

pública de importância internacional decorrente do coronavírus, de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

O requerente materialmente alegou, em síntese, que a Medida Provisória supramencionada violou dados sigilosos, inclusive o telefônico, dos brasileiros; detinha finalidade genérica e imprecisa, qual seja, a produção de estatística oficial mediante a realização de entrevistas não presenciais no âmbito de pesquisas domiciliares; não definiu procedimentos de controle pelo Judiciário, pelo Ministério Público ou por órgãos da sociedade civil para a guarda dos dados disponibilizados no âmbito da Fundação IBGE; não apresentou precisamente a modalidade, a frequência e o objetivo das pesquisas a serem realizadas, nem as razões que justifiquem a necessidade do compartilhamento dos dados para a pesquisa estatística; dentre outros argumentos.

Nesse caminho, o Conselho Federal da Ordem dos Advogados do Brasil/CFOAB argumentou que a Medida Provisória questionada impõe restrições à proteção de direitos fundamentais, haja vista que não atende ao critério da proporcionalidade, notadamente no que tange às dimensões da adequação, da necessidade e da proporcionalidade em sentido estrito. O IBGE, doutro lado, sustentou que o compartilhamento de dados estabelecido na Medida Provisória não se confundia com o rastreamento de clientes, de modo que não haveria acesso ao conteúdo das comunicações telefônicas. Sumariamente, os pontos de vista em combate eram, portanto:

Síntese argumentos CFOAB	Síntese argumentos IBGE
A violação irrestrita ao direito à privacidade em nome do combate à pandemia do coronavírus, agravada pelos objetivos abstratos contidos na MP.	A necessidade de continuidade do recolhimento de dados para a produção de pesquisas oficiais durante a pandemia, em conformidade à confidencialidade estatística.

Quanto ao caso, importa ressaltar que somente um dispositivo da MP nº 954/2020 dispôs sobre a finalidade e o modo de utilização dos dados. Nesse sentido, o §1º do art. 2º limitava-se a enunciar que:

§1º Os dados de que trata o caput serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

É de se ver, como bem observou a Ministra Rosa Weber,⁹ que a norma não delimitou: (i) o objeto da estatística a ser produzida; (ii) sua finalidade específica; (iii) sua amplitude; (iv) a necessidade de disponibilização dos dados; (v) como os dados serão efetivamente utilizados. Outrossim, é imperativo consignar que, mesmo em cenários de crise, o compartilhamento de dados deve estar em conformidade aos mandamentos constitucionais e legais, notadamente no que tange à estrita relação entre adequação e necessidade.

Não por outro motivo, em decisão monocrática que deferiu a medida liminar pleiteada, a Ministra apontou, dentre outros aspectos, que:

Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. (grifos nossos)

Como esclarecido em tópico anterior, o que se busca com a diretriz principiológica inaugurada pela LGPD é uma transição do paradigma do máximo possível de dados para o mínimo necessário de dados. À vista disso, o que há de ser definido no caso concreto, visando à resolução da controvérsia, é: (i) a quantidade e a variedade de dados pessoais efetivamente necessárias; (ii) a finalidade específica ou concreta, geralmente inserida dentro de uma finalidade geral; (iii) o ponto ótimo entre a minimização da coleta de dados pessoais e a efetividade do processo, aplicando-se as normativas cabíveis.

In casu, concluiu-se que a MP 954/2020 não estabeleceu interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. Nesse caminho, ao deixar de definir apropriadamente a forma e a finalidade de coleta dos dados, o dispositivo não ofereceu condições para aferição de sua adequação e necessidade, bem como falha do ponto de vista da transparência necessária para uma adequada conciliação entre a demanda de produção estatística e os direitos fundamentais à proteção de dados e à autodeterminação informativa.

⁹ Ministra relatora da ação direta em análise.

Em 07/05/2020, o Plenário da Corte, referendando a decisão de deferimento da medida cautelar da Ministra relatora, suspendeu a eficácia da questionada MP, com comando para que o IBGE deixasse de solicitar às empresas concessionárias a disponibilização dos dados. Sob o vértice constitucional, assentou o Informativo 976/STF:

O art. 2º da MP 954/2020 impõe às empresas prestadoras do STFC e do SMP o compartilhamento, com o IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas. Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e seu tratamento, desse modo, devem observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

Posteriormente, a ação direta foi julgada prejudicada, por perda superveniente do seu objeto, vez que a Medida Provisória nº 954/2020 não logrou ser convertida em lei no prazo constitucional previsto e teve sua vigência encerrada em 14/8/2020.

2.2. “TK” vs. Associação dos condôminos do edifício M5A (*‘A Asociația de Proprietari bloc M5A-ScaraA’*)

No âmbito europeu, relevante controvérsia foi analisada pelo Tribunal de Justiça da União Europeia (TJUE)¹⁰ envolvendo a aplicação concreta do princípio da minimização. No caso, a Terceira Secção do referido Tribunal proferiu acórdão em controvérsia que envolvia a instalação de sistemas de videovigilância nas partes comuns de um edifício para habitação. Foi analisada questão prejudicial¹¹ em relação à interpretação do artigo 6º, nº 1, alínea ‘c’, e do artigo 7º, alínea ‘f’, da Diretiva 95/46/CE¹² do Parlamento Europeu e do Conselho, de 24 de

¹⁰ O TJUE é o supremo tribunal da União Europeia (UE).

¹¹ Com objetivo de garantir uma aplicação efetiva e isonômica das normas e evitar interpretações divergentes, os juízes nacionais dos estados-membros da UE têm o poder-dever de, no contexto da União Europeia, consultarem o Tribunal de Justiça europeu a fim de que sejam esclarecidos pontos de interpretação do direito da União. Assim, visa-se a verificar a conformidade da respectiva legislação nacional com esse direito. Ademais, o pedido de decisão prejudicial pode ainda ter por finalidade a fiscalização da legalidade de um ato de direito da União Europeia.

¹² A Diretiva 95/46/EC foi substituída pelo RGPD, que se tornou aplicável em 25 de maio de 2018.

outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *In verbis*:

Artigo 6º. 1. Os Estados-Membros devem estabelecer que os dados pessoais serão: (...) **c)** Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;

Artigo 7º. Os Estados-Membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se: (...) ou **f)** O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

A legislação romena concernente ao tema, por sua vez, dispunha que qualquer tratamento de dados pessoais, exceto se referente a dados pertencentes a determinadas categorias¹³, só pode ser efetuado se a pessoa em causa tiver dado expressa e inequivocamente o seu consentimento para esse tratamento. No bojo do processo originário, a decisão da Autoridade Nacional de Supervisão do Tratamento de Dados Pessoais romena (ANSPDCP)¹⁴, relativa ao tratamento de dados pessoais obtidos por videovigilância, na versão aplicável ao processo principal, previa, nos seus artigos 1º; 4º; 5º, nº's 1 a 3; e 6º que:

Art. 1º. A recolha, gravação, armazenamento, utilização, transmissão, divulgação ou qualquer outra operação de tratamento de imagens por videovigilância, que permita,

¹³ Lei nº 677/2001, Art. 5º. 2. “O consentimento do titular dos dados não é exigido nos seguintes casos:

a) quando o tratamento for necessário para a execução de um contrato ou em negociações pré-contratuais em que seja parte o titular dos dados ou para a adoção de medidas, a seu pedido, antes da celebração de um contrato ou durante as negociações pré-contratuais;

b) quando o tratamento for necessário para a proteção da vida, da integridade física ou da saúde do titular dos dados ou de outra pessoa exposta a ameaça;

c) quando o tratamento for necessário para o cumprimento de uma obrigação legal do responsável pelo tratamento;

d) quando o tratamento for necessário para a execução de atribuições de interesse público ou destinadas ao exercício de prerrogativas de poder público de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

e) quando o tratamento for necessário para a realização de um interesse legítimo do responsável pelo tratamento ou do terceiro a quem os dados são comunicados, desde que esse interesse não afete os interesses ou os direitos e liberdades fundamentais do titular dos dados;

f) quando o tratamento disser respeito a dados provenientes de documentos acessíveis ao público, nos termos da lei;

g) quando o tratamento for efetuado exclusivamente para fins estatísticos, de investigação histórica ou científica, e os dados permanecerem anónimos durante todo o tratamento.”

¹⁴ Órgão responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da legislação de tratamento de dados na Romênia.

direta ou indiretamente, identificar pessoas singulares, constituem operações de tratamento de dados pessoais abrangidas pelo âmbito de aplicação da [Lei n° 677/2001].

Art 4°. A videovigilância pode ser realizada principalmente para os seguintes fins: **a)** prevenção e combate à criminalidade; **b)** monitorização do tráfego rodoviário e das infrações ao direito estradal; **c)** segurança e proteção de pessoas, bens e valores, edifícios e instalações de utilidade pública e respectivos recintos; **d)** execução de medidas de interesse público ou exercício de prerrogativas de poder público; **e)** realização de interesses legítimos, desde que não sejam violados os direitos e liberdades fundamentais das pessoas em causa.

Art 5°. **1.**A videovigilância pode ser efetuada em locais e espaços abertos ou destinados ao público, incluindo vias públicas de acesso situadas no domínio público ou privado, nas condições previstas na lei. **2.** As câmaras de videovigilância são instaladas de forma visível. **3.**É proibida a utilização de câmaras de videovigilância dissimuladas, exceto nos casos previstos na lei.

Art 6°. O tratamento de dados pessoais através de sistemas de videovigilância é efetuado com o consentimento expreso e inequívoco da pessoa em causa ou nos casos previstos no artigo 5°, n° 2, da Lei n° 677/2001 [...]

Como antecipado, o pedido prejudicial foi exprimido no âmbito de litígio oposto por um indivíduo – “TK” – em face de uma associação de condôminos, no qual o morador formula requerimento no sentido de que a associação desative o sistema de videovigilância do edifício, além de que remova as câmeras instaladas nas partes comuns dele (fachada, elevador e corredor do piso térreo), por constituir violação do direito à reserva da vida privada. Alegou, ainda, que a associação “tinha assumido a função de responsável pelo tratamento dos dados pessoais sem ter seguido o procedimento de registro previsto na lei para o efeito”.

A associação, em resposta, mencionou que a decisão de instalação de câmeras no prédio foi aprovada em assembleia geral dos condôminos e tinha sido tomada para controlar as movimentações no edifício da forma mais eficaz possível, em razão do fato de o elevador ter sido várias vezes vandalizado, além de apartamentos e partes comuns terem sido objeto de assaltos e furtos.

O Tribunal de Primeira Instância de Bucareste ressaltou a previsão de que o tratamento de dados pessoais necessário para proteger a vida, a integridade física ou a saúde do titular dos dados ou de outra pessoa exposta a ameaça excepciona a necessidade de consentimento

expresso (artigo 5º, nº 2 da Lei romena nº 677/2001). Em adição, sustentou que o sistema de videovigilância *in casu* “não parece ter sido utilizado de forma ou com uma finalidade que não correspondesse ao objetivo declarado pela associação dos condôminos do edifício”, havendo proporcionalidade entre o propósito prosseguido pela ingerência nos direitos e liberdades dos cidadãos e os meios utilizados. Nessas circunstâncias, o órgão jurisdicional local suspendeu o julgamento da lide e submeteu ao Tribunal de Justiça a questão prejudicial.

Nesse contexto, recorreu-se ao TJUE para o fornecimento de orientações sobre como avaliar se um determinado tratamento (no caso, um sistema de videovigilância) poderia ser considerado ‘necessário’ para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento.

O TJUE considerou a necessidade de uma operação de tratamento ser examinada em conjunto com o princípio da minimização de dados, o qual restringe as opções do responsável pelo tratamento àquelas adequadas, relevantes e não excessivas em relação às finalidades para as quais são recolhidos.

Ademais, salientou ser necessária uma ponderação¹⁵ dos direitos e interesses opostos no caso concreto – sendo vedada a mera exclusão da possibilidade de tratamento de determinadas categorias de dados pessoais – para apreciar qual deveria prevalecer: o direito à proteção de dados ou o interesse legítimo prosseguido pelo responsável pelo tratamento.

Sustentou, ainda, não ser exigido o consentimento da pessoa em causa enquanto requisito para o tratamento de dados pessoais na hipótese do artigo 7º, alínea “f” da Diretiva 95/46/CE. Com efeito, ressaltou ser um dos requisitos a legitimidade do interesse visado pelo responsável pelo tratamento – *in casu* a proteção de bens, da saúde e da vida dos condôminos. Frisou o TJUE que tal condição impõe ao órgão jurisdicional nacional que verifique se o interesse legítimo no caso não pode ser razoavelmente alcançado de modo igualmente eficaz por meio de outras formas menos atentatórias aos direitos à reserva da vida privada e à proteção

¹⁵ Nessa ponderação, deve-se considerar diversos elementos, tais como: (i) o caráter variável, a depender da acessibilidade da fonte ao público, da gravidade da violação dos direitos fundamentais da pessoa em causa pelo referido tratamento; (ii) a natureza dos dados pessoais em questão, destacando-se aqueles potencialmente sensíveis, assim como outras características do tratamento, sobretudo o número de pessoas que têm acesso a esses dados e as formas de acesso a eles; (iii) as expectativas razoáveis dos indivíduos de que os seus dados pessoais não serão tratados posteriormente; (iv) a importância, para todos os condôminos do edifício em causa, do interesse legítimo prosseguido no caso vertente pelo sistema de videovigilância, na medida em que visa essencialmente a garantir a proteção de bens, da saúde e da vida.

dos dados pessoais (relacionando-se à vertente da menor intrusividade do princípio da necessidade).

Decidiu, também, que o requisito relativo à proporcionalidade do tratamento dos dados no processo parece ter sido contemplado, eis que (i) foi adotada medida alternativa previamente – sistema de segurança, instalado na entrada do edifício, composto por um intercomunicador e um cartão magnético –, que se revelou insuficiente; e (ii) o sistema de videovigilância está limitado às partes comuns do condomínio e às suas vias de acesso.

Em conclusão, o Tribunal europeu esclareceu que a proporcionalidade deve ser examinada, também, tendo em vista o modo concreto de instalação e funcionamento do dispositivo, que devem limitar o seu impacto sobre os direitos individuais e garantir concomitantemente a eficácia do sistema de videovigilância. Portanto, o controlador deve aferir, entre outros aspectos, “se é suficiente que a videovigilância funcione apenas à noite ou fora do horário normal de trabalho, além de bloquear as imagens captadas em áreas onde a vigilância é desnecessária”.

O dispositivo da questão prejudicial, por último, destacou que, desde que o tratamento dos dados pessoais cumpra os requisitos previstos no artigo 7º, alínea “f”, não haveria vedação jurídico-legal à instalação do sistema de videovigilância.

3. Considerações finais

Do exposto, resta perceptível que o princípio da necessidade – denominado, na legislação europeia, de princípio da minimização – possui vital importância na compreensão e na aplicação da LGPD e do RGPD. Com efeito, para além de conferir maior efetividade à coleta e ao tratamento de dados, tal princípio evita exposições desnecessárias dos tutelados pelos diplomas supramencionados, na medida em que baliza a realização do tratamento ao que se mostrar imprescindível à consecução da finalidade previamente delimitada.

Como visto, existem diferentes dimensões que resultam da obrigação de minimização dos dados, eis que essa deve ser aplicada à quantidade de dados recolhidos, à extensão do processamento, ao período de armazenamento e à própria acessibilidade aos dados. Nesse caminho, releva destacar que o entendimento e a aplicação do princípio em análise se conectam a outros princípios, notadamente o da eficiência, da proporcionalidade, da finalidade e da adequação, como vêm decidindo os tribunais.

Por último, insta repisar o imperioso objetivo do princípio em comento, qual seja promover a difícil transição da lógica do máximo possível de dados para o mínimo necessário de dados, com menores intrusividade e lesividade aos indivíduos, e de modo a barrar, ainda, o uso incondicional de dados.

Referências bibliográficas

ÁVILA, HUMBERTO. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. 19. ed. rev e atual. - São Paulo: Malheiros, 2019.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa. 2021
BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. *Lei nº 13.709, de 14 ago. 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)*, Brasília, DF. BRASIL, Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 6387. Relatora: Min. Rosa Weber, julgado em 7/5/2020, DJe 12/11/2020. 2020.

DATA PROTECTION NETWORK. Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation. Reino Unido, 2017. Disponível em: <https://www.dpnetwork.org.uk/wp-content/uploads/2018/11/DPN-Guidance-A4-Publication-17111.pdf>. Acesso: 22 mar. 2022.

DOHMANN, Indra. A Proteção de Dados Pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. RDP, Brasília, Volume 17, n. 93, 9-32, maio/jun. 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da

formação da Lei Geral de Proteção de Dados. 2. ed. -- São Paulo: Thomson Reuters Brasil. 2020.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo, *et al.* Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

FALK, Matheus. Os “princípios jurídicos” da LGPD e do RGPD: uma leitura a partir da Teoria dos Princípios de Humberto Ávila. In: WACHOWICZ, Marcos. Proteção de dados pessoais em perspectiva: LGPD e RGPD na ótica do direito comparado. Curitiba: Gedai, UFPR 2020.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Disponível em: Minha Biblioteca UnB.

PINHEIRO, Patrícia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018. São Paulo: Saraiva Educação, 2018.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão de 11.12.2019, processo C-708/18. 2019. Disponível em: <<https://curia.europa.eu/juris/document/document.jsf?jsessionid=4A9F71BCDFB6F507CC5D0302FA1AE329?text=&docid=221465&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=35786932>>. Acesso: 6 abr. 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz

respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE . 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso: 5 abr. 2022

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso: 5 abr. 2021.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia (2016/C 202/02). 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso: 5 abr. 2021.

WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder Público*. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p.271-288. Disponível em: Minha Biblioteca UnB.

