

— 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

OBRIGAÇÕES DOS AGENTES DE TRATAMENTO DE DADOS: INTERFACES ENTRE A REGULAÇÃO BRASILEIRA E EUROPEIA

Sofia de Medeiros Vergara¹

Dispositivo LGPD	Dispositivo RGPD
<p>Art. 5º (definições dos agentes de tratamento);</p> <p>Art. 42 (responsabilidade dos agentes de tratamento);</p> <p>Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:</p> <p>I – finalidade;</p> <p>II – adequação;</p> <p>III - necessidade;</p> <p>IV - livre acesso;</p> <p>V - qualidade dos dados;</p> <p>VI - transparência;</p> <p>VII - segurança;</p> <p>VIII - prevenção;</p> <p>IX - não discriminação;</p> <p>X - responsabilização e prestação de contas.</p> <p>Art. 7º (hipóteses de tratamento de dados pessoais);</p> <p>Art. 14. (O tratamento de dados pessoais de crianças e de adolescentes).</p> <p>Art. 20, § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.</p> <p>Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.</p> <p>Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas</p>	<p>Art. 4 (7) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;</p> <p>Art. 4 (8) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes</p> <p>Art. 26 (1) Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.º e 14.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados.</p> <p>Art. 5 (Princípios relativos ao tratamento de dados pessoais);</p> <p>Art. 6 (Licitude do tratamento);</p> <p>Art. 7 (condições aplicáveis ao consentimento);</p> <p>Art. 12 (1) O responsável pelo tratamento toma as</p>

¹ Graduanda em Direito na Faculdade de Direito da Universidade de Brasília (UnB); Editora-Assistente na Revista dos Estudantes de Direito da UnB; membra do Grupo de estudos em Empresarial e Arbitragem da UnB (GEA), membra do Grupo de Estudos sobre Constituição, Empresa e Mercado da UnB (GECM); membra do Observatório de LGPD; e membra do Women Inside Trade Starters (WIT Starters).

pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

Art. 8 (Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação)

Art. 15 (1) (h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n. 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Art. 30. (Registos das atividades de tratamento)

Art. 29. O subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

Art. 37 (Designação do encarregado da proteção de dados)

Art. 24 (1) Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Art. 25 (Proteção de dados desde a conceção e por defeito;)

Art. 28 (Subcontratante);

Art. 32 (Segurança do tratamento);

Art. 31. O responsável pelo tratamento e o subcontratante e, sendo caso disso, os seus

representantes cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições.

Art. 33. Notificação de uma violação de dados pessoais à autoridade de controlo

Art. 34. Comunicação de uma violação de dados pessoais ao titular dos dados

Introdução

Com a globalização e digitalização da sociedade atual, a preocupação com o tratamento de dados pessoais cresce cada vez mais, principalmente diante dos grandes conglomerados de tecnologia que têm livre acesso e controle aos dados de milhões de usuários. Nesse contexto, diversas jurisdições têm iniciado sua trajetória para regulamentação do tratamento de dados pessoais, dentre as quais não se pode deixar de mencionar a União Europeia e o Brasil.

O bloco europeu foi um dos pioneiros na busca pela proteção de dados, editando ainda no ano de 1995 a Diretiva de Proteção de Dados Pessoais (95/46/CE), que, em 2016, foi substituída pelo Regulamento Geral sobre a Proteção de Dados (RGPD). A diretiva abriu o caminho para a discussão acerca da segurança de dados na rede e dos deveres e regras que esses agentes que realizam o tratamento de dados devem se ater. Foi justamente inspirado no RGPD, que o congresso brasileiro promulgou a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD) no ano de 2019, com clara influência do normativo europeu.

Nesse contexto, o presente artigo pretende perpassar pelas principais obrigações dos agentes de tratamento diante dessa nova era de regulamentação da internet que se mostrou extremamente necessária no mundo digital, traçando um paralelo entre o que é definido pelo RGPD e pela LGPD. A fim de aprofundar a discussão legislativa, serão abordados também dois casos práticos envolvendo a empresa Whatsapp Inc. em que essas obrigações foram evidenciadas pelas autoridades de proteção de dados responsáveis, um brasileiro e outro no âmbito da União Europeia.

1. Comentários

O tratamento de dados corresponde a “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (art. 5º, inciso X, da LGPD).

Como ensina Mario Viola e Chiara de Teffê (2020, p. 131), o pressuposto para a regulação do tratamento de dados é justamente a proteção do titular, de forma que na “Lei Geral de Proteção de Dados, parte-se da ideia de que todo dado pessoal tem importância e valor. Por essa razão, adotou-se conceito amplo de dado pessoal, assim como estabelecido no Regulamento europeu 2016/679, sendo ele definido como informação relacionada a pessoa natural identificada ou identificável”. Nesse sentido, um passo importante para a proteção do dado pessoal é a identificação de quais são os agentes que poderão tratá-lo, bem como quais são os parâmetros e diretrizes que deverão ser seguidas nesse tratamento.

Conforme estipula a Lei Geral de Proteção de Dados, são considerados agentes de tratamento: o controlador e o operador. Embora essa classificação como “agente de tratamento de dados”, enquanto categoria aglutinadora dos conceitos supra, não seja feita no âmbito da União Europeia, o RGPD também apresenta as categorias de controlador (“*controller*”) e processador (“*processor*”), de forma que, para os fins deste artigo, serão analisados como equivalentes aos agentes definidos na LGPD.

Assim, antes de adentrar na discussão acerca das obrigações dos agentes de tratamento, faz-se necessário indicar, primeiro, como a LGPD e o RGPD classificam esses agentes e quem são as pessoas físicas ou jurídicas que se enquadram nessa categoria.

No âmbito da LGPD, os agentes de tratamento são considerados a partir de seu caráter institucional, isto é, “não são considerados controladores (autônomos ou conjuntos) 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” (ANPD, 2021b, p. 5). Tanto pessoas jurídicas quanto pessoas físicas podem ser abarcadas por essas categorias. Ressalta-se, porém, que a pessoa física apenas poderá ser considerada controladora quando agir em prol de seu próprio interesse, dispondo de autonomia para determinar as finalidades e elementos essenciais do tratamento. Por outro lado, poderá ser considerada operadora quando atuar de acordo com os interesses do operador, com a autonomia para definição de elementos não essenciais à finalidade do tratamento (ANPD, 2021b).

No contexto da pessoa jurídica, é a própria organização que será considerada como agente de tratamento, de forma que os funcionários que atuam em subordinação às decisões do

controlador, representando-o, não deverão ser confundidos com operadores. Outrossim, a caracterização como controlador ou operador não é permanente, sendo definida a cada operação de tratamento de dados pessoais. Isto é, uma mesma empresa ou entidade poderá desempenhar os papéis de controlador ou operador a depender do seu papel em determinado tratamento de dados (ANPD, 2021b).

Pois bem, passado para as diferenças entre controlador e operador/processador, tem-se que a LGPD define que o controlador será aquele a “quem compete tomar as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI, LGPD), de forma similar ao controlador do RGPD, que consiste na “pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que, isoladamente ou em conjunto com outros, determine os fins e os meios de tratamento dos dados pessoais” (art. 4 (7), RGPD). Embora seja possível identificar uma diferença conceitual — a explicitação da possibilidade de controladores conjuntos —, é possível perceber a similitude quanto à característica principal dessa categoria de agente: o poder de decisão — isto é, o controle dos elementos essenciais para o cumprimento da finalidade do tratamento.

A diferente classificação de controladores e operadores/processadores tem relevância não somente teórica, mas também prática. Isso porque tanto o RGPD quanto a LGPD atribuem responsabilidades diferenciadas e específicas para cada um desses.

No âmbito nacional, são exemplos de obrigações específicas do controlador: (i) a elaboração de relatório de impacto à proteção de dados pessoais (art. 38, LGPD); (ii) a comunicação à ANPD sobre eventual ocorrência de incidentes de segurança (art. 48); e (iii) a comprovação de que o consentimento obtido atende às exigências legais (art. 8, § 2º, LGPD). Tal distinção também se aplica à responsabilidade em relação à reparação por danos ilícitos, definida nos arts. 42 a 45 da LGPD, que é aplicada de forma diferente de acordo com a qualificação do agente (ANPD, 2021b).

Ressalta-se, a título de exemplo, que o operador será solidariamente responsável para com o controlador pelos danos causados aos titulares quando houver descumprido a legislação ou quando aquele não tiver seguido as instruções lícitas desse (art. 42, §1º, I). Por outro lado, os controladores serão sempre responsáveis solidários entre si quando ocorrerem danos ao titular de dados (art. 42, §1º, II). Veja que, quanto ao operador, deverá ser comprovada a atividade ilícita ou descumprimento de instruções, enquanto o controlador responderá objetivamente, aos moldes da responsabilização por atividades de risco disposta no art. 927,

Parágrafo Único, do Código Civil. Quanto às matérias de defesa que poderão ser alegadas, essas estão restritas à comprovação das exceções descritas no art. 43 para os controladores. Por outro lado, o operador poderá, além das exceções retro, comprovar que cumpriu os dispositivos legais, que a instrução do controlador foi cumprida e/ou que essa era ilegal (justificando o seu descumprimento).

Enquanto isso, no âmbito da União Europeia, o controlador será responsável por realizar e demonstrar o *compliance*, em alinhamento ao princípio da “*accountability*” (art. 5 (2), RGPD); bem como pela realização da avaliação do impacto da proteção de dados para examinar, em particular, a origem, natureza, particularidade e gravidade desse risco (Consideração nº 84, RGPD). O controlador também será responsável, entre outros, por demonstrar que o processamento ocorreu com o consentimento do titular de dados (art. 7 (1), RGPD), facilitar o exercício dos direitos dos titulares de dados, ressalvadas as hipóteses de não identificação do titular e providenciar cópias dos dados pessoais que passam pelo tratamento de dados (art. 15 (3), RGPD).

Em relação aos controladores conjuntos, embora não esteja expresso na LGPD, a ANPD, no exercício de sua função regulamentar, reconheceu essa possibilidade para o ordenamento jurídico brasileiro. Para tanto, apontou os seguintes critérios para que esteja configurada uma controladoria conjunta: (i) mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais; (ii) há interesse mútuo de dois ou mais controladores, com base nas finalidades próprias, sobre um mesmo tratamento; e (iii) dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades de tratamento (ANPD, 2021b, p. 13).

De forma análoga, o Comitê Europeu para Proteção de Dados (EDPB, 2020, p. 18) indicou que duas decisões podem ser consideradas convergentes quando complementam uma à outra e quando for necessário para que o processamento ocorra de forma a impactar, de modo tangível, a determinação dos propósitos e meios de processamento.

Por sua vez, o operador será aquele que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD), de forma similar ao processador do RGPD, que consiste na “pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que processa dados pessoais em nome do responsável pelo tratamento” (art. 4 (8), RGPD). “Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador” (ANPD, 2021b,

p. 16). Conforme explica o Parecer 1/2010 (WP29, 2010, p. 25) a “existência de processador depende de decisão do controlador, que pode decidir processar dados dentro de sua organização [...] ou delegar todas ou parte das atividades de processamento a uma organização externa, ou seja, [...] para pessoa separada legalmente agindo em seu nome”.

Um aspecto relevante no ordenamento jurídico brasileiro é a questão vinculada às obrigações de tratamento da pessoa jurídica de direito público, isso porque em muitos casos existirá apenas uma pessoa jurídica (entidade da administração pública direta ou indireta) dividida internamente em vários órgãos (entes despersonalizados). Quando estes órgãos realizam o tratamento de dados, surge um problema para a identificação do controlador. A ANPD (2021b) dispõe que nesses casos deverão ser considerados dois aspectos: de um lado, conforme o art. 5º, VI, da LGPD, o controlador é a União, que detém personalidade jurídica; por outro, a LGPD atribuiu aos órgãos públicos obrigações típicas de controlador, de forma que suas atribuições são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte. O mesmo raciocínio pode, regra geral, ser aplicado analogamente para os estados e municípios, detentores de personalidade jurídica, suas secretarias e demais órgãos públicos a eles vinculados.

Detalhados os conceitos de controlador e operador, bem como suas funções, cumpre analisar, de modo geral, dada a grande amplitude do tema, as principais obrigações dos agentes de tratamento de dados — buscando, sempre que possível, traçar um paralelo entre as duas jurisdições. Para tal, considera-se que “o modelo de tratamento de dados instituído pela LGPD se ampara nas seguintes características básicas: a ampliação do conceito de dado pessoal; o respeito à base legal; e o legítimo interesse como hipótese autorizativa e necessidade de realização de um teste de balanceamento de interesses” (MENEZES; COLAÇO, 2019). Isso porque,

A LGPD é categórica em relação às hipóteses que autorizam o tratamento de dados pessoais, ainda que os arts. 7.º (tratamento de dados pessoais), 11 (tratamento de dados pessoais sensíveis) ou 14 (tratamento de dados pessoais de crianças e adolescentes) do diploma arrolem conceitos jurídicos indeterminados (como “legítimo interesse”, nos termos do art. 7.º, IX, da LGPD) e confirmem margem para inovações regulatórias ou contratuais (arts. 7.º, II, V, e 11, II, “a”, da LGPD) não minudenciadas na lei (ALVES JR., 2020).

Importante ressaltar que princípios legais como legítimo interesse, bem como a adequação, finalidade, proporcionalidade e necessidade são conceitos que permitem uma amplitude de interpretações, de modo que as expectativas dos titulares recebem um peso considerável na aplicação desses princípios. Assim, quanto “mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse” (VIOLA; TEFFÊ, 2020).

Outra obrigação importante e que parece embasar as demais obrigações dos agentes de tratamento é a obrigação de transparência. O princípio da transparência é entendido como um dos pilares no tratamento de dados, conforme evidenciou a Convenção nº 108 do Conselho da Europa. Tal princípio foi recepcionado tanto pelo RGPD, em seu art. 12º, em consonância com o Considerando nº 58 — ao aduzir que “o princípio da transparência exige que qualquer informação dirigida ao público ou ao titular dos dados seja concisa, facilmente acessível e fácil de entender, com linguagem clara e simples e, além disso, onde apropriado, a visualização deve ser usada”² — quanto como pela LGPD, em seu art. 6º, VI, a qual garante aos titulares dos dados informação clara, precisa e facilmente acessível sobre a realização do tratamento.

A obrigação de transparência não apenas adquire um papel importante na garantia de *accountability* das empresas que realizam o tratamento de dados, mas também aduz um importante papel social, especialmente quando contraposta aos princípios da dignidade humana e não discriminação. Essa relação é resumida com clareza na seguinte afirmação dos pesquisadores Bruno Bioni, Marina Kitayama e Mariana Rielli (2021, p. 35):

Adotando a perspectiva de que a proteção de dados tutela bens jurídicos de interesse da coletividade, como a não discriminação e a dignidade humana, a publicidade sobre as práticas de tratamento é de extrema importância. Há casos em que o tratamento abusivo de dados leva a violações de direitos afetos a todos de um segmento populacional, sendo conhecidas as situações de discriminação por raça, gênero e perfil socioeconômico em virtude de usos abusivos de dados pessoais. A transparência ativa das empresas desempenha também um papel de responsabilidade social, sujeitando suas próprias práticas à apreciação pública de um lado; e criando uma cultura que padroniza essa atitude nos mercados, de outro.

² Tradução livre.

Ademais, o capítulo VI da LGPD trata especificamente dos agentes de tratamento de dados, dispondo algumas das obrigações específicas desses agentes perante a nova legislação em vigor. Nesse sentido, dispõe que caberá ao controlador e ao operador manter o registro das operações de tratamento de dados pessoais que realizarem (art. 37, LGPD). De forma similar, o RGPD estipula, em seu art. 30, a necessidade de documentação dos processos. Contudo, diferentemente da LGPD, o RGPD aprofunda nesse tema ao dispor sobre a obrigação de revisão e de atualização dos procedimentos adotados de acordo com as necessidades que esses apresentem (PECK, 2020).

As obrigações dos agentes de tratamento de dados não são determinadas apenas durante o período de processamento dos dados, mas também quando esse tratamento é finalizado. Assim, os arts. 15 e 16 da LGPD definem as hipóteses do término do tratamento de dados e a obrigação dos agentes em eliminá-los, ressalvadas as hipóteses legais. O término poderá ocorrer por diversas situações, dentre as quais: (i) o alcance da finalidade pretendida; (ii) os dados pessoais deixam de ser necessários ou pertinentes para o alcance da finalidade específica; (iii) determinação da autoridade nacional de proteção de dados; (iv) manifestação do titular requerendo o término do tratamento, entre outros (ALVES JR., 2020).

Por sua vez, o RGPD define de forma expressa a necessidade de prazos para o apagamento dos dados ou revisão periódica, introduzindo uma limitação temporal para o tratamento de dados — que não aparece de forma expressa na LGPD — ao determinar que:

Considerando (39) (...) A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica.

Artigo 5.º Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

(...)

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (“limitação da conservação”);

Verificou-se, portanto, que o conjunto de obrigações e condutas sobre as quais devem se pautar os agentes de tratamento é extensa, apresentando tanto um conjunto de parâmetros gerais que devem ser observados, como os princípios da finalidade, consentimento, adequação, transparência, dentre outros; quanto responsabilidades específicas, como a apresentação de relatórios de impacto, entre outros. Assim, diante da dificuldade de perpassar pormenorizadamente por cada uma das obrigações legais, optou-se por realizar a análise dos normativos sob uma perspectiva geral.

Com a finalidade de aprofundar essa análise, realizar-se-á, no próximo tópico, estudo de dois casos que foram julgados ou discutidos nas duas jurisdições analisadas, buscando apontar como essas obrigações se traduzem na prática e qual o papel da autoridade na fiscalização e observância destas.

2. Estudos de Caso

Com a finalidade de melhor aprofundar o estudo sobre as obrigações dos agentes de tratamento ante aos comandos e diretrizes da Lei Geral de Proteção de Dados e do Regulamento Geral sobre a Proteção de Dados, principalmente diante da necessidade de transparência desse tratamento, o presente tópico se ocupará da análise de dois casos práticos envolvendo a política de privacidade de uma mesma empresa: WhatsApp Inc. (“WhatsApp”).

A escolha pelos casos se deu com o intuito de traçar um paralelo consistente entre os contextos analisados, buscando, tanto quanto possível, explorar condutas semelhantes sob o escopo das duas jurisdições. Para tal, optou-se por comparar possíveis violações às obrigações legais dos agentes de tratamento de dados por parte da empresa WhatsApp segundo apontaram as investigações pela Autoridade Nacional de Proteção de Dados (ANPD), no Brasil, e pelo *Irish Data Protection Commission* (DPC), principal responsável por supervisionar as atividades do grupo Facebook no âmbito da União Europeia.

Cabe apontar que atualmente a Política de Privacidade vigente na União Europeia, Estados Unidos e Canadá é distinta dos demais países, uma vez que o provimento é realizado por diferentes subsidiárias: WhatsApp Ireland na Europa e WhatsApp LLC no Brasil (ANPD, 2021), por exemplo. Em que pese pontuais divergências entre as políticas, o escopo maior do tratamento de dados diante das políticas de privacidade permite realizar a comparação pretendida.

2.1. *Irish Data Protection Commission v. Facebook Ireland Limited*: Ausência de transparência na política do WhatsApp

Em 2018, o *Data Protection Commission* (DPC) iniciou uma investigação contra o WhatsApp a fim de verificar o cumprimento das obrigações de transparência em sua política de privacidade, especialmente no que tange à prestação de informações suficientes acerca de como os dados dos titulares eram processados. A investigação não foi vinculada a nenhuma denúncia, de forma que, definindo seus próprios parâmetros de investigação, o DPC buscou determinar se as ações do Facebook Ireland Ltd. (controladora do WhatsApp) no que se referem à transferência de dados pessoais de indivíduos da União Europeia eram legítimas e legais.

Em consonância com a discussão travada no tópico anterior acerca de controladores e processadores/operadores, o DPC reservou uma sessão na decisão final para definir em qual dessas categorias se enquadrava o WhatsApp quando do processamento de dados pessoais. Entendeu a autoridade que apenas o WhatsApp teria tomado todas as decisões relacionadas aos aspectos centrais do processamento de dados de não-usuários, bem como seria ele o único que poderia implementar alguma modificação no referido processamento, seja por novo código ou por emendas aos termos e condições de serviço, configurando-se, portanto, como um controlador (DPC, 2021).

A partir da definição acerca do tipo de agente de tratamento, o DPC pôde analisar quais obrigações específicas do controlador estariam sendo ou não cumpridas pela empresa. Assim, a investigação foi dividida em três principais seções: (i) transparência no contexto de não usuários; (ii) transparência no contexto de usuários; (iii) transparência no contexto de compartilhamento de dados pessoais entre o WhatsApp e as empresas pertencentes ao grupo Facebook.

Pautando-se na obrigação de transparência, a investigação entendeu que, quando há coleta de dados pessoais, é obrigação do agente de tratamento providenciar informações acerca do processamento desses dados, havendo "um requisito cumulativo, que resulta nos artigos 13 (1) (c) e 13 (1) (d) operando em conjunto para aplicar ao controlador de dados um requisito para estabelecer os objetivos do processamento em relação à base jurídica do legítimo interesse, juntamente com os interesses legítimos perseguidos na realização das operações de tratamento" (EDPB, 2021, p. 11).

O DPC indicou haver diversas violações ao RGPD, principalmente aos artigos de 12 a 14, isto é, violações aos direitos dos titulares de dados. Entendeu o departamento irlandês que a questão estava atrelada diretamente à autonomia individual do titular em compartilhar os seus dados pessoais, de modo que “se as informações necessárias não foram fornecidas, o titular dos dados foi privado da capacidade de tomar uma decisão totalmente informada sobre se deseja ou não se tornar um usuário do Serviço” (DPC, 2021, p. 203). O princípio da transparência é aqui tomado como o fundamento para um regulamentar o tratamento de dados, não apenas porque reforça outros princípios, como o da *accountability*, mas também porque é dele que grande parte das obrigações do RGPD derivam (DPC, 2021).

Ademais, ao analisar se havia intenção (dolo) ou negligência (culpa) na conduta do WhatsApp, embora essa classificação não exista no RGPD — mas apenas nas “*Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*”—, o DPC apontou que o WhatsApp já havia sido alvo de outra investigação realizada em conjunto entre o “*Office of the Privacy Commissioner of Canada*” (OCO) e a autoridade de proteção de dados da Holanda em 2012. Considerando, então, que as mesmas violações foram apontadas nas duas investigações, o DPC entendeu que o WhatsApp possuía conhecimento de que estaria infringindo as obrigações delineadas no RGPD.

Diante das irregularidades verificadas, o DPC determinou a condenação do WhatsApp, indicando que a empresa teria deixado de cumprir com as obrigações dos artigos 13, (1), (c), (d), (e) e (f), 12 (1), 13 (2), (a), (c), e (e) do RGPD, que tratam principalmente da obrigação de transparência. O caso acabou sendo alçado para a alta corte europeia, quando foi confirmada a regularidade da investigação que reconheceu existência de ilegalidades no tratamento de dados realizado pelo WhatsApp, culminando na condenação em 225 milhões de euros em multa (HIGH COURT, 2021).

Não obstante, o WhatsApp informou que, desde então, diversas atualizações foram feitas na política de privacidade (BBC, 2021). Uma das alterações mencionadas pelo WhatsApp diz respeito a uma atualização geral na Política de Privacidade que ocorreu em todas as regiões do globo em que a plataforma opera. Importa frisar que, como apontou a própria Autoridade Nacional de Proteção de Dados (2021a), em razão da vigência do RGPD, a atualização que ocorreu nos países da União Europeia foi significativamente diferente da que tomou lugar no Brasil. Tais diferenças se deram essencialmente quanto à base legal para o tratamento de dados, à forma como ocorre esse tratamento de dados e à disposição de como exercer os direitos do

titular, todas essas obrigações dos agentes de tratamento que foram incluídas na política de privacidade europeia, mas não tiveram correspondentes no Brasil.

Em que pese a grande influência do RGPD na legislação de proteção de dados brasileira, tais disposições não parecem ter sido observadas no caso em questão. A fim de melhor explorar os pontos que foram deixados de fora da política de privacidade do WhatsApp no Brasil, bem como discutir quais são as obrigações dos agentes de tratamento no âmbito da LGPD a partir de uma das primeiras manifestações da ANPD, parte-se para a análise da Nota Técnica nº 02/2021/CGTP/ANPD, na qual são realizados apontamentos técnicos da autoridade acerca da referida política.

2.2. Nota Técnica nº 02/2021/CGTP/ANPD: Política de Privacidade do WhatsApp em face das obrigações definidas pela LGPD

Em janeiro de 2021, o Whatsapp notificou seus usuários acerca de atualizações na sua Política de Privacidade e Termos de Serviço, que seriam implementadas a partir de 15.05.2021. Em razão da grande base de dados a qual tem acesso, principalmente considerando fazer parte do grupo econômico do Facebook (com o qual compartilha metadados desde 2016), as alterações na política do WhatsApp geraram forte repercussão nacional e internacional (ANPD, 2021a).

Nesse contexto, a ANPD acompanhou de perto essa atualização, solicitando informações adicionais e realizando reuniões com as representantes da empresa e outros órgãos públicos. Assim, a referida autoridade elaborou dois documentos, a Nota Técnica nº 02/2021 e a Recomendação Conjunta, nos quais são apresentadas recomendações de adequação da Política de Privacidade do WhatsApp à LGPD, orientando e esclarecendo quais seriam os direitos dos usuários nesse cenário (BRASIL, 2021b).

No decorrer da Nota Técnica nº 02/2021 e também na Recomendação Conjunta, a Autoridade Nacional de Proteção de Dados, em colaboração com o Ministério Público, Conselho Administrativo de Defesa Econômica e Ministério da Justiça e Segurança Pública, fez apontamentos importantes sobre o enquadramento do tratamento de dados realizado pela empresa na recém promulgada Lei Geral de Proteção de Dados, dando um importante direcionamento para verificar como essa autoridade se colocará diante das obrigações dos

agentes de tratamento de dados. Por essa razão, serão aqui analisados os principais pontos tratados nas duas manifestações.

Diferentemente, porém, do que ocorreu no âmbito da União Europeia, importa frisar que quando essa Nota Técnica foi formulada pela ANPD, as sanções administrativas (arts. 52 a 54) ainda não estavam em vigor, conforme determinação do art. 65, I-A, da LGPD. Desse modo, o objeto do processo administrativo não foi apurar a ocorrência de infrações, mas sim balizar a atuação de um importante agente de tratamento de dados, uma vez que as demais obrigações constantes na LGPD não se submetiam ao período de *vacatio legis*. Dessas obrigações, a Nota Técnica nº 02/2021 ressalta:

Normas relativas a indicação de base legal adequada para o tratamento de dados pessoais (arts. 7º, 8º, 10, 11 e 33), à transparência na relação entre os agentes de tratamento e titulares (art. 6º, IV e VI; art. 9º), à adoção de medidas de prevenção e segurança (arts. 6º, VII e VIII; arts. 46 a 51) e à garantia de direitos dos titulares (arts. 17 a 22), inclusive de crianças e adolescentes (art. 14). (ANPD, 2021, p. 4)

Assim, diante das obrigações elencadas na LGPD, a referida autoridade discorreu sobre alguns pontos que levantaram preocupações na nova política de privacidade, dentre os quais, evidenciou os seguintes: tratamento de dados realizado pela empresa desde 2016; as novas práticas de compartilhamento em razão do uso da ferramenta WhatsApp Business, que permite que o conteúdo de mensagens e dados de usuários saiam do domínio do WhatsApp e entrem em domínio de terceiros; e o compartilhamento de dados de usuários de seu aplicativo com a plataforma do Facebook.

A fim de instruir o processo, a ANPD (2021a) requisitou uma série de esclarecimentos acerca do compartilhamento de dados, sendo possível inferir quais as principais áreas de preocupação no tratamento de dados e merecem maior atenção pelos agentes de tratamento. São elas: (i) tipos de dados compartilhados; (ii) informações adicionais sobre os agentes de tratamento com os quais os dados são compartilhados; (iii) fonte dos dados pessoais; (iv) forma de armazenamento e compartilhamento; (v) finalidade do compartilhamento e do tratamento de dados subsequente realizado pelos agentes com os quais os dados são compartilhados; (vi) base legal da LGPD que autoriza o compartilhamento dos dados pessoais; (vii) justificativa para a aplicação da referida base legal; (viii) forma de obtenção e de armazenamento de consentimento; (ix) forma e consequências da recusa de concessão de consentimento pelos titulares dos dados pessoais compartilhados; (x) forma de concessão dos direitos determinados

no art. 18 da LGPD, aos titulares em relação ao compartilhamento de dados pessoais; (xi) mecanismos de segurança adotados para o compartilhamento.

Apontou a ANPD que a nova política de privacidade do WhatsApp padece de algumas irregularidades perante a LGPD, principalmente ao retirar da sua política de privacidade a possibilidade de restrição de compartilhamento dos dados com as empresas da família Facebook, seja para a finalidade de anúncios ou outra correlata; não apresentar informações suficientes quanto à dupla coleta de informação do lado do usuário e empresa; não informar com clareza quanto à coleta de dados de localização; não trazer as bases legais nas quais se embasam as finalidades do tratamento; e omitir questões de compartilhamento de dados que constavam na política de privacidade anterior.

Ao comparar a Política de Privacidade da empresa no Brasil e na União Europeia, a ANPD também notou um descompasso importante acerca das obrigações firmadas. Dentre essas, destacam-se as seguintes seções que restaram presentes na União Europeia, mas ausentes na política brasileira, apesar de constarem previsões na LGPD: (i) “Como tratamos seus dados”, obrigação que consta no art. 10, § 2º da LGPD; (ii) “Nossa base legal para tratar dados”, adequando-se ao disposto no art. 7º da LGPD; (iii) “Como exercer seus direitos”, conforme dispõe o art. 18 da LGPD.

Nesse contexto, a ANPD utiliza o princípio da transparência como elemento-chave para a análise efetuada na Nota Técnica. Para tal, traçou um paralelo com caso julgado pela *Commission Nationale l’Informatique et des Libertés* (CNIL) — autoridade francesa de proteção de dados — que condenou o Google, entre outras empresas, pela ausência de informações acessíveis aos usuários ou, quando presentes, havendo dificuldade de acessá-las, desconformidade com o RGPD; finalidades descritas de forma genérica e vaga; falta de clareza na base legal; e ausência de informação sobre o período de retenção de dados. Assim, seria somente com a transparência que “os titulares poderão [poderiam] exercer a chamada autodeterminação informacional e exercer seus direitos, em especial o de livre acesso” (ANPD, 2021a, p. 21).

Isso porque, embora o WhatsApp afirmasse que a atualização garantiria a transparência do processamento de dados, existem alguns requisitos para que realmente possa se considerar um tratamento de dados transparente que não foram devidamente cumpridos, como: informação clara, precisa e facilmente acessível. A autoridade aponta, entre outras considerações, que a análise de precisão e clareza da informação no Brasil deve considerar a cultura de privacidade

do país, o que, por ainda não ser amadurecida, dificulta o completo entendimento dos usuários acerca dos riscos envolvidos no tratamento. Tal análise deverá atrelar-se à ponderação do poder do tratamento de dados pessoais quantitativa e qualitativamente, bem como à capacidade de assimilação dos titulares dos novos produtos e serviços apresentados para seu uso. Quanto à facilidade de acesso, indica a importância de as informações sobre privacidade serem destacadas das outras provisões contratuais.

A autoridade apresenta também como importantes parâmetros de análise o princípio da necessidade e o legítimo interesse, pontuando as diferenças entre os dois conceitos. Afirmou a ANPD (2021a) que o legítimo interesse só pode ser justificado se não for sobreposto pelos direitos e liberdades fundamentais do titular, não sendo, portanto, absoluto. Para verificar a sobreposição, é necessário fazer um teste de sopesamento entre as razões para que se verifique se prevalece o legítimo interesse do controlador sobre os direitos do titular no caso concreto, sendo necessária uma interpretação conjunta do princípio da necessidade e do legítimo interesse.

Ao fim, a autoridade teceu diversas recomendações visando a assegurar que o WhatsApp tome as providências necessárias para regularizar a situação, a saber: (i) condução de Relatório de Impacto de Proteção de Dados sobre a integração dos serviços do WhatsApp Business e WhatsApp; (ii) criação de seções na Política de Privacidade que informem aos titulares as bases legais utilizadas e correlacione às finalidades e categorias de dados pessoais tratados; (iii) posição de destaque na Política de Privacidade do link que informa quais dados o WhatsApp compartilha com as Empresas do Facebook, aumentando a transparência do usuário; (iv) inserção na política de privacidade de um novo link que informe “Quais informações o WhatsApp compartilha com as empresas no WhatsApp?”; (v) disponibilização em destaque das informações para que o titular possa exercer seus direitos na própria Política de Privacidade; (vi) inserção de informação sobre o Aviso de Privacidade – Brasil, em seção específica, eliminando uma camada de acesso a informação; (vii) correção dos links disponibilizados no Aviso de Privacidade; (viii) correções quanto a revogação de consentimento ou aceitação; (ix) divulgação pública da identidade do encarregado; (x) acrescentar circunstâncias em que o tratamento de dados sensíveis poderia ocorrer de forma não intencional; (xi) acrescentar operações de tratamento de dados de crianças e adolescentes; (xii) descarte e exclusão seguros de dados; (xiii) implementação de controles administrativos relativos à privacidade da informação; (xiv) implementação *de privacy by design and by default*, para além da criptografia fim-a-fim dos conteúdos das mensagens (ANPD, 2021a).

Considerações Finais

Diante do exposto, restou clara a importância das definições de obrigações dos agentes de tratamento, a fim de balizar a sua conduta e evitar quaisquer tipos de abusos no tratamento de dados. Nesse contexto, com bem aponta o RGPD, “o risco para os direitos e liberdades das pessoas físicas, de probabilidade e gravidade variáveis, pode resultar do processamento de dados pessoais que podem levar a danos físicos, danos materiais ou não materiais, em particular: [...] onde os titulares dos dados possam ser privados dos seus direitos e liberdades ou impedidos de exercer controle sobre seus dados pessoais”.

Da análise dos casos concretos, verificou-se que, embora os deveres dos agentes de tratamento já estejam devidamente estipulados na LGPD, parece haver uma falta de familiaridade dos agentes de tratamento com os dispositivos da lei, em contraposição ao regulamento europeu, que já está consolidado a mais tempo. Em que pese a LGPD tenha previsto a obrigatoriedade de determinação da base legal para o tratamento, os direitos dos titulares e a necessidade de transparência acerca do tratamento de dados, com disposições bastante semelhantes às constantes no RGPD, tais obrigações não foram traduzidas na política de privacidade do WhatsApp, diferentemente do que ocorreu na União Europeia.

Referências bibliográficas

ALVES JR., SÉRGIO. Fechando um ciclo: do término do tratamento de dados pessoais (art. 15 e 16 da LGPD). In. BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Disponível em: Minha Biblioteca, Grupo GEN, 2020.

ANPD, Autoridade Nacional de Proteção de Dados. Nota Técnica nº 02/2021/CGTP/ANPD. Processo nº 00261.000012/2021-04. Assunto Atualização da Política de Privacidade do WhatsApp. Brasília, 22 de mar. 2021a. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos->

[para-link-nas-noticias/NOTATECNICADACGTP.pdf](https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NOTATECNICADACGTP.pdf)

ANPD, Autoridade Nacional de Proteção de Dados. Guia Orientativo para definições dos agentes de tratamento de dados pessoais e encarregado. Brasília/DF, mai. 2021b.

BBC, British Broadcasting Corporation. WhatsApp issued second largest GDPR fine of 225m. Publicado em 2 set. 2021. Disponível em: <https://www.bbc.com/news/technology-58422465>

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. Recomendação Conjunta. Colaboração entre Ministério Público Federal, Conselho Administrativo de Defesa Econômica, Autoridade Nacional de Proteção de Dados e Ministério da Justiça e Segurança Pública. Brasília, 7 de mai. 2021a. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/recomendacao_whatsapp_-_assinada.pdf

BRASIL. ANPD divulga orientações aos usuários sobre a nova política de privacidade do WhatsApp. Publicado em 14 de mai. de 2021b. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/a-nova-politica-de-privacidade-do-whatsapp>

DPC, Data Protection Commission. Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act, 2018 and Articles 60 and 65 of the General Data Protection Regulation. DPC Inquiry Reference: IN-18-12-2, Helen Dixon, Commissioner for Data Protection. Publicado em 20 Ago. 2021. Disponível em: https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, set. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controller_processor_en.pdf

EDPB. Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR. Publicada em 28 jul. 2021. Disponível em [https://edpb.europa.eu/system/files/2021-](https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_w_hatsapp_redacted_en.pdf)

[09/edpb_bindingdecision_202101_ie_sa_w_hatsapp_redacted_en.pdf](https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_w_hatsapp_redacted_en.pdf)

HIGH COURT. European Union. Facebook Ireland Limited v. Data Protection Commission. Judicial Review. 2020 No. 617 Jr; No. 126 COM. Judgement of Mr. Justice David Barniville delivered on the 14th day of May, 2021. Disponível em: <https://www.dataprotection.ie/sites/default/files/uploads/2021-08/Facebook%20v.%20DPC%20Judgment%2014.5.21.pdf>

MENEZES, Joyceane Bezerra; COLAÇO, Hian Silva. Capítulo 6: Quando a Lei Geral de Proteção de dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1. ed. - São Paulo: Thomson Reuters Brasil, 2019.

PECK, Patrícia. Proteção de dados pessoais. Disponível em: Minha Biblioteca, (2nd edição). Editora Saraiva, 2020.

VIOLA, Mario; DE TEFFÊ, Chiara Spadaccini. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11º. In: BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Disponível em: Minha Biblioteca, Grupo GEN, 2020.

WP29. Opinion 1/2010 on the concepts of "controller" and "processor". Adotado em 16 fev. de 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

