

— 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 CONSENTIMENTO VÁLIDO NA INTERPRETAÇÃO DO RGPD E DA LGPD: UMA ANÁLISE ENTRE AS SIMILITUDES E DISPARIDADES ENTRE AMBAS AS LEGISLAÇÕES

Isabela de Araújo Santos¹

Dispositivos da LGPD	Dispositivos do RGPD
Art. 5º Para os fins desta Lei, considera-se: (...) XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (...)	Artigo 4º - Definições Para os fins deste Regulamento, entende-se por: (...) (11) “consentimento” do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento; (...)

Introdução

Em um Estado Democrático de Direito, a regulação jurídica do tratamento de dados pessoais está amparada na ideia de que o indivíduo deve usufruir de autodeterminação informacional, ou seja, “deve ter o poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de livre desenvolvimento de sua personalidade” (MENDES, 2014, p. 60).

Logo, para que o indivíduo consiga exercer seu poder de autodeterminação informativa, torna-se necessário um instituto jurídico pelo qual possa expressar sua vontade de autorizar ou não o processamento e tratamento de seus dados pessoais: o consentimento (MENDES, 2014).

Veremos, no presente artigo, que diversas são as situações envolvendo o consentimento dos titulares de dados no contexto europeu e no brasileiro. O primeiro caso que será analisado é o “Processo C-61/19”, que consiste em um acórdão do Tribunal de Justiça da União Europeia (TJUE) cujas justificativas do julgamento elucidam muito bem a definição de consentimento válido sob a luz da legislação europeia. O segundo caso a ser apresentado será o acórdão de um Agravo de Instrumento julgado pelo Tribunal de Justiça do Distrito Federal (TJDFT), do qual

¹ Bacharela em Direito pela Universidade de Brasília e atuante na área de proteção de dados pessoais e análise regulatória de novas tecnologias na Bioni Consultoria.

poderemos extrair a importância dada pela Lei Geral de Proteção de Dados (LGPD) brasileira ao consentimento dos titulares de dados.

Ademais, insta salientar que o Guia (*Guidelines*) de nº 5 do *European Data Protection Board* (EDPB) trata, minuciosamente, da importância do consentimento como alicerce de garantia ao direito à proteção de dados, além de determinar critérios para sua utilização como base legal adequada para o tratamento de dados pessoais. A Lei Geral de Proteção de Dados, por sua vez, também apresenta requisitos específicos para utilização do consentimento dos titulares, de modo que se coaduna a diversos dispositivos do *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados - RGPD), divergindo, todavia, sutilmente em certos pontos, como veremos adiante.

1. Estudos de Caso

Passemos, desta feita, à análise dos casos europeu e brasileiro, a fim de esmiuçar os aspectos relevantes para a definição de consentimento válido em cada uma das respectivas legislações.

1.1. Case C-61/19 - TJUE

O primeiro caso a ser avaliado no presente artigo é o processo C-69/19, julgado pelo TJUE em 11 de novembro de 2020. Trata-se de um pedido de decisão prejudicial apresentado pela empresa Orange România S.A. - que presta serviços de telecomunicações móveis no mercado romeno - contra a Autoridade Nacional de Supervisão de Tratamento de Dados Pessoais da Romênia (ANSPDCP), que havia aplicado multa à empresa por ter recolhido e conservado cópias de títulos de identidade dos seus clientes, sem o consentimento válido destes, tendo a autoridade lhe ordenado que destruísse essas cópias (UNIÃO EUROPEIA, 2020b).

A condenação à pena pecuniária foi aplicada com fundamento na Diretiva 95/46 da União Europeia, que estabelece, em seu artigo 2º, alínea 'h', que o consentimento somente será considerado válido se for uma manifestação de vontade livre, específica e informada, por meio da qual o titular aceita que seus dados pessoais sejam objeto de tratamento. Ademais, a Diretiva ainda preconiza, em seu artigo 10, que os Estados-Membros da União Europeia devem estabelecer que os responsáveis pelo tratamento dos dados forneçam aos titulares pelo menos as seguintes informações:

- i) identidade do responsável pelo tratamento e, eventualmente, do seu representante;
- ii) finalidades do tratamento a que os dados se destinam;
- iii) outras informações, tais como: os destinatários ou categorias de destinatários dos dados, ou a existência do direito de acesso aos dados que lhe digam respeito e do direito de os retificar, desde que sejam necessários, tendo em conta as circunstâncias específicas da obtenção dos dados, para garantir aos titulares um tratamento adequado de suas informações.

Ademais, a ANSPDCP justificou a aplicação da multa à Orange România com base nos artigos 32 e 42 do Regulamento 2016/679 - cuja vigência revogou a Diretiva 95/46 -, que enunciam, dentre outras hipóteses, os requisitos para a verificação do consentimento válido dos titulares de dados. Tal consentimento válido, segundo os dispositivos citados do Regulamento 2016/679, deve ser obtido mediante um **ato positivo claro** que indique uma manifestação de **vontade livre, específica, informada e inequívoca** de que o titular de dados consente ao tratamento dos dados que lhe digam respeito, como, por exemplo, mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral.

Logo, sob a égide da legislação europeia, sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento autorizado e do seu alcance.

Após verificar que os preceitos e pré-requisitos de tratamento de dados pela base legal do consentimento coadunavam-se explicitamente com a legislação europeia, o TJUE concluiu, no presente caso, que **os clientes não validaram seu consentimento livremente**, uma vez que a Orange România havia recolhido cópias das carteiras de identidades de clientes que não teriam autorizado validamente o tratamento de tais informações, bem como obteve o consentimento dos clientes estritamente por meio de cláusula contratual relativa à conservação de cópias dos atos que continham dados pessoais para fins de identificação.

Isso porque **o simples fato de a cláusula contratual ter sido validada não demonstraria uma manifestação positiva do consentimento** desses clientes para que fosse recolhida e conservada uma cópia do seu documento de identidade. Afinal, não há como demonstrar que essa cláusula foi efetivamente lida e, muito menos, entendida por esses titulares em seu conteúdo e alcance.

Ademais, torna-se importante destacar que caberia ao próprio responsável pelo tratamento dos dados - no caso, a Orange România - provar que os titulares dos dados manifestaram seu consentimento por ação livre e inequívoca. Igualmente, também caberia à empresa demonstrar previamente que foram disponibilizadas informações a respeito de todas as circunstâncias relacionadas com esse tratamento, de modo inteligível e de fácil acesso e numa linguagem clara e simples - o que não ocorreu na situação narrada.

Por essas razões, o pedido da Orange România foi negado pelo TJUE, tendo sido mantida a decisão de primeiro grau, bem como a multa aplicada pela ANSPDCP.

1.2. Agravo de Instrumento nº 0749765-29.2020.8.07.0000 - TJDFT

O TJDFT julgou, em 01 de junho de 2021, uma situação similar ao Processo C-61/19, no que tange à definição do consentimento válido e em que momento esse consentimento deve ser requerido, de acordo com as respectivas legislações.

No caso, o Ministério Público do Distrito Federal e Territórios (MPDFT) interpôs agravo de instrumento contra decisão de primeiro grau que havia indeferido concessão de tutela de urgência a fim de suspender a comercialização, por parte da SERASA S.A., de dados pessoais de titulares por intermédio de produtos inscritos em serviços de “Lista Online” e “Prospecção de Clientes”.

O MPDFT afirmou que a empresa estaria comercializando os dados de milhões de brasileiros - tais como sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagem de risco - por meio desses serviços. O custo do serviço girava em torno de R\$ 0,98 por indivíduo e exigiria um universo de 150.000.000,00 de CPFs, demonstrando claramente que a situação se configuraria como um grande incidente de segurança monetizável ou mesmo um vazamento de dados.

Desta feita, o TJDFT entendeu que a atitude por parte da SERASA S.A. iria de encontro com a LGPD, uma vez que esse diploma normativo impõe a necessidade de manifestação específica para cada uma das finalidades para as quais os dados estão sendo tratados. Por essa razão, o compartilhamento dos dados, na forma como realizado pela empresa, seria ilegal e desrespeitaria o direito à privacidade dos cidadãos brasileiros - como disposto no artigo 5º, inciso X, da Constituição Federal brasileira -, assim como feriria seus direitos à intimidade,

privacidade e honra dos titulares dos dados - como estabelecido no artigo 2º, incisos I e IV da LGPD.

O Tribunal ainda acrescentou que, em relação aos dados pessoais sensíveis - que também estiveram envolvidos no caso em questão -, de acordo com o artigo 11 da LGPD, em seu inciso I, o tratamento somente é cabível com o consentimento do titular ou responsável, manifestado de forma específica e destacada, ressalvadas hipóteses excepcionais, descritas no inciso II, em que é dispensado o consentimento do titular.

Ademais, **diferentemente do que alegava a empresa, o fato de a LGPD dar tratamento específico aos dados sensíveis não exclui a proteção aos demais dados pessoais, conforme se extrai da interpretação do artigo 7º da LGPD.** Não haveria como considerar, portanto, a situação fática apresentada como uma hipótese de dispensa do consentimento, pois **não seria um caso de legítimo interesse da empresa** - preconizado no inciso IX do referido artigo -, **muito menos de compartilhamento de dados com finalidade de proteção ao crédito** - como explicita o inciso X do artigo 7º.

Segundo o TJDFT, a interpretação que se extrai do art. 7º, da LGPD, portanto, é a de que **o consentimento pelo titular é a regra principal a ser observada para o tratamento de dados pessoais**, “tanto é que o § 4º, daquele dispositivo, prescreve textualmente - de forma a evitar dúvidas interpretativas - a dispensa do consentimento apenas para os dados tornados manifestamente públicos pelo titular” (DISTRITO FEDERAL E TERRITÓRIOS, 2021).

Portanto, para os dados não sensíveis, o controlador que, nos termos da lei, tenha interesse e legitimidade, deveria, de igual forma, obter o consentimento dos titulares, ressalvada a hipótese de dados tornados manifestamente públicos pelo titular - o que não se verifica na situação em análise, por não se tratar de hipótese meramente cadastral, mas, sim, comercial.

O Tribunal, destarte, considerou ilícito o compartilhamento de dados realizados pela SERASA S.A., determinando a suspensão da comercialização de dados pessoais pela empresa por meio de produtos por “Lista Online” e “Prospecção de Clientes”, além de ter aplicado uma multa no valor de R\$ 5.000,00 por venda efetuada.

2. Legislação europeia e brasileira: o consentimento dos titulares de dados pessoais

Tendo em vista os julgamentos relatados, é possível relacioná-los com outras questões importantes relativas aos direitos de titulares de dados em ambos os ordenamentos jurídicos mencionados.

No primeiro momento, será examinado o RGPD e suas nuances a respeito da base legal do consentimento, bem como será mencionado o Guia de nº 5 do *European Data Protection Board*, que originaram o entendimento no que tange ao consentimento contido no regulamento, para, em seguida, realizarmos uma análise da legislação brasileira. Com isso, a partir de uma perspectiva comparada, será possível identificarmos as diferenças e semelhanças da posição adotada por cada legislação quanto à base legal do consentimento dos titulares de dados pessoais.

2.1. O Regulamento Geral sobre a Proteção de Dados europeu

Assim como a Diretiva 95/46 e o Regulamento 2016/679, o Guia de nº 5 do *European Data Protection Board*, de 4 de maio de 2020, estabelece uma análise da noção do consentimento no Regulamento Geral sobre a Proteção de Dados da União Europeia, focando nas mudanças dessa concepção desde a publicação no “Opinion 15/2011” publicado pelo extinto Article 29 Working Party.

Segundo o referido Guias, passou a ser obrigação dos controladores de dados a descoberta de novas soluções de operação com observância de parâmetros legais a respeito da proteção de dados pessoais e do interesse dos seus fornecedores.

De acordo com o artigo 6(1) do RGPD, o consentimento é uma das seis bases legais para o tratamento de dados pessoais:

Artigo 6. Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

(a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

(b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

(c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

- (d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- (e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- (f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. (UNIÃO EUROPEIA, 2016a) - (grifos nossos)

Ademais, o artigo 4(11) do RGPD define o consentimento como “uma manifestação livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento” (UNIÃO EUROPEIA, 2016b).

Desta feita, para que se entenda plenamente como o consentimento deve ser aplicado sob a ótica do RGPD, devemos analisar cada elemento que caracteriza sua validade: a necessidade de ele ser dado livremente, de ser específico, de ser informado e de ser fornecido explicitamente por ato positivo claro e inequívoco.

2.1.1. O consentimento livre

O elemento da liberdade, no contexto da proteção de dados, implica a real possibilidade de escolha e de controle do titular sobre seus dados. Logo, se houver qualquer tipo de pressão ou coação para a concessão desse consentimento, sob pena de consequências negativas exageradas, o consentimento não será tido como lícito.

Além disso, a relação entre o controlador e o titular de dados é considerada desequilibrada, principalmente quando esse controlador é uma autoridade pública ou em contexto laboral entre empregado e empregador. Nesses casos, pode-se discutir a inadequação do consentimento como base legal a ser utilizada para fundamentar o tratamento de dados pessoais, tendo em conta essa assimetria de poder relacional.

Desse modo, para que o consentimento seja efetivamente livre, não pode estar vinculado a nenhum tipo de empacotamento (*bundling*) com aceitação de termos ou condições, nem a nenhuma amarração (*tying*) com previsões contratuais ou serviços que não sejam necessários para a plena eficácia contratual. Ou seja, as bases legais do consentimento e do contrato não

podem, de maneira alguma, serem confundidas, pois isso limitaria a liberdade de escolha dos titulares de dados.

Logo, é necessária uma vinculação objetiva entre o processamento de dados e o propósito de execução do contrato. Um exemplo em que não há respeito a essa conexão de finalidade contratual seria a situação hipotética de um aplicativo de edição de foto requer, ao seu usuário ou à sua usuária, o acesso a sua geolocalização, sem dar a opção a esses usuários de não consentir com esse fornecimento de informação para usufruir de seu serviço. Considerando que a geolocalização não é um dado necessário para a edição de fotos – finalidade a que o aplicativo se propõe –, torna-se ilícito o consentimento dado pelos usuários, a partir do momento em que se constata que o consentimento não foi fornecido livremente (UNIÃO EUROPEIA, 2020a).

Outrossim, insta salientar que, quando um serviço envolve múltiplos processamentos de dados para mais de um fim, há a necessidade de que o titular e eventual fornecedor dos dados possa escolher quais dados ele permite serem processados, em vez de terem de consentir por todo um pacote de dados para diversos propósitos. O consentimento deve ser dado para cada um deles, devendo haver, portanto, **granularidade**.

Um caso que exemplifica claramente uma situação não granular de consentimento é a situação em que uma loja pede o consentimento dos seus clientes cadastrados para fornecer dados a fim de enviar-lhes, por e-mail, as ofertas do mês e, concomitantemente, para divulgar esses mesmos dados com outras lojas do mesmo grupo empresarial para finalidades de *marketing*. Considerando que, nessa situação, não houve separação de autorizações para cada finalidade, não houve granularidade no requerimento do consentimento.

Ademais, cabe destacar que, para que o consentimento seja livre, há a necessidade de o controlador de dados demonstrar que o titular pode recusar ou retirar o consentimento sem detrimento algum, ou seja, sem nenhum custo ou desvantagem. Algumas situações que podem configurar detrimento são: intimidação, coerção ou qualquer outro tipo de consequência negativa para o titular e eventual fornecedor dos dados.

2.1.2. *O consentimento específico*

Além de livre, o consentimento válido deve ser específico e, para que isso ocorra, a noção de granularidade tem suma relevância novamente: o controlador deve separar informações a fim de determinar especificamente os propósitos para os quais pretende tratar aqueles dados.

Essa exigência de especificidade do uso dos dados coletados tem como objetivo evitar a ocorrência do fenômeno denominado de *function creep*, isto é, quando nossos dados são usados para um fim diferente daquele originalmente justificado. Isso faz com que os controladores que desejem obter consentimento de coleta de dados para vários diferentes propósitos devam proporcionar aos titulares opções *opt-in* separadas para cada um desses fins aos quais serão destinados esses dados.

Por fim, já que os controladores devem fornecer informações específicas sobre a finalidade do tratamento dos dados, isso já indica também para a necessidade de que o consentimento seja informado, como outro pressuposto de sua validade.

2.1.3. *O consentimento informado*

Para que se configure o consentimento informado, o RGPD elenca, em seu artigo 20 o conjunto mínimo de informações necessárias a serem passadas ao fornecedor de dados, sendo elas (UNIÃO EUROPEIA, 2016a):

- i) a identidade do controlador;
- ii) o propósito de cada operação de processamento;
- iii) que tipo de dados serão coletados e usados;
- iv) a existência do direito de retirada do consentimento;
- v) informações relativas a decisões automatizadas; e
- vi) possíveis riscos concernentes à transferência de dados.

Portanto, pode-se constatar que o RGPD não prescreve a forma pela qual as informações mínimas devem ser veiculadas, de modo que a informação sobre o consentimento pode ser alcançada de diversas maneiras, como, por exemplo, por declarações escritas ou orais, por mensagens de vídeos ou por áudios.

Todavia, independentemente da forma veiculada, essa informação deve apresentar uma linguagem clara e compreensível para todas as pessoas. E, se por um acaso, esse controlador

visa a obter consentimento de titulares que são responsáveis por crianças, pessoas analfabetas, ou portadoras de deficiências auditivas e/ou visuais, por exemplo, ele deve adequar a linguagem da informação veiculada para que seja compreensível para o respectivo público.

2.1.4. *O consentimento explícito por ato positivo claro e inequívoco*

O consentimento ainda requer um ato positivo claro e inequívoco que não demonstre, de maneira alguma, ambiguidade. Isso significa que o fornecedor deve ter consentido por meio de uma ação afirmativa, que pode ter sido obtida por diversos meios - escritos, orais, inclusive eletrônicos.

Logo, o silêncio ou a mera falta de manifestação do titular de dados não podem ser considerados formas de obtenção do consentimento. Contudo, os controladores ainda têm a liberdade de obter o consentimento por meios alternativos, a exemplo de movimentos físicos dos titulares, desde que estes sejam qualificados como atos afirmativos.

Um possível exemplo de manifestação de consentimento por movimento físico é ilustrado na situação em que, em um aplicativo de *delivery*, como iFood e Uber Eats, para permitir o acesso à geolocalização, o usuário ou a usuária tenha de clicar o dedo sobre a tela do aparelho móvel para fornecer esse consentimento de maneira explícita.

Contudo, de maneira a obter o consentimento explícito propriamente dito, é necessária a configuração de situações em que há claro risco de falha na proteção de dados dos titulares. O Guia de nº 5 do EDPB elencam duas hipóteses mais usuais: na transferência internacional de dados e na automatização de decisões, incluindo casos de *profiling* (perfilização).

Logo, o termo “explícito” refere-se ao modo como o titular expressou seu consentimento: ele deve explicitá-lo normalmente por meio de uma declaração escrita para que seja evitada potencial dúvida futura quanto à validade daquele consentimento. Porém, é fato que hoje temos outros meios de obtê-lo, a exemplo de preenchimento de formulário online, envio de e-mail, escaneamento de documento assinado ou assinando-o eletronicamente.

2.1.5. *Condições adicionais para a obtenção de consentimento válido segundo o RGPD*

Cumpra ainda frisar que há uma obrigação do controlador de dados de demonstrar o consentimento dado pelo titular. O RGPD não diz exatamente como essa demonstração deve ser feita, contudo, é fato que há esse ônus da prova do controlador evidenciado nas Diretrizes de nº 5 (UNIÃO EUROPEIA, 2020a).

Ademais, o RGPD não estabelece uma regra de tempo de duração do consentimento, pois isso dependeria do contexto e da finalidade aos quais a coleta de dados se propôs a cumprir. Quando essa finalidade acaba, os dados devem ser, a princípio, deletados.

Em relação à revogação do consentimento, vale apontar ainda que o RGPD não faz menção se a obtenção e a retirada devem ser feitas pela mesma ação. Todavia, se o consentimento foi obtido, por exemplo, por meio eletrônico, como deslizando a tela do celular, a retirada dele deve ser realizada por um meio e por uma ação de igual facilidade e acessibilidade.

O EDPB ainda menciona, nessa diretiva, a situação atribuída às crianças: os menores de dezesseis anos só poderão dar seu consentimento sob autorização de seus responsáveis, exceto se o controlador de dados for autoridade pública, o que autorizaria o menor a partir dos 13 anos a fornecer esses dados livremente, sem prévia autorização.

Por fim, as Diretrizes de nº 5 esclarecem que, quando os dados são coletados para fins de pesquisa, a especificidade e a granularidade podem ser flexibilizadas. Porém, isso não significa que não deve haver transparência por parte do controlador e do operador dos dados. Logo, como forma de proteção dos titulares, os controladores são incentivados a se utilizar de ferramentas, como a anonimização e a minimização, para que os direitos desses fornecedores de dados sejam resguardados ao máximo.

2.2. **Entendimentos atuais da LGPD no que concerne o consentimento dos titulares**

O consentimento na Lei Geral de Proteção de Dados Brasileira é interpretado de maneira semelhante ao do Regulamento Geral sobre a Proteção de Dados Europeu, embora possua suas particularidades, a serem elucidadas nesta seção.

Em seu artigo 5º, inciso XII, a LGPD define o consentimento como uma “**manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados

“pessoais para uma finalidade determinada” - grifos nossos (BRASIL, 2018). Assim, o consentimento pode ser considerado, em certa medida, um processo de tomada de decisão do titular de dados. Em adição, em seu artigo 7º, o consentimento é elencado como uma das dez bases legais para o tratamento de dados (BRASIL, 2018):

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - Mediante o fornecimento de consentimento pelo titular; (...)

Ademais, a LGPD, em seu artigo 8º, estabelece que o consentimento deverá ser fornecido por escrito ou por qualquer outro meio que demonstre a manifestação de vontade do titular; e, caso seja fornecido por escrito, deverá constar de cláusula destacada das demais cláusulas contratuais.

A legislação brasileira, assim como a europeia, estabelece que cabe ao controlador de dados o ônus da prova de que o consentimento foi obtido dentro dos limites legais. Outra semelhança com o RGPD seria a de que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Outrossim, a LGPD declara vedado o tratamento de dados pessoais mediante vício de consentimento, além de considerar que o consentimento deve referir-se a finalidades determinadas, sendo tidas como nulas as autorizações genéricas para o tratamento de dados.

O artigo 9º da LGPD, ademais, enuncia o direito que o titular de dados tem ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva para atendimento do princípio do livre acesso.

Dentre as informações sobre o tratamento dos dados, estão inclusas (BRASIL, 2018):

- i) finalidade específica do tratamento;
- ii) forma e duração do tratamento, observados os segredos comercial e industrial;
- iii) identificação do controlador;
- iv) informações de contato do controlador;

- v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- vi) responsabilidades dos agentes que realizarão o tratamento; e
- vii) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Insta salientar ainda que, no §1º do art. 9º, da LGPD é estabelecido que, caso as informações fornecidas ao titular, quando o consentimento for requerido, tenham conteúdo abusivo ou enganoso ou não tenham sido previamente apresentadas com transparência, de forma clara e inequívoca, o consentimento será considerado nulo.

Contudo, na prática, esses pré-requisitos de validade do consentimento na LGPD, assim como no RGPD, podem se deparar com alguns contratempos quando observa-se a realidade dos titulares de dados, afinal muitos usuários de aplicativos, sites e plataformas digitais nem ao menos leem os termos de política de privacidade e de uso dos respectivos controladores e, quando o fazem, acabam por não entender a linguagem técnica desses termos. “Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja não desfrutar de importantes produtos e serviços online. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais (...)” (MENDES; FONSECA, 2020, p. 352).

“Por isso, a disciplina do consentimento não deve ser tratada sob viés negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão.” (TEPEDINO; FRAZÃO; OLIVA, p. 48). Logo, pode-se inferir que nada adianta uma base legal prevista em lei se não há de fato um livre fluxo informacional e uma real autonomia dos titulares de dados pessoais. Até porque, como bem elucida Bruno Bioni:

O ser humano não é uma ilha, ele se conforma e se desenvolve quando se relaciona com os demais “no seio da sociedade que o abriga”. Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade (BIONI, 2019, p. 83).

Ainda sobre o tema Bioni enfatiza que:

Trata-se, portanto, de se afastar de uma estratégia regulatória puramente liberal, que é incoerente com a posição de vulnerabilidade do sujeito em causa. Necessário se faz uma maior intervenção, seja do ponto de vista do desenho normativo ou da formulação

de políticas públicas em *lato sensu* para que se **empodere o sujeito vulnerável e, por outro lado, que não se foque apenas na instrumentalização do controle dos dados pessoais** a ponto de se pensar em uma normatização substantiva da privacidade informacional. (BIONI, 2019, p. 166) - (grifos nossos)

No caso brasileiro, desta feita, cabe à Autoridade Nacional de Proteção de Dados (ANPD) garantir a observância da autodeterminação informativa dos cidadãos, de modo a promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais. Além disso, a ANPD torna-se responsável por estimular a adoção de uma padronização de conduta por parte dos fornecedores de serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados e, conseqüentemente, faça haver a observância de um consentimento livre, informado, inequívoco e expresso - como bem preceitua a LGPD.

Considerações Finais

A partir da análise dos casos e dos dispositivos legais apresentados neste artigo, observa-se que a legislação europeia somente considera como livre o consentimento em que há a possibilidade de escolha por parte do titular de dados ou se o titular puder revogá-lo, sem prejuízo para si de ordem contratual e consumerista.

Em contrapartida, na LGPD, o consentimento será considerado válido se as informações apresentadas pelo controlador de dados não estiverem eivadas de conteúdo enganoso e se forem mostradas de forma clara, transparente e inequívoca.

Os casos aqui elucidados ilustram e exemplificam as delimitações das definições do consentimento trazidas por cada legislação, europeia e brasileira. De todo modo, vê-se uma clara tentativa nas duas legislações de garantia da autodeterminação informacional dos titulares de dados, a partir do momento em que se empenham em proporcionar aos indivíduos meios de exercerem essa autodeterminação por meio de seu empoderamento autorizativo frente ao tratamento e processamento de dados pessoais.

As legislações analisadas vão ao encontro, portanto, da visão do professor Danilo Doneda (2016, p. 410), no sentido de que a adoção da solução de mercado para o problema dos dados não é adequada, diante da multiplicidade de situações e interesses a eles relacionadas, que não se limitam a vetores patrimoniais.

Nesse cenário, torna-se de suma relevância compreender que a crença de que o ser humano é um sujeito completamente racional, dotado da capacidade de desempenhar um processo de verdadeira tomada decisória a fim de controlar seus dados pessoais é ameaçada por toda a complexidade envolvida no fluxo dessas informações. O titular de dados, na realidade, encontra-se em uma situação de vulnerabilidade perante os controladores, visto que há uma evidente relação assimétrica de poder entre quem disponibiliza e quem obtém esses dados (BIONI, 2019, p. 147).

Isso porque, por fim, devemos lembrar que o consentimento não é a única base legal capaz de assegurar a autodeterminação informativa dos indivíduos em um Estado Democrático de Direito, devendo haver uma conjugação de princípios e dispositivos legais favoráveis aos titulares de dados, a fim de que seu direito à proteção de dados seja devidamente observado e respeitado.

Referências bibliográficas

BIONI, B.R. Proteção de Dados Pessoais. A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

BRASIL, Lei nº 13.709, de 14 ago. 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm >, Acesso em 07 dez. 2020.

DISTRITO FEDERAL E TERRITÓRIOS. Tribunal de Justiça. Agravo de instrumento n. 0749765-29.2020.8.07.0000. Antecipação de tutela recursal. Ação Civil pública. Comercialização de cadastro de dados pessoais. Lei Geral de Proteção de Dados Pessoais. Consentimento do titular. Relator: César Loyola. Brasília, 01 de junho de 2021. Disponível em: < <https://tj-df.jusbrasil.com.br/jurisprudencia/1223323853/7497652920208070000-df-0749765-2920208070000/inteiro-teor-1223324034> > Acesso em 18 set 2021.

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

MENDES, L.S. Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

MENDES, L.S.; FONSECA, G.C.S. da. Proteção de Dados Para Além do Consentimento: Tendências de Materialização. In: BIONI, Bruno Ricardo; DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz (org.). Tratado de proteção de dados pessoais. São Paulo: Gen-Forense, 2020.

TEPEDINO, G; FRAZÃO, A; OLIVA, M.D. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Revista dos Tribunais, 2019.

UNIÃO EUROPEIA. Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020a. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt>, Acesso em: 7 dez. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça. *Reenvio Prejudicial. Processo C-61/19*. Diretiva 95/46/CE. Tratamento de dados pessoais e proteção da vida privada. Recolhimento e conservação das cópias de títulos de identidade por um prestador de serviços de telecomunicações móveis. Conceito de consentimento. Manifestação de vontade livre, específica e informada. Relator: T. von Danwitz, 2020b. Disponível em:

<
<https://curia.europa.eu/juris/document/document.jsf?jsessionid=016DCA915515F41082B5259E51BAEE93?text=&docid=233544&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=6980149> >.

Acesso em 18 set 2021.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

