DOI: 10.33242/rbdc.2020.03.005

O CONSENTIMENTO NA CIRCULAÇÃO DE DADOS PESSOAIS

CONSENT TO THE PROCESSING OF PERSONAL DATA

Gustavo Tepedino

Professor Titular de Direito Civil e Ex-Diretor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ). Doutor em Direito Civil pela Universidade de Camerino (Itália). Livre-Docente pela Faculdade de Direito da UERJ. Presidente do Instituto Brasileiro de Direito Civil (IBDCivil). Advogado. Consultor e Parecerista em Direito Privado.

Chiara Spadaccini de Teffé

Doutoranda e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Atualmente, é Professora de Direito Civil e de Direito e Tecnologia na Faculdade de Direito do IBMEC. Leciona também em cursos do Ceped-UERJ, na Pós-Graduação da PUC-Rio, na EMERJ, no Instituto New Law, no ITS Rio e na Pós-Graduação em Advocacia Contratual e Responsabilidade Civil da Ebradi. Membro do Conselho Executivo da revista eletrônica *Civilistica.com*. Coordenadora da disciplina Direito e Internet no Instituto New Law. Membro do Fórum Permanente de Mídia e Liberdade de Expressão da EMERJ. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Consultora em Proteção de Dados Pessoais e Advogada.

Resumo: Com base na recente Lei Geral de Proteção de Dados brasileira, no presente artigo visa-se analisar o consentimento do titular dos dados, base legal de grande relevância para o tratamento de informações pessoais. Para tanto, será realizado o estudo das normas gerais para a expressão do consentimento válido e eficaz, sua caracterização e relação com os direitos do titular. Em seguida, passa-se para a estrutura protetiva desenvolvida em termos de dados sensíveis e, por fim, para a norma relativa ao tratamento de dados pessoais de crianças e adolescentes, com ênfase nas disposições relativas ao consentimento para o tratamento dessas informações. A partir do tema proposto, busca-se levantar indagações e avaliar possibilidades de aplicação da LGPD, sempre em favor da pessoa humana e de suas situações existenciais.

Palavras-chave: Proteção de dados pessoais. Consentimento do titular. Tratamento de dados pessoais. Privacidade. Dignidade da pessoa humana.

Abstract: This article aims to analyze the Brazilian General Data Protection Law, from an approach based on the consent of the data subject, a relevant legal basis for the processing of personal information. To this end, we have developed a study focusing on the general rules for the expression of valid and effective consent and the relationship between the consent and the rights of the data subject. Then, we analyzed the protective structure developed for sensitive data and the legal standard for the processing of personal data of children and adolescents, with emphasis on the provisions on consent for the processing of such information. In this study, we seek to raise questions and evaluate possibilities of application of the LGPD, always in favor of the human person and the existential situations.

Keywords: Protection of personal data. Data subject's consent. Processing of personal data. Privacy. Human dignity.

Sumário: **1** Introdução: a Lei Geral de Proteção de Dados Pessoais – **2** O consentimento para o tratamento de dados – **3** Dados sensíveis: requisição de consentimento específico e destacado – **4** O tratamento de dados pessoais de crianças e adolescentes – **5** Considerações finais

1 Introdução: a Lei Geral de Proteção de Dados Pessoais

A cada minuto, uma infinidade de dados é extraída, transferida e organizada de forma incalculável. Cadastros em lojas, *logins* em *sites* e a utilização de mídias sociais e aplicativos de transporte fornecem dados pessoais a diversos destinatários, públicos e privados, sem que muitas vezes seja possível ao titular controlar a finalidade da utilização de suas informações, quem realizará o tratamento e por quanto tempo. Dados genéticos, preferências culturais, estéticas e de consumo, orientações políticas ou religiosas e opção sexual: tudo é coletado em tempo real e nos mais variados meios. Tais informações relacionam-se diretamente com os direitos da personalidade e afetam as liberdades fundamentais do ser humano, devendo ser protegidas de forma destacada e contextualizada com o desenvolvimento tecnológico.

Por isso mesmo, com relação à tutela dos dados, o direito deve ocupar-se tanto de aspectos preventivos – valorizando a autonomia dos interessados para decidir a respeito da disponibilidade de suas informações e impondo deveres aos agentes – quanto de aspectos ressarcitórios – atinentes à violação da privacidade e dos dados pessoais e à consequente reparação dos danos individuais ou coletivos causados. A proteção dos dados relativos à pessoa natural mostra-se hoje vital para que ela se realize integralmente e se relacione em sociedade, representando garantia de maior segurança às informações e impedindo práticas autoritárias e de vigilância em massa.

O desenvolvimento de mecanismos destinados a regular o tratamento dos dados auxilia a evitar discriminações que não encontrem fundamento constitucional, como aquelas que possam dificultar o acesso ao crédito ou a empregos por determinados grupos ainda marginalizados. Além disso, afasta práticas que possam prejudicar a liberdade dos indivíduos, como exemplo, decisões a partir de análises de dados não informadas ao titular e sob critérios não transparentes. A depender da forma como os algoritmos são programados, as bases de dados selecionadas e os processos estabelecidos e valorados, o resultado pode ampliar assimetrias, preconceitos e desigualdades.[1]

[1] Cf. NOBLE, Safiya Umoja. *Algorithms of oppression*: how search engines reinforce racism. Nova York: NYU Press, 2018.

No Brasil, até agosto de 2018, não se dispunha de lei específica para a proteção dos dados pessoais. Sua tutela era pleiteada com base em determinadas previsões estabelecidas na Constituição Federal e em algumas normas setoriais,[2] que direta ou indiretamente tratam de questões relacionadas à privacidade e aos dados pessoais, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e a Lei do Cadastro Positivo. Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às partes, o que, além de gerar insegurança jurídica, acabava tornando o país menos competitivo no contexto de uma sociedade cada vez mais movida a dados.[3]

Com base na recente Lei Geral de Proteção de Dados (Lei nº 13.709/18 – LGPD), no presente artigo visa-se analisar o consentimento do titular dos dados, base legal de grande relevância para o tratamento de informações pessoais. Para tanto, será realizado o estudo das normas relativas à expressão do consentimento válido voltado ao tratamento de dados pessoais. Em seguida, passa-se para a estrutura protetiva desenvolvida em termos de dados sensíveis e, por fim, para a norma relativa ao tratamento de dados pessoais de crianças e adolescentes, com ênfase na disposição acerca do consentimento para o tratamento dessas informações. A partir do tema proposto, busca-se levantar indagações e avaliar possibilidades de interpretação e aplicação da LGPD, sempre em favor da pessoa humana e de suas situações existenciais. Adicionalmente, serão realizados alguns paralelos entre a LGPD e o Regulamento Europeu de Proteção de Dados 2016/679 (*General Data Protection Regulation* – GDPR).

Diante do desenvolvimento de tecnologias cada vez mais sofisticadas para o tratamento de dados, da maior aplicação da inteligência artificial em sistemas e processos e da ampliação da capacidade de armazenamento de informações, mostrou-se urgente a edição e atualização de legislações (em âmbito nacional, regional e internacional) que visem a tratar de maneira mais específica a temática aqui desenvolvida, especialmente no que tange aos dados sensíveis e aos dados de crianças e adolescentes.

[2] MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *Jota*, 14 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 28 dez. 2018.

[3] "Com a entrada em vigor da Lei Geral de Proteção de Dados, muito se questiona sobre a situação de tais leis de proteção de dados no Brasil. Nesse cenário, a LGPD pode ser vista como uma diretiva geral para a proteção de dados no Brasil. Isso significa que a nova lei busca não substituir as que existem atualmente, mas estabelecer regras e princípios gerais para que as mesmas possam ser cumpridas de uma maneira mais benéfica para os titulares dos dados pessoais" (MONTEIRO, Renato Leite *et al*. Manual normativo: Lei Geral de Proteção de Dados e GDPR. *Baptista Luz Advogados*, 30 jan. 2019. p. 16. Disponível em: https://baptistaluz.com.br/institucional/manual-normativo-lei-geral-de-protecao-de-dados-e-gdpr/?fbclid=IwAR0UIsvjzeGTaAC2_iHspgcDDaBA1jyGXjFn2N1-cgywGF62kozYKwoRt3U. Acesso em: 2 fev. 2019).

A tecnologia expande o alcance da memória humana, registrando o paradeiro, o itinerário, as referências geográficas e biométricas, a origem e o destino de cada um, bem como as pessoas com quem se estabelece qualquer tipo de relacionamento, as preferências de consumo, as idiossincrasias. Para a melhor tutela dos direitos fundamentais, há que se definir quando, onde, como e para que fins poderão ser colhidas informações pessoais, devendo ser estabelecidas restrições para o seu tratamento, tendo em vista especialmente os valores estratégico e comercial que elas detêm.[4]

Nas últimas décadas, a privacidade vem sendo compreendida também como o direito de manter controle sobre as próprias informações,[5] passando a fazer referência à possibilidade de a pessoa natural conhecer, controlar, endereçar e, até mesmo, interromper o fluxo das informações a ela relacionadas. Abriu-se, assim, espaço para a chamada autodeterminação informativa, que representa a faculdade de o particular controlar a obtenção, a titularidade, o tratamento e a transmissão de seus dados.

Nessa perspectiva, a atenção voltou a se dirigir para o consentimento dos interessados, admitindo-se a evolução do consentimento implícito (situação em que se entende que a pessoa consentiu em razão de sua própria conduta) para o consentimento informado, o qual orienta inclusive normas relativas à circulação de informações, "visto que se manifesta em uma série de disposições que prescrevem quais devem ser as informações fornecidas ao interessado para que seu consentimento seja validamente expresso".[6] No momento atual, o consentimento informado vem ganhando cada vez mais prestígio, por tornar o usuário participante ativo no processo de consentimento.

Nessa esteira, não se mostra mais suficiente, para proteger a privacidade, a garantia de não ingerência alvitrada por Warren e Brandeis, em seu *right to be left alone*, do final do século XIX. A identificação da privacidade como autodeterminação informativa demonstra que a liberdade, em especial nas relações existenciais, não implica ausência do direito, mas, ao contrário, pressupõe que o direito atue de maneira a proteger a parte mais vulnerável, fornecendo-lhe meios para efetivamente poder discernir, decidir e agir. O oferecimento aos cidadãos de instrumentos que lhes garantam assumir efetivamente controle sobre o uso e a integridade

[4] Para uma análise mais profunda do tema, permita-se remeter a TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. 4. ed. Rio de Janeiro: Renovar, 2008. p. 25-62.

[5] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 92.

[6] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 75.

de suas informações representa garantia de liberdade e igualdade, tendo em vista o papel predominante da informação para as escolhas do ser humano.[7]

A Lei Geral de Proteção de Dados brasileira e o Regulamento Europeu sobre a Proteção de Dados[8] representam no contexto atual instrumentos para a proteção e garantia da pessoa humana, uma vez que facilitam o controle dos dados tratados, impõem deveres e responsabilidades aos agentes de tratamento e proporcionam segurança à circulação de informações. Os dois sistemas encontram-se fortemente alinhados, como desejou o legislador brasileiro, para que a norma nacional, nos próximos anos, seja reconhecida como adequada ao sistema europeu, uma vez que isso facilitará a realização de transações e cooperações com países do bloco. Na América Latina,[9] apenas Argentina e Uruguai até o momento conseguiram tal reconhecimento.[10] [11]

---

7 "A excessiva liberdade suscitada pelas tecnologias na sociedade contemporânea apresenta faces antagônicas. Em primeiro lugar, avulta o aspecto emancipador da liberdade, traduzido nas extraordinárias possibilidades oferecidas ao usuário dos engenhos eletrônicos e das redes sociais; da cibernética e dos meios de comunicação. A volta ao mundo sem deslocamento físico é usualmente anunciada, assim como corriqueiros *conference calls*, videoconferências, acessos a bibliotecas de todos os continentes a partir de uma única base. O acesso à informação mostra-se o bem mais valioso ao exercício da cidadania. De outra parte, contudo, tem-se a feição hostil dos engenhos eletrônicos, manifestada pela interferência excessiva e reiterada na esfera privada. O controle dos dados pessoais, especialmente aqueles considerados sensíveis, cujo tratamento pode dar azo à discriminação do seu titular, transmuda-se em ameaça real à liberdade individual" (TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v. 419, p. 77-96, 2014).

8 No dia 25.5.2018, o GDPR entrou em vigor. Apesar de ser uma norma da União Europeia, ela apresenta eficácia e aplicação extraterritorial. Por essa razão, por exemplo, muitas empresas nacionais que têm filiais na Europa ou oferecem serviços a pessoas localizadas no continente tiveram que se adaptar, sob pena de severas sanções ou de perderem contratos. A norma cria também obstáculos para a transferência internacional de dados pessoais para países que não sejam considerados detentores de um nível adequado de proteção.

9 Na América do Sul, Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai e Guiana Francesa também possuem leis gerais para a proteção dos dados dos titulares. Na Argentina, a Lei de Proteção de Dados Pessoais foi aprovada em 2000 (Lei nº 25.326 de 2000). No Uruguai, a Lei nº 18.331, que trata da proteção de dados pessoais e da ação de *habeas data*, está publicada desde o ano de 2008.

10 "The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection. The adoption of an adequacy decision involves a proposal from the European Commission; an opinion of the European Data Protection Board; an approval from representatives of EU countries; the adoption of the decision by the European Commission. At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data". Até agora, a Comissão Europeia reconheceu Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroe, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça e Uruguai, por exemplo, como fornecendo proteção adequada (EUROPEAN COMMISSION. *Adequacy decisions*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 1º ago. 2020).

11 No dia 16.7.2020, o Tribunal Superior de Justiça da União Europeia invalidou o *Privacy Shield*, protocolo de compartilhamento de dados que permitia às empresas norte-americanas transferir informações pessoais

Diante de tal circunstância, foi estabelecido modelo legislativo no Brasil que privilegia a prevenção de danos à pessoa humana e a segurança no tratamento de dados pessoais, instituindo deveres e responsabilidades específicas aos agentes,[12] além de amplo rol de princípios e direitos aos titulares dos dados. Busca-se antecipar os riscos de violação à privacidade, como também evitar tratamentos abusivos de informações e vazamentos de dados.[13] Nessa direção, adverte a doutrina, à luz do regime implementado pela recente lei, que a proteção dos dados pessoais pode, inclusive, ser vislumbrada atualmente como direito fundamental autônomo, figurando a privacidade apenas como uma de suas referências axiológicas no regime instituído pela LGPD.[14]

Foram incorporados e positivados, assim como ocorreu no Regulamento europeu,[15] os pilares da chamada proteção da privacidade e dos dados pessoais

sobre os cidadãos da UE aos EUA para processamento de dados. O tribunal alega que o regulamento não pode ser confiável, pois não protege os cidadãos da UE dos programas de vigilância em massa operados por agências de inteligência dos EUA, como a Agência de Segurança Nacional. A decisão traz efeitos para várias empresas americanas, mas impactará particularmente as empresas de tecnologia e mídia social que processam grandes quantidades de dados pessoais, exatamente as informações que a UE deseja proteger (COURT OF JUSTICE OF THE EUROPEAN UNION. *Judgment in Case C-311/18*. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf. Acesso em: 5 ago. 2020).

[12] O caráter preventivo da LGPD é lembrado, por exemplo, nos seguintes dispositivos: art. 6º, II, VI, VII, VIII e X; art. 44; art. 46; art. 47; art. 48; art. 49; e art. 50.

[13] Recomenda-se a leitura de estudo da IBM, em colaboração com o Instituto Ponemon, intitulado *2018 Cost of a Data Breach Study: Global Overview* (Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 2 fev. 2019). No ano de 2018, foram noticiados graves casos de vazamento de dados em empresas, instituições e serviços, como: Google+, C&A, Uber, Sky Brasil, FIESP, Stone Pagamentos, Banco Inter, Buscapé, Netshoes, Marriott, Facebook e Twitter (PAYÃO, Felipe. Hackerspectiva de 2018: vazamento de dados foi ponto alarmante. *Tecmundo*, 20 dez. 2018. Disponível em: https://www.tecmundo.com.br/seguranca/137353-hackerspectiva-2018-vazamento-dados-ponto-alarmante.htm. Acesso em: 2 fev. 2019).

[14] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 99-130. Afirma a autora: "seja em razão do amplo alcance da LGPD, seja em razão da sua preocupação com a tutela das situações existenciais dos titulares de dados, pode-se dizer que foi acolhida concepção convergente com a daqueles que, a exemplo de Rodotà, sustentam que a proteção de dados corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante" (p. 103).

[15] Art. 25 GDPR – "Data protection by design and by default. 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by

por *design* e por padrão (*by default*). A partir desses paradigmas, entende-se que a proteção dos dados deve ser pensada desde a concepção do produto ou serviço disponibilizado, devendo ser implementadas medidas técnicas e organizacionais que assegurem a tutela dos direitos do titular. Há de se obter a garantia de que os dados pessoais serão processados com a mais alta proteção da privacidade (por exemplo, apenas os dados necessários devem ser tratados; o período de armazenamento deve ser curto; e o acesso aos dados deve ser limitado), de forma que os dados sejam automaticamente (como padrão) protegidos em qualquer sistema de TI ou prática de negócios. Atua-se, assim, no sentido de incorporar fortes medidas de segurança ao ciclo dos dados, para se garantir o gerenciamento seguro das informações do começo ao fim. Seja qual for a prática ou tecnologia envolvida, ela deverá levar em conta, em primeiro lugar, os interesses dos titulares dos dados e operar de acordo com as promessas e objetivos declarados, estando sujeita inclusive à verificação independente.[16]

A lei brasileira parte do pressuposto de que todo dado pessoal é importante, conferindo especial proteção a determinadas informações do ser humano. Por essa razão, adotou conceito amplo de dado pessoal: "informação relacionada a pessoa natural identificada ou identificável".[17] Dados que pareçam não relevantes em determinado momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados e/ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela. Diante do cuidado com o tema, foi estabelecido como regra geral (art. 1º) que qualquer pessoa que trate dados, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada nos meios digitais, deverá ter uma base legal para fundamentar sua atividade.

Vive-se em ambiente marcado por elevada assimetria informacional: uma parte, geralmente grandes empresas e Estados, detém mais poder, recursos e melhores informações do que a outra, o cidadão comum, por vezes consumidor

default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article" (Disponível em: https://gdpr-info.eu/art-25-gdpr/. Acesso em: 2 fev. 2019).

[16] Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 27 dez. 2018.

[17] A disposição brasileira segue o previsto no GDPR: "Artigo 4º Definições. Para efeitos do presente regulamento, entende-se por: «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; [...]".

nas relações desenvolvidas. Esse cenário enseja diversos questionamentos acerca, por exemplo, da validade do consentimento do titular dos dados nos contratos celebrados, principalmente quando eles são de adesão. Tal assimetria informacional não se revela apenas no poder que o agente dispõe sobre os dados pessoais de terceiros, mas também nas novas modalidades de negócio, em que informações pessoais de seus usuários representam uma das bases centrais do sistema desenvolvido.[18]

A posição de destaque que o tratamento de dados tem em muitos produtos e serviços oferecidos ao público por empresas de tecnologia – as quais, por vezes, não exigem remuneração direta dos usuários, mas o preenchimento de cadastro, a criação de perfil e/ou o acesso aos contatos e mensagens trocadas –[19] revela a importância fundamental dos dados na criação, desenvolvimento e manutenção de diversos modelos de negócio da Web 3.0. Exemplos significativos são as mídias sociais[20] e as ferramentas de intermediação de compra e venda *on-line* e transporte privado de passageiros.

[18] À vista disso, e antes da elaboração da lei em comento, em outra sede já se difundia o caráter essencial de uma lei geral de proteção de dados pessoais como nova face da privacidade. Na ocasião, declarou-se que "as relações existenciais, afetivas, comerciais e profissionais cada vez mais se desenvolvem por meios informatizados – para os quais é imprescindível o fornecimento de informações pessoais. Por isso, franquear ao cidadão brasileiro instrumentos de efetivo controle sobre o uso e a integridade de suas informações torna-se mecanismo de garantia da liberdade, tendo em conta o papel predominante da informação para as escolhas individuais" (TEPEDINO, Gustavo; DONEDA, Danilo. A outra face da liberdade. *O Globo*, 15 jun. 2010. Disponível em: https://oglobo.globo.com/in/a-outra-face-da-liberdade-2993811. Acesso: 12 fev. 2019).

[19] Entende-se que a relação entre os usuários das redes sociais e o provedor de aplicações de internet responsável por elas não seria marcada pela gratuidade, havendo uma situação de remuneração indireta entre as partes, visto que, apesar de o provedor não receber um valor financeiro diretamente de seus usuários, ele seria remunerado diretamente pela publicidade, que tem como público-alvo os usuários da rede, e, indiretamente, pelos próprios usuários, que disponibilizam seus dados pessoais para a empresa, ao criarem perfis, interagirem com outros usuários e postarem conteúdos. Há, portanto, uma estrutura de remuneração capaz de assegurar facilmente a manutenção dessas redes, sem haver qualquer contraprestação financeira direta e imediata por parte de seus usuários. É de conhecimento público que o *marketing* direcionado promovido nas redes sociais vai muito além de *banners* e *links* patrocinados e tem como base o próprio conteúdo inserido pelos usuários (TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil: análise a partir do Marco Civil da Internet. *Pensar*, Fortaleza, v. 22, n. 1, p. 108-146, jan./abr. 2017). Esse raciocínio foi chancelado pela jurisprudência do Superior Tribunal de Justiça: "O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo 'mediante remuneração' contido no art. 3º, §2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor" (STJ, 3ª T. REsp nº 1.193.764. Rel. Min. Nancy Andrighi. *DJe*, 8 ago. 2011).

[20] Tendo-se como exemplo as mídias sociais, sua estrutura revela a necessidade da constante inserção de dados pessoais por parte de seus usuários. É essencial ao negócio a existência de uma massa substancial de usuários, os quais são estimulados a inserir de forma ininterrupta diversas informações sobre si e terceiros. Posteriormente, parte-se para a exploração e monetização dos dados inseridos no sistema, por meio, por exemplo, da venda de espaços para publicidade e anúncios, do desenvolvimento de perfis para o direcionamento de produtos e informações e da possibilidade de acesso aos dados de seus usuários por parte de parceiros comerciais.

Por essa razão, recomenda-se a escolha de canais seguros, que façam uso de boas práticas e informem com clareza o uso de dados pessoais. Além disso, cada pessoa deve realizar a gestão de sua identidade e privacidade *on-line*, avaliando que tipo de dados deseja expor ao público, bem como verificar cuidadosamente as configurações de privacidade de aplicativos e programas para personalizá-las e reduzir a coleta e o armazenamento de dados.

Nesse ambiente, algumas organizações vêm enxergando na proteção de dados vantagem competitiva dentro da gestão de sua reputação. O cuidado com a privacidade e as informações pessoais dos clientes passa a ser apresentado como elemento adicional ao serviço prestado e diferencial da empresa em termos de segurança e prevenção de riscos. Além disso, verifica-se por parte de algumas empresas maior investimento em tecnologia, seguros e capacitação de pessoal para lidarem melhor com questões relativas a dados. Como já apontado,[21] o ambiente regulatório é composto não apenas por normas jurídicas, identificando-se um conjunto de elementos relevantes a influenciar e moldar condutas.

Entende-se que a evolução funcional dos bens jurídicos exige a separação das lógicas patrimonial e existencial. O direito à proteção de dados apresenta relação direta com a tutela da personalidade, e não da propriedade,[22] de forma que sua proteção deverá ser colocada em posição de preeminência, quando em conflito com questões patrimoniais. Assim, também, certas categorias de dados, especialmente os de natureza médica e genética, não deverão ser utilizados para fins meramente negociais.[23]

Mostra-se útil, nessa esteira, a invocação do que se tem designado como razoável expectativa de privacidade, a ser construída caso a caso, como meio de

[21] LESSIG, Lawrence. The law of the horse: what cyberlaw might teach. *Harvard Law Review*, n. 113, p. 501-549, 1999. Disponível em: https://cyber.harvard.edu/works/lessig/finalhls.pdf. Acesso em: 13 out. 2018.

[22] "A proteção de dados pessoais é tema de fundamental importância na sociedade da informação, à medida que cresce o grau de exposição dos indivíduos e sua sujeição a estruturas tecnológicas pertencentes a empresas que não somente guardam, mas exploram comercialmente tais dados. Mostra-se, nesse sentido, nova dimensão do direito fundamental à privacidade, sendo possível ir além para se afirmar que a proteção de dados consiste propriamente em um novo direito fundamental a ser reconhecido. (p. 306) [...] o âmbito de proteção do direito fundamental à proteção de dados pessoais pode ser vislumbrado em uma dimensão subjetiva, na qual o direito se constitui como um direito subjetivo de defesa contra os riscos que ameaçam a personalidade do indivíduo em face da coleta, processamento, utilização e circulação dos dados pessoais; e uma dimensão objetiva, consubstanciada no dever de proteção estatal que decorre da garantia individual de controle dos fluxos de dados (p. 310)" (FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de. Os gigantes da internet e a apropriação e exploração de dados pessoais: direitos fundamentais e direito ao esquecimento digital. *In*: VERONESE, Alexandre *et al* (Org.). *A efetividade do direito em face do poder dos gigantes da internet*: diálogos acadêmicos entre o Brasil e a França. Belo Horizonte: Fórum, 2018. v. 1. p. 303-342).

[23] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 19.

proteção da pessoa humana e incentivo à lealdade recíproca e mútua confiança nas relações. Todavia, a adoção do critério da legítima expectativa somente se justifica se a ponderação conseguir se desprender da lógica proprietária que, tradicionalmente, acaba por associar a liberdade existencial à prerrogativa de se murar contra agressões alheias ou interferências externas.

A defesa da privacidade e dos dados pessoais deve integrar os controles individuais e coletivos de proteção aos direitos fundamentais. Quando se controla o tratamento de informações pessoais, não se resguarda apenas o indivíduo cujos dados estão relacionados, mas também o grupo social do qual ele faz parte, interesses coletivos e as futuras gerações. Nesse sentido, entende-se que também às coletividades devem ser garantidos meios jurídicos, técnicos e sociais que aumentem seu poder e controle sobre os dados.

O impacto da LGPD será efetivo nos mais diversos setores da sociedade, trazendo direitos aos titulares e deveres e responsabilidades aos agentes de tratamento.[24] Todos os sujeitos terão que se adaptar à nova cultura de tutela dos dados pessoais, cabendo especialmente à doutrina, ao Judiciário e à Autoridade Nacional de Proteção de Dados harmonizarem a interpretação e aplicação da lei.

2 O consentimento para o tratamento de dados

A base legal do consentimento para o tratamento de dados do titular representa instrumento de autodeterminação e livre construção da esfera privada. Permite diferentes escolhas e configurações em ferramentas tecnológicas, o que pode ter reflexos diretos na personalidade do indivíduo. Ainda que represente figura de grande relevância nas leis de dados, o consentimento não é, contudo, a única hipótese para o tratamento de dados pessoais nem é hierarquicamente superior às demais bases legais dispostas nos arts. 7º e 11 da Lei nº 13.709/18.

Uma análise minuciosa dos princípios da LGPD – que têm grande parte de seu centro gravitacional baseado na tutela integral do ser humano – revela a preocupação da norma com a participação do indivíduo no fluxo de suas informações pessoais.[25] Verifica-se no texto legal cuidadosa caracterização do consentimento, seguindo a linha do GDPR e das normas mais atuais sobre o tema, além de uma

[24] Para análise da responsabilidade civil no âmbito da LGPD, remeta-se a TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do direito civil*: responsabilidade civil. Rio de Janeiro: Forense, 2020. v. 4. p. 245-261.

[25] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 134.

série de disposições que oferecem regramento específico para concretizar, orientar e reforçar o controle dos dados através do consentimento.[26] [27]

No que diz respeito ao tratamento dos dados, ele deverá ocorrer, como regra, de acordo com as hipóteses estabelecidas no art. 7º da LGPD, sendo certo que no caso de dados sensíveis e de dados de crianças e adolescentes foram positivadas normas mais rígidas, conforme se verá adiante. Como restou estabelecido, eventual dispensa da exigência do consentimento não desobrigará os agentes de tratamento das demais obrigações previstas na lei, especialmente da observância dos princípios gerais e dos direitos do titular. Ou seja, as proteções conferidas ao titular permanecem e são de cumprimento obrigatório.

O maior cuidado com o consentimento do titular mostra-se de grande relevância no cenário tecnológico atual, no qual se verifica a coleta em massa de dados pessoais, a mercantilização desses bens por parte de uma série de sujeitos e a ocorrência de situações de pouca transparência no que tange ao tratamento de dados. Diante desse cenário, defende-se que a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida para o tratamento dos dados para outros meios além daqueles pactuados, para momento posterior, para fim ou contexto diverso ou, ainda, para pessoas distintas daquelas informadas ao titular.[28] Além disso, o consentimento deverá ser manifestado pelo titular antes do tratamento da informação.

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular.[29] Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível à proteção do indivíduo e à circulação de informações.[30]

---

[26] Por exemplo, no art. 8º, §§1º e 4º, art. 7º, §6º, e art. 18, §2º.

[27] Cf. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 13 maio 2020.

[28] Nessa direção, já se enfatizou, há três décadas, a importância do consentimento ante as diversas antinomias provenientes do binômio "progresso tecnológico-bem-estar", afirmando-se que: "ao avançar da tecnologia é preciso contrapor novas formas de controles legais preventivos, que tutelam valores existenciais, como é o caso da intimidade. É razoável estabelecer, de já, que o cruzamento de informações pessoais deva ser subordinado à prévia e expressa autorização do interessado" (TEPEDINO, Gustavo. Computador bisbilhoteiro. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. 4. ed. Rio de Janeiro: Renovar, 2008. p. 563 – texto publicado originariamente na página de opinião do *Jornal do Brasil*, em 3.10.1989).

[29] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 377. Para o autor, "a fundamentação deste consentimento reside na possibilidade de autodeterminação em relação aos dados pessoais, e que esta autodeterminação deve o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento".

[30] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 379.

Nessa direção, mostra-se inadequado atribuir natureza negocial ao consentimento, visto que tal entendimento reforçaria o sinalagma entre o consentimento e determinada vantagem econômica obtida por aquele que consente – a reforçar indesejada índole patrimonial e de fomento à utilização de esquemas proprietários para o trato dos dados pessoais.[31]

Segundo a LGPD, o consentimento é caracterizado como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII).

Livre no sentido de o titular poder escolher entre aceitar ou recusar a utilização de seu bem, sem intervenções ou situações que viciem o seu consentimento. Nessa linha, estabeleceu-se que é "vedado o tratamento de dados pessoais mediante vício de consentimento".[32] A respeito dessa característica, mostra-se relevante que se analise eventual assimetria entre as partes e a vulnerabilidade de algum contratante, para se garantir que o consentimento realmente se deu de forma livre, informada e inequívoca.[33] Como observado em doutrina, "deve-se verificar qual é o 'poder de barganha' do cidadão com relação ao tratamento de seus dados pessoais, o que implica considerar quais são as opções do titular com relação ao tipo de dado coletado até os seus possíveis usos".[34]

No sentido de fortalecer o indivíduo, a lei também estabelece que, se o tratamento dos dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos enumerados no art. 18 da lei. Regula-se, assim, a lógica binária das chamadas políticas de

[31] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 379, para o qual "o consentimento para o tratamento de dados pessoais toca diretamente elementos da própria personalidade, porém não dispõe destes elementos. Ele assume mais propriamente as vestes de um ato unilateral, cujo efeito é o de autorizar um determinado tratamento para os dados pessoais, sem estar diretamente vinculado a uma estrutura contratual" (p. 377-378).

[32] Em termos técnicos, a norma teria sido mais harmônica com o Código Civil se afirmasse que o tratamento de dados pessoais mediante vício de consentimento acarreta anulabilidade (invalidade relativa).

[33] Tratando do GDPR, doutrina afirma que o consentimento tem que ser voluntário e livre: "In order to ensure its voluntariness, consent may not serve as legal basis for data processing where there is a clear imbalance between the data subject and the controller in a specific case. Imbalance is likely in a specific situation where the controller is a public authority. However, the legislator does not explicitly mention other cases of a clear imbalance. Thus, the notion will have to be specified in the future. The legislator deleted the reference to a clear imbalance in the context of an employment relationship as statutory example, which had been included in an earlier draft of the GDPR. Nevertheless, a clear imbalance might still be identified in this context. This will have to be identified on a case-by-case basis" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A practical guide. [s.l.]: Springer, 2017. p. 95).

[34] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 197.

tudo ou nada (*take-it-or-leave-it choice*),[35] em que o usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo.[36]

Não se trata apenas de consentir ou não, mas fundamentalmente da possibilidade de fazê-lo de forma livre, informada e racional, mesmo havendo desequilíbrio de forças entre os contratantes.[37]

Sabe-se que não são todos os sujeitos que têm a habilidade de negociar ou a possibilidade concreta de rejeitar a condição imposta nos termos de serviços e políticas de privacidade das plataformas. Assim, ao invés de realmente concordar com o uso dos próprios dados, o que se verifica na prática é a obediência do titular à vontade das empresas, o que facilita práticas de controle e de uso indiscriminado de dados pessoais.[38] Dessa forma, mostra-se necessário realizar mudanças significativas tanto na maneira pela qual o consentimento é implementado nos termos e políticas, quanto no desenho e arquitetura das plataformas.

Em tal perspectiva, o legislador pretende por meio da LGPD oxigenar processos de tomada de decisão, além de incentivar configurações de privacidade personalizáveis e a possibilidade de manifestação do consentimento de forma granular, podendo o cidadão emitir autorizações fragmentadas no tocante ao fluxo

[35] "On the internet, we encounter many take-it-or-leave-it choices regarding our privacy. Social network sites and email services typically require users to agree to a privacy statement or to terms and conditions – if people do not agree, they cannot use the service. Some websites use a tracking wall, a barrier that visitors can only pass if they agree to tracking by third parties. When confronted with such take-it-or-leave-it choices, many people might click 'I agree' to any request. It is debatable whether people have meaningful control over personal information if they have to consent to tracking to be able to use services or websites. [...] For instance, chat and email services often require users to agree to a data use policy – if people do not agree, they cannot use the service. An app might require access to the camera or the contact list on an end-user's phone, while that access is unnecessary for providing the service. A 'smart' TV might listen to the sounds in people's living rooms, and might only work when people 'consent' to that. Internet of Things equipment may only work if people 'consent' to data collection for marketing" (BORGESIUS, Frederik J. Zuiderveen; KRUIKEMEIER, Sanne; BOERMAN, Sophie C.; HELBERGER, Natali. Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy Regulation. *European Data Protection Law Review*, 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 28 dez. 2018).

[36] "Pode-se adotar todos os argumentos historicamente adotados para criticar a "liberdade" do consentimento, na presença de contextos nos quais existem condicionamentos tais que excluem uma real possibilidade de escolha. [...] o condicionamento deriva do fato de que a possibilidade de usufruir de determinados serviços, essenciais ou importantes, ou tidos como tais, depende não somente do fornecimento de determinadas informações por parte do usuário do serviço, mas também do fato de que tais informações (eventualmente com base no consentimento do interessado) podem posteriormente ser submetidas a outras elaborações. Este é o caso de todos os serviços obtidos através das novas mídias interativas, cujos gestores, por evidentes razões de ordem econômica, estão prontos a exercer forte pressão sobre os usuários para que estes autorizem a elaboração (e a eventual transmissão a terceiros) de 'perfis' pessoais ou familiares baseados nas informações coletadas por ocasião do fornecimento dos serviços" (RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 76).

[37] PEREZ HERNANDEZ, Yolinliztli. Consentimiento sexual: un análisis con perspectiva de género. *Rev. Mex. Sociol*, México, v. 78, n. 4, p. 741-767, 2016.

[38] PEÑA, Paz; VARON, Joana. O poder de dizer NÃO na Internet. *Coding Rights*, 2019. Disponível em: https://medium.com/codingrights/o-poder-de-dizer-não-na-internet-17d6e9889d4a. Acesso em: 29 jul. 2019.

de seus dados: "Abre-se espaço, assim, para que o controle do dados seja fatiado de acordo com cada uma das funcionalidades que são ofertadas e se deseja ter e que demandam, respectivamente, tipos diferentes de dados".[39]

Na mesma linha de raciocínio, pode-se entender que, em alguns casos, o consentimento não será efetivamente livre se não manifestado de modo separado para diferentes operações de tratamento de dados pessoais. A adequação de tal consentimento separado à cada situação dependerá do contexto do processamento dos dados. Doutrina[40] oferece o seguinte exemplo: G administra uma rede social via internet. Para esse propósito, G coleta e armazena dados pessoais. G vende espaço publicitário na página da rede social para terceiros. Como as demais entidades do gênero, ali se realiza publicidade comportamental e, para se inscrever na rede e realizar interações, é necessário que o usuário consinta com o uso de seus dados em tal publicidade.

Entende-se que, dentro da cultura das novas normas de proteção de dados, os usuários devem estar em condições de dar seu consentimento de forma livre e informada em relação ao recebimento de publicidade comportamental, independentemente de seu acesso à rede social. Busca-se que, dentro desses moldes, a própria sociedade exija dos setores público e privado boas práticas institucionais e o cumprimento integral da LGPD. Dessa forma, no caso, G deveria disponibilizar em seu *site* local específico onde constariam informações aos usuários acerca das operações de processamento pretendidas e das opções alternativas. Esse espaço ofereceria aos usuários a possibilidade de selecionar o uso dos dados por eles permitido e deveria informá-los sobre as consequências da recusa do consentimento para certos tipos de atividades de processamento.

O vocábulo *informado* na LGPD significa que o titular do bem tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados. A informação é fator determinante para a expressão de um consentimento livre e consciente, circunscrito, portanto, a certo tratamento, para determinado agente e sob determinadas condições. Para diminuir as assimetrias técnica e informacional existentes entre as partes, exige a lei que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados.

Na lógica do consentimento informado, o art. 9º da LGPD dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados,

[39] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 197-198.

[40] VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A practical guide. [s.l.]: Springer, 2017. p. 97.

que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da: (I) finalidade específica do tratamento; (II) forma e duração do tratamento, observados os segredos comercial e industrial;[41] (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; (VII) e direitos do titular, com menção explícita aos direitos contidos no art. 18.[42]

Na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações.

A manifestação de vontade deve ser também *inequívoca*, ou seja, não ambígua, evidente, e deve ocorrer de forma clara, sendo relevante analisar o grau e a qualidade de interação entre as partes. Aqui, mostra-se relevante analisar a expectativa do titular em uma relação específica.

Por essa razão, termos de uso e políticas de privacidade pré-aceitas, ou seja, já marcadas, não serão consideradas adequadas perante a LGPD, tendo em vista a inação do titular. Da mesma forma, o silêncio não importará no consentimento. Ainda sobre essa qualificação do consentimento, cabe ressaltar que há questionamentos voltados a avaliar se a manifestação do titular de dados poderia se dar de forma tácita, a partir de um comportamento concludente.[43]

A validade do consentimento relaciona-se também com o princípio da finalidade, que dispõe que a realização do tratamento de dados deverá se dar para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[41] "O que precisa ser esclarecido, por ora, é que, com exceção daquilo que possa ser considerado como segredo comercial e industrial, todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, sem o que não restará observado o requisito do consentimento informado" (FRAZÃO, Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. *Jota*, 12 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 2 fev. 2019).

[42] "Art. 8º [...] §6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração".

[43] SOMBRA, Thiago. *Fundamentos da regulação da privacidade e proteção de dados pessoais*. São Paulo: Thomson Reuters Brasil, 2019. p. 137.

Dessa forma, a manifestação deverá referir-se a finalidades determinadas, de modo que autorizações genéricas para o tratamento de dados pessoais serão nulas. A informação é fator determinante para a expressão do consentimento livre e consciente, de forma que se deve destacar a importância do princípio da finalidade para restringir a generalidade na utilização do bem.

A *finalidade da coleta* dos dados deve ser previamente conhecida. O princípio em questão diz respeito à relação entre os dados colhidos e a finalidade perseguida pelo agente, apresentando relação também com o princípio da utilização não abusiva e com a recomendação de eliminação ou transformação em dados anônimos das informações que não sejam mais necessárias.[44] Defende-se também que, a depender do tipo de informação, seria possível desmembrar o consentimento em algumas categorias, com requisitos menos ou mais rígidos, conforme a natureza dos interesses.

O consentimento do titular apresenta-se na LGPD como a primeira possibilidade para a realização do tratamento de dados pessoais (art. 7º, I), sendo que ele, nesse caso, deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular (art. 8º). A lei não exige, portanto, o consentimento escrito, mas, caso assim ele seja colhido, deverá constar em cláusula destacada das demais cláusulas contratuais. Vale lembrar, porém, que, embora não precise necessariamente estar consubstanciado em declaração escrita (podendo, portanto, ser dado de forma oral), o consentimento não poderá ser extraído da omissão do titular, mas tão somente de atos que revelem claramente sua real vontade.[45]

Não se deve confundir a validade do consentimento, especialmente de seus requisitos formais, com a sua prova. Todavia, é aconselhável ao agente de tratamento que tenha registrado em documento escrito o consentimento dado pelo titular. Isso porque, como dispõe o art. 8º, §2º, da LGPD, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na lei, o que é influência direta do princípio da responsabilização e prestação de contas (art. 6º, X).

Para obter o consentimento no ambiente *on-line*, recomenda-se o procedimento de *double opt-in*. Na primeira etapa, o titular dos dados adiciona suas informações nos campos de um *site*, demonstrando seu interesse em receber

[44] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 59.

[45] FRAZÃO, Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. *Jota*, 12 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 2 fev. 2019.

newsletter, comunicados em geral, realizar compras ou consentir com termos de uso, por exemplo. Na segunda, o participante recebe *e-mail* de verificação contendo *link* personalizado que precisa seguir para finalizar seu consentimento, reafirmando pela segunda vez seu interesse em receber tais comunicações. Assim, o controlador pode comprovar que obteve o consentimento do titular dos dados.

Dispõe a lei que o controlador que obteve o consentimento referido no inc. I, do art. 7º, que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta lei. A partir dessa disposição, afirma-se que existiria dever que não se restringiria ao controlador originário, devendo ser observado por todos aqueles que tenham acesso aos dados: dever de verificar a licitude do procedimento de acesso ou compartilhamento, inclusive no que tange ao consentimento do titular.

Outra disposição relevante afirma que o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Defende-se a possibilidade de revogação incondicional desse tipo de consentimento com base na autodeterminação em relação à construção da esfera privada e na proteção da personalidade, que tem entre seus atributos a indisponibilidade. Entretanto, não parece razoável que quem recebeu a autorização para o tratamento dos dados tenha que sofrer risco ilimitado, nem que a revogação se dê em flagrante prejuízo ao interesse público. Em caso de abuso do titular do bem, caberá a devida reparação, que será analisada no caso concreto, podendo o intérprete guiar-se por mecanismos como o *venire contra factum proprium*.[46] Dessa forma, dentro das hipóteses relativas ao término do tratamento dos dados, encontra-se a comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no §5º, do art. 8º, da LGPD,[47] resguardado o interesse público (art. 15, III).

Quanto aos direitos do titular, no que tange ao consentimento, ele tem direito a obter do controlador, em relação aos dados por ele tratados, a qualquer momento e mediante requisição: a eliminação dos dados pessoais tratados com seu consentimento, exceto nas hipóteses previstas no art. 16 da LGPD; informação

[46] Sobre o tema, v., por todos, SCHREIBER, Anderson. *A proibição de comportamento contraditório*: tutela da confiança e venire contra factum proprium. 4. ed. São Paulo: Atlas, 2016.

[47] "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. [...] §5º 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, nos termos do inciso VI do caput do art. 18 desta Lei".

das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento, nos termos do §5º, do art. 8º, da lei. Além disso, quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos da regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

Dispensa o legislador a exigência do consentimento previsto no *caput* do art. 7º para os dados "tornados manifestamente públicos pelo titular", resguardados os direitos do titular e os princípios previstos na norma. Assim como na hipótese dos dados de acesso público,[48] aqui, deve ser considerado o contexto em que a informação foi disponibilizada, bem como haver compatibilidade entre o seu uso e as circunstâncias pelas quais tal informação foi tornada pública, tendo em vista a ressalva disposta na lei, que não autoriza o uso indiscriminado desses dados. Esses tipos de dados, ainda que considerados públicos, não deixam de ser pessoais, sendo necessário considerar sempre a finalidade da circulação e o que justifica sua disponibilização.[49] [50]

[48] "Art. 7º [...] §3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização".

[49] A doutrina oferece exemplos de utilização que esclarecem as possibilidades desses dados: "[...] a princípio, terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de *marketing*. As circunstâncias pelas quais tais dados foram tornados públicos pelo seu próprio titular deram-se para uma outra finalidade, que é a de se relacionar com quem integra o seu círculo social. Por outro lado, a princípio, seria compatível o uso de dados de perfis públicos de uma rede profissional (*e.g.*, Linkedin) por terceiros, como *headhunters*, para aproximar seus usuários às vagas profissionais de seu eventual interesse. Esse uso é compatível com a finalidade não só da plataforma em si, como, principalmente, a razão pela qual tais dados são públicos" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 271).

[50] "[...] afirmou o legislador que o tratamento posterior dos dados pessoais (públicos) a que se referem os §§3º e 4º do Art. 7º poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (§7º). Vale fazer, porém, uma distinção entre as hipóteses do §3º e do §4º do Art. 7º da LGPD. Na hipótese do §4º, pode-se entender que não haveria necessidade de uma nova base legal para o tratamento desses dados, já que se trataria de verdadeira hipótese autorizativa para o tratamento de dados sem o consentimento de seu titular. Já no caso do §3º, o enquadramento em uma das bases legais autorizativas contidas no rol do Art. 7º ou do Art. 11 se mostraria necessário. Entende-se não ser razoável admitir que dados disponíveis publicamente possam ser tratados sem uma base legal específica, pois isso seria o mesmo que autorizar que qualquer informação publicada, por exemplo, por força de uma obrigação legal, pudesse ser utilizada para uma finalidade distinta sem que o novo controlador precisasse demonstrar que existia uma base legal que autorizava o tratamento de tal dado, especialmente quando ele não foi tornado público por seu titular. Tanto é que o referido §3º não dispensa a exigência de consentimento como faz o §4º" (TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 13 maio 2020).

Vale lembrar que a definição positivada na LGPD para consentimento inspira-se na concepção europeia, pois no GDPR se entendeu por consentimento a "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco,[51] que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".[52]

O art. 7º do diploma europeu, ao tratar das condições aplicáveis ao consentimento, afirma que, quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deverá poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento. Se o consentimento do titular for manifestado no contexto de declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deverá ser apresentado de forma a distingui-lo claramente das outras matérias, sendo inteligível, de fácil acesso e em linguagem clara e simples. Quanto à revogação, o titular dos dados tem direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não comprometerá a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados será informado desse fato. De acordo com o Regulamento europeu, a retirada do consentimento deverá ser tão fácil quanto o ato de dar. Foi estabelecido também que, quando se avaliar se o consentimento foi dado livremente, deverá ser verificado com a máxima atenção se a execução do contrato ou a prestação do serviço encontra-se subordinada ao consentimento para o tratamento de dados pessoais não necessários à execução desse contrato.[53]

[51] "The GDPR does not provide for formal requirements as to the consent. Whereas under the former legislative situation some EU Member States' legislation laid down such requirements, consent under the GDPR could be given by oral or written statement, including by electronic means. Nevertheless, written form is advisable regarding the controller's burden of proof. Given its practicability, a lot of entities might opt for obtaining consent by electronic means in the future. In order to be able to demonstrate that valid consent has been obtained, entities will have to protocol the declared electronic consent" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A practical guide. [s.l.]: Springer, 2017. p. 94).

[52] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 2 fev. 2019.

[53] A respeito da revogação do consentimento no GDPR, afirma-se que: "The withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. Thus, its exercise only produces effects for the future. Nevertheless, this data subject's right, which already existed under the Data Protection Directive, will make it more difficult for entities to obtain valid consent as they will have to be prepared for withdrawals at any given moment and, thus, would lose their legal justification for processing. It might be advisable to work around this issue by using another legal basis for processing in addition to the data subject's consent. The controller needs to inform the data subject of its right to withdraw prior to it giving consent, Arts. 7 Sec. 3 phrase 3, 13 Sec. 2 lit. c GDPR. Please note that a violation of the information obligation about the right to withdrawal is punishable with fines of up to EUR 20,000,000.00 or up to 4% of the total worldwide annual turnover, Art. 83 Sec. 5 lit. b GDPR. Furthermore, it shall be as easy to withdraw as to give consent, Art. 7 Sec. 3 phrase 4 GDPR" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A practical guide. [s.l.]: Springer, 2017. p. 97).

Dessa forma, no âmbito do GDPR,[54] o consentimento do titular dos dados deverá ser dado mediante ato positivo claro[55] que indique manifestação de vontade livre, específica, informada e inequívoca de que o titular dos dados consente com o tratamento dos destes, como exemplo, mediante declaração escrita, inclusive em formato eletrônico, ou declaração oral. Segundo o considerando 32 do Regulamento, o consentimento pode ser manifestado mediante validação de opção ao se visitar *site* na internet ou através de outra declaração ou conduta que indique claramente que o titular aceita o tratamento proposto para seus dados pessoais. O silêncio, opções pré-validadas ou a omissão não configuram consentimento.

Dispõe o considerando 42 do GDPR que 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. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados se encontra plenamente ciente do consentimento dado e do seu alcance. Uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de escolha livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.

O considerando 43 do GDPR afirma ainda que, a fim de se assegurar que o consentimento seja dado de livre vontade, ele não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, como exemplo, quando o responsável pelo tratamento for uma autoridade pública, pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.

[54] Acerca do consentimento no GDPR, recomenda-se a seguinte leitura: *Guidelines 05/2020 on consent under Regulation 2016/679*, publicado pelo European Data Protection Board (EDPB) e adotado em 4.5.2020 (Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt. Acesso em: 20 maio 2020).

[55] "In practice, a clear affirmative act of the data subject is required, which could be as follows: – ticking an unticked box when visiting an Internet website; – choosing technical settings for information society services (such as technical settings of an Internet browser allowing for the use of cookies); – any other statement or conduct that clearly indicates acceptance of the proposed processing. On the contrary, silence, pre-ticked boxes or inactivity should not constitute consent. An opt-out model is therefore generally not permissible" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A practical guide. [s.l.]: Springer, 2017. p. 94-95).

De acordo com a norma, presume-se que o consentimento não foi dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações.

Traçadas essas considerações sobre o regime geral do consentimento na LGPD e no GDPR, passa-se para o estudo do consentimento nas relações atinentes ao tratamento de dados pessoais sensíveis e de crianças e adolescentes.

3 Dados sensíveis: requisição de consentimento específico e destacado

Os dados denominados *sensíveis* representam espécie de dado pessoal e se encontram presentes nos conjuntos informacionais do ser humano. Na LGPD, entendeu o legislador que a melhor forma de proteger essa categoria especial seria trazendo exemplos claros de dados assim considerados.[56] Dados sensíveis versam, por exemplo, sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou à organização de caráter religioso, filosófico ou político. São também sensíveis aqueles referentes à saúde[57] ou à vida sexual e dados genéticos[58] ou biométricos.[59]

[56] Como observa Danilo Doneda, "deve-se ter em conta que o próprio conceito de dados sensíveis atende à uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos" (DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 27).

[57] TEFFÉ, Chiara Spadaccini de. A saúde na sociedade da vigilância: como proteger os dados sensíveis? *Migalhas*, 14 abr. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia-como-proteger-os-dados-sensiveis. Acesso em: 21 maio 2020.

[58] Nesse sentido, dispõe o considerando 23 da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho: "Os dados genéticos deverão ser definidos como todos os dados pessoais relacionados com as características genéticas, hereditárias ou adquiridas, de uma pessoa, e que dão informações únicas sobre a fisionomia ou a saúde do indivíduo, [...] Tendo em conta a complexidade e a natureza sensível das informações genéticas, existe um elevado risco de utilização injustificada e de reutilização para diversos fins não autorizados por parte do responsável pelo tratamento. As discriminações com base em características genéticas deverão ser proibidas".

[59] "A biometria é a ciência de se estabelecer a identidade de alguém, a partir da medição e análise de seus atributos fisiológicos ou comportamentais mensuráveis. No primeiro caso, são exemplos: a impressão digital, o reconhecimento da íris, a identificação por retina, a definição dos traços do rosto, a arcada dentária, a geometria da mão e a altura da pessoa. No segundo, a forma como a pessoa digita, como anda, gestos característicos, voz e dinâmica da assinatura (velocidade do movimento da caneta, acelerações, pressão exercida e inclinação). Dados biométricos oferecem meios de identificar e autenticar indivíduos de maneira confiável e rápida, com base em um conjunto de dados reconhecíveis e verificáveis, que são únicos e específicos sobre seus titulares. O corpo torna-se a senha, meio único e exclusivo de individualização da pessoa" (TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora Raad. Reconhecimento facial: laissez-faire, regular ou banir? *Migalhas*, 16 jul. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial-laissez-faire-regular-ou-banir Acesso em: 29 jul. 2020).

Encontra-se nos dados sensíveis o "núcleo duro" da privacidade, tendo em vista que, pelo tipo e natureza de informação que trazem, constituem-se em dados cujo tratamento pode ensejar a discriminação ilícita ou abusiva de seu titular, devendo, por conseguinte, ser protegidos de forma mais rígida e específica.[60] São dados especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, cujo uso pode gerar riscos significativos para seu titular.[61]

Questiona-se: em se tratando de informações pessoais, seria possível considerar exaustivo o rol legal de dados sensíveis? Quais outros dados deveriam assim ser considerados? Mais ainda: tendo em vista as diversas possibilidades de utilização e cruzamento de informações, haverá algum dado realmente não sensível? Há casos, por exemplo, registrados nos Estados Unidos, de negativa de concessão de crédito para pessoas cujos nomes são, estatisticamente, os mais recorrentes na comunidade afrodescendente. É dizer: o simples prenome, em certo contexto, poderia ser considerado dado sensível para fins de tutela da igualdade.[62] Nessa direção, entende-se que a definição de certo dado pessoal como dado sensível deve ocorrer levando-se em conta o uso efetivo da informação, seu contexto e aplicação concreta.[63]

[60] RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Coordenação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 78; 96.

[61] No GDPR, em seu art. 9º, esses dados foram considerados dentro de uma categoria especial, restando como regra "proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".

[62] "Por exemplo, ao fornecer o número do CPF para obter descontos nas farmácias, a lista de medicamentos associada a esse dado pode conter informações delicadas sobre nossa saúde. É possível que essas informações sejam utilizadas de maneira discriminatória por seguradoras de saúde, alterando o valor da franquia de acordo com o perfil. Da mesma forma, nosso histórico de compras *on-line* diz bastante sobre poder aquisitivo e preferências pessoais. Por meio dessas informações, é possível embasar o direcionamento de propagandas compatíveis com o nosso gosto, tentando-nos a comprar algo que não precisamos, bem como cobrar preços mais altos ou limitar o acesso ao crédito para determinados perfis. Dados sobre orientação sexual, em uma sociedade que ainda vive preconceitos contra a diversidade, também podem servir a práticas de segregação, restringindo, por exemplo, as oportunidades de trabalho" (VARON, Joana. Privacidade e dados pessoais. *Panorama setorial da Internet*, ano 11, n. 2, jun. 2019. p. 12).

[63] "Deve-se averiguar em concreto, à luz do contexto de utilização daquele dado e da relação que se pode estabelecer com as demais informações disponíveis, a potencialidade de que seu tratamento possa servir como instrumento de estigmatização ou discriminação, à luz da privacidade, identidade pessoal e, de modo geral, da dignidade da pessoa humana" (KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 460).

Dispõe a LGPD que o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem;
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (Redação dada pela Lei 13.853/19); ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[64]

A primeira possibilidade para o tratamento, prevista no art. 11, inc. I, ocorre com o consentimento do titular ou seu responsável legal, de forma específica e destacada, para finalidades específicas.[65] A LGPD oferece camada adicional de

[64] Observa-se o relativo paralelismo entre as hipóteses do art. 7º e aquelas previstas no art. 11 da LGPD, devendo todos os cuidados já previstos para o tratamento dos dados ser aplicados de forma ainda mais intensa ao tratamento dos dados sensíveis, já que para eles se espera um padrão ainda mais rigoroso de proteção. É possível observar que ficaram de fora do tratamento de dados pessoais sensíveis as hipóteses de execução de contratos (art. 7º, V), de legítimo interesse do controlador (art. 7º, IX) e de proteção do crédito (art. 7º, X). No lugar do legítimo interesse do controlador, o art. 11, II, "g", da LGPD previu hipótese bem mais restritiva: garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

[65] Esse tipo de consentimento também é requerido no art. 7º, §5º ("O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei"); no art. 14, §1º ("O tratamento de dados

proteção para que tais dados não sejam utilizados contra os titulares, trazendo-lhes restrições ao acesso a bens e serviços ou mesmo ao exercício de direitos.[66]

Aqui, um dos desafios é compreender a dimensão e o real significado do consentimento caracterizado como específico e destacado. Segundo entendimento doutrinário, deve-se "enxergá-lo como um vetor para que haja mais *assertividade* do titular com relação a esses movimentos 'específicos' de seus dados".[67] A noção, no caso, aproxima-se da ideia de consentimento expresso,[68] por exigir maior atuação do titular dos dados, além de cuidado mais elevado com o tratamento da informação pelo agente.

Acerca das qualificações "específico" e "destacado", Teffé e Viola afirmam:

> *Específico* deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações de granularidade. *Destacado* pode ser interpretado no sentido de que é importante que o titular

pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal"); e no art. 33, VIII ("Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...] VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; [...]").

66 "Acresce que discussões mais recentes apontam para a ocorrência de fenômeno de publicidade comportamental voltado à formação de perfis de consumo, fato que se relaciona diretamente à regulação do tratamento de dados pessoais, em especial os dados sensíveis. Na verdade, na seara consumerista, assim como na seara trabalhista, são inúmeros os riscos da utilização de tais dados para praticar toda sorte de discriminações e violações a consumidores, empregados e candidatos a emprego em processos de seleção ou recrutamento" (FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *Jota*, 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 4 fev. 2019).

67 BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 202. O autor apresenta a seguinte crítica em relação à adjetivação inserida pelo legislador nacional ao consentimento para o tratamento de dados sensíveis: "[...] sob o ponto de vista de técnica legislativa, teria sido melhor que a LGPD tivesse adotado o adjetivo *expresso*, tal como fez a GDPR, bem como o Marco Civil da Internet [...], quando se quis prever um tipo de consentimento especial. Esse qualificador é o que semanticamente representaria melhor esse nível de participação mais intenso do cidadão no fluxo dos dados. Apesar dessa diferença semântica, entre os qualificadores expresso e específico, a consequência normativa tende a ser a mesma. Isso porque o que está em jogo é reservar um tipo de autorização singular em situações igualmente singulares no que tange ao tratamento de dados, sendo esta a racionalidade que percorre a LGPD, a GDPR e parte das leis setoriais brasileiras de proteção de dados pessoais" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 203).

68 No direito brasileiro, o consentimento expresso em termos de dados pessoais aparece no Marco Civil da Internet (Lei nº 12.965/14), em seu art. 7º: "VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...]".

> tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento, devendo tais disposições virem destacadas para que a expressão do consentimento também o seja. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento.[69]

No mesmo sentido, Sombra destaca que o consentimento específico "estabelece a necessidade de fornecimento de informações claras, granulares e delimitadas sobre as atividades de tratamento de dados".[70] Adicionalmente, o consentimento em destaque impõe "uma conduta afirmativa ou indicação assertiva de que o titular dos dados autorizou o tratamento [...]". Nesse tipo de consentimento não seria possível, portanto, trabalhar com a ideia de comportamento concludente ou consentimento tácito ou implícito.

Parte da doutrina encontra, no art. 11, inc. I, a existência de certa preferência à hipótese legal do consentimento, em razão da técnica legislativa utilizada, qual seja, a inserção de dois incisos no art. 11, sendo o primeiro sobre o consentimento e o segundo dispondo que, sem o fornecimento de consentimento do titular, poderá ocorrer o tratamento de dados sensíveis (apenas) nas hipóteses em que for indispensável para as sete situações estabelecidas nas alíneas. Todavia, parece mais adequado compreender que tanto na hipótese de tratamento de dados sensíveis por meio do consentimento quanto nos casos que se referem às demais situações que independem de tal manifestação de vontade, a técnica legislativa utilizada coloca todas as bases legais em posição de igualdade, não havendo prevalência ao consentimento.[71]

Nos termos da LGPD, será aplicada a proteção disposta no art. 11 a qualquer tratamento de dados pessoais que revele dados sensíveis e que possa causar danos ao titular, ressalvado o disposto em legislação específica. Mesmo os dados que, inicialmente, não sejam sensíveis, podem assim se tornar quando, em determinado contexto fático, levarem a informações sensíveis a respeito dos titulares.[72]

---

[69] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, Rio de Janeiro, ano 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 13 maio 2020.

[70] SOMBRA, Thiago. *Fundamentos da regulação da privacidade e proteção de dados pessoais*. São Paulo: Thomson Reuters Brasil, 2019. p. 137.

[71] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de proteção de dados pessoais. *Revista do Advogado*, n. 144, p. 47-53, nov. 2019.

[72] Sobre o ponto, anota Ana Frazão: "a linha distintiva entre dados pessoais e dados pessoais sensíveis pode não ser tão nítida, até porque a perspectiva de análise deve ser dinâmica e não estática. Dessa maneira, há boas razões para sustentar que são sensíveis todos os dados que permitem que se chegue,

Ainda segundo a LGPD, a comunicação ou o uso compartilhado de dados sensíveis entre controladores, com objetivo de obter vantagem econômica, poderá ser objeto de vedação ou de regulamentação por parte da Autoridade Nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.[73]

Confirma-se, assim, que o tratamento de dados sensíveis exige tutela diferenciada e permanentemente atualizada, de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar preconceitos e discriminações ilícitas ou abusivas em face do titular.

Conforme observado em doutrina, a mera proibição do tratamento de dados sensíveis mostra-se inviável, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, além de existirem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como exemplo, algumas entidades de caráter político, religioso ou filosófico. Dessa forma, entende-se que o tratamento de dados sensíveis é possível e, inclusive, necessário em determinadas circunstâncias. Contudo, deverá ser considerado excepcional, pela relevância dos valores em questão, e autorizado quando não houver utilização discriminatória das informações coletadas. [74]

4 O tratamento de dados pessoais de crianças e adolescentes

Em seu art. 14, a LGPD dispõe de forma específica acerca do tratamento de dados pessoais de crianças e adolescentes.[75] Conforme disposto, o tratamento deverá ser realizado no melhor interesse desses sujeitos, levando-se em

como resultado final, a informações sensíveis a respeito das pessoas" (FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *Jota*, 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 4 fev. 2019).

73 Art. 11, §4º, da LGPD: "É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o §5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. §5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários".

74 DONEDA, Danilo. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 27.

75 Cf. TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e de adolescentes. *Revista do Advogado*, n. 144, p. 54-59, nov. 2019; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento. *In*: NIC.BR; CETIC.BR. *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil*: TIC kids online Brasil 2018. São Paulo: Comitê Gestor da Internet no Brasil, 2019.

conta especialmente as normas protetivas estabelecidas na Constituição Federal, no Estatuto da Criança e do Adolescente e na Convenção sobre os Direitos da Criança. Busca-se, assim, assegurar seu desenvolvimento físico, mental, moral, espiritual e social em condições dignas,[76] havendo o reconhecimento da criança e do adolescente como protagonistas da dinâmica familiar.

Em relação às crianças (pessoas de até doze anos de idade incompletos), afirma-se que, quando a base legal for o consentimento, o tratamento dos dados pessoais desses sujeitos deverá ser realizado com o consentimento específico[77] e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal (§1º), devendo esse consentimento ser também livre, informado e direcionado a tratamento de dados pessoais para finalidade determinada.

Dessa forma, o consentimento dado por sujeito fora do requisito legal ou pela própria criança não poderá ser admitido. Optou a lei por oferecer tutela destacada à criança, sujeito hipervulnerável (ou de vulnerabilidade agravada pela idade reduzida)[78] e absolutamente incapaz, o qual deve ser representado sob pena de nulidade absoluta do ato praticado.[79]

Todavia, ao não mencionar o adolescente (pessoa entre doze e dezoito anos de idade), o §1º do art. 14 não deixou claro se, neste caso, o consentimento manifestado por ele sem assistência ou representação deveria ser considerado válido, como hipótese de capacidade especial, ou se simplesmente o legislador teria optado por não tratar do tema, por já existir legislação geral sobre a matéria no Código Civil (arts. 3º, 4º e 1.634, VII, por exemplo). Ao que parece, o legislador pretendeu reconhecer a validade do consentimento manifestado pelo adolescente. Tomando-se como base a realidade da utilização da internet e das mídias sociais, que têm entre seus usuários milhares de adolescentes, é possível que se tenha optado por considerar jurídica hipótese fática dotada de ampla aceitação social.

[76] MACHADO, Diego Carvalho. Capacidade de agir e direitos da personalidade no ordenamento jurídico brasileiro: o caso do direito à privacidade. *RBDCivil*, v. 8, abr./jun. 2016. p. 74-75.

[77] Semelhante caracterização do consentimento é encontrada na base legal de tratamento dos dados sensíveis (art. 11, I, da LGPD), havendo exigência de maior participação do titular, como também de cuidado mais elevado com o tratamento da informação pelo agente. A noção, aqui, aproxima-se da ideia de consentimento expresso.

[78] MIRAGEM, Bruno. *Curso de direito do consumidor*. 6. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2016. p. 131-132.

[79] Código Civil de 2002: "Art. 3º São absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 (dezesseis) anos. [...] Art. 166. É nulo o negócio jurídico quando: I - celebrado por pessoa absolutamente incapaz; [...]".

Vale lembrar, inclusive, que tanto o Código Civil quanto o Estatuto da Criança e do Adolescente trazem em suas normas determinadas disposições que valorizam a vontade dos menores[80] e oferecem hipóteses de capacidade especial a eles.[81]

A internet oferece enormes possibilidades e benefícios para as crianças e adolescentes, facilitando a participação deles em discussões e atividades criativas, bem como o acesso à informação e educação de qualidade. Nos últimos anos, o acesso à internet vem se afirmando como direito fundamental, por proporcionar melhor qualidade de vida e promover o desenvolvimento das pessoas. Diante disso, mostra-se necessário estabelecer políticas e normas equilibradas que, de um lado, protejam os menores de riscos e danos a sua integridade e liberdade e, de outro, facilitem o acesso desses sujeitos à rede, de forma segura, responsável e ética.[82]

Segundo pesquisa, no ano de 2018, 86% da população entre 9 e 17 anos era usuária de internet no país.[83] No mesmo ano, 83% da população investigada reportou ter assistido a vídeos, programas, filmes ou séries *on-line*. Pela primeira vez no estudo, essas atividades passaram a ser as mais frequentes entre as crianças e os adolescentes usuários de internet no Brasil, superando pesquisas na internet para trabalhos escolares (74%) e o envio de mensagens instantâneas (77%). Ainda considerando atividades multimídia, estimou-se que 82% das crianças e adolescentes usuários de internet escutaram música *on-line*, 60% jogaram na internet sem conexão com outros jogadores e 55% jogaram conectados com outros jogadores.

O celular segue sendo o principal dispositivo utilizado por crianças e adolescentes. Em 2018, também, cerca de 20 milhões de crianças e adolescentes (de 9 a 17 anos e usuários de internet) possuíam perfil em redes sociais, o que equivalia a 82% dos usuários nessa faixa etária. O aplicativo WhatsApp foi a plataforma em que crianças e adolescentes reportaram possuir perfil em maiores proporções (72%), superando o Facebook (66%). Já o Instagram apresentou o maior crescimento em

[80] Exemplos de flexibilização do regime das incapacidades no ECA: art. 16, II; art. 28, §§1º e 2º; art. 100, XII; art. 111, V; e art. 161, §3º. Além desses exemplos, pode-se citar o próprio Código Civil, em seu art. 1.740, III.

[81] Existem atos e negócios que os relativamente incapazes (maiores de dezesseis e menores de dezoito anos) podem praticar, mesmo sem assistência, como se casar, exigindo-se autorização de ambos os pais, ou de seus representantes legais; elaborar testamento; servir como testemunha de atos e negócios jurídicos; e ser eleitor.

[82] TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Infância conectada: direitos e educação digital. *In*: NIC.BR; CETIC.BR. *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil*: TIC kids online Brasil 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. p. 31-40.

[83] NIC.BR; CETIC.BR. *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil*: TIC kids online Brasil 2018. São Paulo: Comitê Gestor da Internet no Brasil, 2019. p. 24-25. Disponível em: https://cetic.br/pesquisa/kids-online/publicacoes. Acesso em: 20 maio 2020.

relação ao número de crianças e adolescentes que possuem perfil na plataforma (saltando de 36%, em 2016, para 45%, em 2018).

Contudo, a mencionada previsão do art. 14, §1º, encontra críticas na doutrina, que afirma que a norma "teria andado melhor se exigisse o consentimento dos pais até os 16 anos".[84] Destaca-se que, dada a relevância que o consentimento relativo ao uso de dados possui e por não se tratar de uma manifestação de vontade simples ou corriqueira, não se mostra necessariamente certo que se deva admitir que a prestação de consentimento entre 12 e 18 anos de idade receba eficácia, prescindindo totalmente da participação parental, sendo necessário, conforme salientado por Teixeira e Rettore, repensarmos criticamente os termos da LGPD nesse assunto.[85]

Vale lembrar, porém, que como regra as principais mídias sociais determinam a idade mínima de 13 anos para a abertura de contas e utilização desses canais, exigindo-se idade mais elevada a depender das leis do país onde o serviço será oferecido. Como exemplos, basta recordar os termos de uso do Instagram, Facebook, WhatsApp, YouTube, Twitter e Snapchat para o Brasil, em que a exigência de idade mínima de 13 anos foi mantida. Essa determinação tem como pano de fundo norma norte-americana que considera criança o indivíduo com menos de 13 anos de idade: o *Children's Online Privacy Protection Act* de 1998 (COPPA – §312.1).[86]

Observa-se que a LGPD, no ponto relativo à proteção de crianças e adolescentes, além de tomar como fonte a norma europeia (GDPR), inspirou-se também no COPPA. Todavia, não definiu em detalhes determinadas expressões e conceitos adotados, como o fez o regramento norte-americano.

Quanto à idade mínima para a utilização de redes sociais, na Europa há disposições diversas nos termos de uso de algumas ferramentas. Como alguns países ainda vêm se adequando ao art. 8º do GDPR, é possível encontrar disposições que exigem a idade mínima de 16 anos para a utilização do serviço.[87]

---

[84] TEIXEIRA, Ana Carolina Brochado; RETTORE, Anna Cristina de Carvalho. A autoridade parental e o tratamento de dados pessoais de crianças e adolescentes. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019. p. 525-526.

[85] Sobre a disposição, encontra-se também o seguinte entendimento: "Uma vez que o caput afirma que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente, e considerando que o artigo é um todo, composto por partes que se dividem em caput, parágrafos, incisos, alíneas e itens, não se podem excluir os adolescentes do procedimento previsto nos parágrafos" (AMARAL, Claudio do Prado. Proteção de dados pessoais de crianças e de adolescentes. *In*: LIMA, Cíntia de (Coord.). *Comentários à Lei Geral de Proteção de Dados*. [s.l.]: Almedina, 2020. p. 175).

[86] Disponível em: https://www.ecfr.gov/cgi-bin/text-idx?SID=d9fdda9d81a3e854c8793fd56bd8a059&mc=true&node=pt16.1.312&rgn=div5#se16.1.312_15. Acesso em: 2 jan. 2019.

[87] Como exemplo, vale recordar os termos de uso do WhatsApp: "Se você reside em um país do Espaço Econômico Europeu (que inclui a União Europeia) ou em qualquer outro país ou território incluído (coletivamente,

O art. 8º da norma europeia dispõe, em síntese, que, quando for aplicável o art. 6º, n. 1, "a",[88] quanto à oferta direta de serviços da sociedade da informação para crianças, o tratamento dos dados pessoais de uma criança será legal quando ela tiver pelo menos 16 anos de idade. Caso a criança tenha menos de 16 anos, o tratamento só será lícito se o consentimento for dado ou autorizado pelos titulares da autoridade parental. Contudo, destaca-se que os Estados-Membros poderão estabelecer idade menor para os efeitos referidos, desde que não inferior a 13 anos.[89] Nesses casos, o responsável pelo tratamento deverá promover todos os esforços adequados para verificar se o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.[90]

Ainda quanto ao art. 14 da LGPD, na hipótese do tratamento do §1º, os controladores deverão manter públicas as informações sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos

Europa), deve ter pelo menos 16 anos (ou mais, se for exigido em seu país) para se cadastrar e usar o WhatsApp. Se você reside em qualquer outro país, e não nos países pertencentes à Região Europeia, você deve ter pelo menos 13 anos (ou mais, se for exigido em seu país) para se cadastrar e usar o WhatsApp. [...] Criar uma conta com informações falsas caracteriza uma violação de nossos Termos. Registrar uma conta em nome de um menor de idade também é considerado violação dos nossos Termos" (Disponível em: https://faq.whatsapp.com/pt_br/android/26000151/?category=5245250. Acesso em: 28 jul. 2019).

[88] "Artigo 6º 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; [...]".

[89] No estudo *The GDPR child's age of consent for data processing across the EU – one year later (July 2019)*, foram apresentadas as idades mínimas estabelecidas por alguns países europeus para um menor consentir com o tratamento de seus dados por serviços da sociedade da informação (Disponível em: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751. Acesso em: 28 jul. 2019). A lei dinamarquesa de proteção de dados foi adotada oficialmente em maio de 2018. A idade de consentimento para crianças que usam serviços digitais foi fixada em 13 anos. A razão dessa decisão levou em conta os benefícios educacionais e sociais dos serviços *on-line* para crianças, bem como sua participação e inclusão no mundo digital. Em junho de 2018, a Lei francesa nº 2018-493, relativa à proteção dos dados pessoais, foi adotada e publicada no jornal oficial. Seu artigo 20 declara que um menor pode consentir sozinho com o processamento de seus dados pessoais, quando diante da oferta de serviços da sociedade da informação, a partir dos seus 15 anos. A segunda parte do artigo introduz um consentimento conjunto, afirmando que quando o menor tiver menos de quinze anos, o tratamento será lícito apenas se o consentimento for dado conjuntamente pelo menor em causa e pelo(s) seu(s) pai(s). Em 18.4.2018, o parlamento sueco adotou a nova lei sueca de proteção de dados, estabelecendo a idade de consentimento para as crianças aos 13 anos. Nos países baixos, o ato de implementação final do GDPR foi publicado no jornal oficial em 22.5.2018. O artigo 5º do ato fixa a idade para o consentimento do uso de serviços digitais em 16 anos. O Ato de Proteção de Dados do Reino Unido (*UK Data Protection Act 2018*) foi adotado em 23.5.2018. A Seção 9 do ato determina a idade de consentimento das crianças, em relação aos serviços da sociedade da informação, em 13 anos. Na Itália, o decreto responsável por alinhar o sistema jurídico italiano ao GDPR estabeleceu que o menor que completou quatorze anos poderá expressar seu consentimento para o processamento de seus dados pessoais, em relação à oferta direta de serviços da sociedade da informação. Sendo o titular menor de 14 anos, o consentimento será realizado pelo titular da responsabilidade parental.

[90] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: 29 dez. 2018.

direitos a que se refere o art. 18 da lei (artigo esse que se encontra no capítulo dos direitos do titular). Isso porque o consentimento, por si só, não afasta a responsabilidade do agente de avaliar todos os riscos do processamento dos dados nem seu dever de observar fielmente as disposições protetivas da LGPD. Além disso, os controladores deverão realizar todos os esforços razoáveis para verificar se o consentimento a que se refere o §1º foi manifestado pelo responsável pela criança, consideradas as tecnologias disponíveis (art. 14, §5º). Identifica-se, aqui, dever de cuidado atribuído ao controlador. Pondera a doutrina que se, por um lado, o controlador não pode tratar dados antes do consentimento, por outro, precisará de tais dados para contatar o responsável legal pela criança.

Dessa forma, os controladores deverão estar atentos e passar a exigir a data de nascimento do usuário e outras informações adicionais pertinentes, a fim de apurar sua verdadeira idade, para, se for o caso, suspender o tratamento de seus dados até a obtenção do consentimento do responsável. Outras informações que, a depender da situação e do tipo de serviço, podem ser relevantes para a melhor identificação do emissor do consentimento são o número de seu cartão de crédito e o número de seu CPF.

Assim como no GDPR, a questão do consentimento do responsável pela criança na LGPD levanta muitas questões sobre sua implementação. Por exemplo, como as empresas verificarão se a pessoa que forneceu o consentimento é realmente um dos responsáveis? Não está claro na lei em que se constituirá o "esforço razoável" por parte do controlador e quem avaliará a tecnologia implementada e o esforço desempenhado por ele. Seria essa uma atividade da Autoridade Nacional de Proteção de Dados? Certamente, algumas empresas, pelo porte e pelo poderio econômico, estarão em posição muito melhor para investir nas medidas necessárias. Outros desafios a se cogitar são as chances de as medidas de implementação ocasionarem maior processamento de dados pessoais, em contrariedade ao princípio da minimização dos dados; além do risco de que crianças desenvolvam estratégias para contornar a regra relativa ao consentimento parental. Do ponto de vista educacional, questiona-se ainda qual seria a extensão dos espaços de liberdade na internet a serem assegurados às crianças e adolescentes sem a interferência de seus pais.

O §4º, do art. 14, da LGDP prevê que os controladores não deverão condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade, mostrando-se assim refratário à requisição excessiva de dados de crianças em serviços de divertimento e entretenimento. O dispositivo prestigia o princípio da minimização dos dados, segundo o qual os dados devem ser adequados, pertinentes e limitados ao que for necessário relativamente às finalidades

para as quais serão tratados. Se houver desrespeito a tal previsão, o tratamento dos dados poderá ser considerado abusivo, mesmo tendo havido o consentimento do responsável pela criança.[91] Por meio dessa disposição, busca-se afastar políticas de tudo ou nada, já comentadas acima, em que o usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo.

Dispõe também a norma que as informações sobre o tratamento de dados referidas no art. 14 deverão ser fornecidas de maneira simples, clara e acessível,[92] consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. Portanto, as ações direcionadas ao cumprimento dos deveres de informação e de transparência precisarão se adequar inclusive à capacidade de compreensão das crianças e adolescentes, sujeitos tutelados pela doutrina da proteção integral e que apresentam condição peculiar, por se encontrarem em desenvolvimento.[93]

Há também na LGPD hipóteses de tratamento de dados de menores sem a necessidade de consentimento. Como afirmado na primeira parte do texto, o consentimento é uma das bases legais para o tratamento de dados, mas não a única. No caso em tela, que envolve menores de idade, não parece ter sido estabelecida norma com rol específico e exclusivo para o tratamento dos dados desses sujeitos, devendo ser aplicadas, como regra, as disposições dos arts. 7º e 11.[94] Entende-se que o art. 14 complementa as mencionadas bases legais,

[91] FRAZÃO, Ana. Nova LGPD: tratamento dos dados de crianças e adolescentes. *Jota*, 3 out. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-tratamento-dos-dados-de-criancas-e-adolescentes-03102018. Acesso em: 28 dez. 2018.

[92] Nesse sentido, o art. 12 do GDPR: "Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados. 1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13º e 14º e qualquer comunicação prevista nos artigos 15º a 22º e 34º 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".

[93] Observa-se que a norma acima deve ser lida juntamente com as disposições do Estatuto da Criança e do Adolescente, especialmente seus arts. 70 e 71, segundo os quais é dever de todos prevenir a ocorrência de ameaça ou violação aos direitos da criança e do adolescente, sujeitos esses que têm direito à informação, cultura, lazer, esportes, diversões e produtos e serviços que respeitem suas condições peculiares de pessoas em desenvolvimento.

[94] Há de se questionar, todavia, a aplicação das disposições acerca da tutela do crédito (art. 7º, X) e do atendimento dos interesses legítimos do controlador ou de terceiro (art. 7º, IX) para o tratamento de dados de menores. No caso do legítimo interesse, o legislador ressalvou que a hipótese não será possível "se prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Sobre a exceção, é necessário ponderar que, no caso de dados de crianças e adolescentes, será importante considerar tal ressalva com maior cuidado, assim como optou o Regulamento europeu em seu

trazendo algumas restrições e hipóteses específicas para o tratamento de dados de menores. Esse entendimento, porém, ainda se encontra em construção e, em razão da importância da temática, deverá ser objeto de esclarecimento por parte da Autoridade Nacional de Proteção de Dados brasileira.

Como complemento às hipóteses de autorização legal para o tratamento de dados, afirma-se no §3º, do art. 14, que poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o §1º do mencionado artigo quando: a) a coleta for necessária para contatar os pais ou o responsável legal, devendo os dados ser utilizados uma única vez e sem armazenamento; ou b) para a proteção da criança. Porém, em nenhum caso, esses dados poderão ser repassados a terceiro sem o consentimento de que trata o §1º.

Como visto, a disposição relativa ao tratamento de dados de crianças e adolescentes mostra-se significativa e bastante relevante, exigindo-se interpretação que priorize o melhor interesse desses sujeitos e a constante incorporação à norma infraconstitucional dos valores e princípios constitucionais.

5 Considerações finais

O desenvolvimento das relações humanas torna inafastável o fornecimento de informações e dados pessoais no ambiente físico e digital. Nessa direção, a Lei Geral de Proteção de Dados, ao disciplinar o uso e a integridade dos dados de cada pessoa, sobretudo aqueles considerados sensíveis, protege e garante o princípio da dignidade da pessoa humana e seus corolários. Ao trazer tutela focada na pessoa e no livre desenvolvimento de sua personalidade, a LGPD assegura o exercício da liberdade existencial e a igualdade material, diante do papel relevante da informação para as escolhas individuais e o estabelecimento de vínculos na sociedade.

Em cenário de elevada circulação de informações, foram estabelecidas ferramentas específicas de controle em favor do titular. Entre elas, destaca-se o consentimento, caracterizado como livre, informado, inequívoco e direcionado a uma finalidade determinada, da mesma forma como tratado no regulamento europeu. O cuidado e a qualificação oferecidos ao consentimento, base legal objeto desse artigo, revelam a preocupação do legislador com a participação do indivíduo no

art. 6º: "Artigo 6º Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: [...] 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".

fluxo de suas informações pessoais, incentivando comportamento ativo da parte do titular, e exigindo responsável prudência por parte do agente que realizar o tratamento dos dados.

O regulamento europeu de proteção de dados pessoais funciona como modelo de referência que países como o Brasil deverão levar em conta tanto na interpretação e aplicação de suas leis, quanto na própria elaboração de legislação acerca da temática, em cotejo com o almejado fluxo de informações e convergências derivadas de diplomas em nível internacional. Especialmente no campo tecnológico, mostra-se relevante o desenvolvimento de normas que apresentem entendimentos mais uniformes, a facilitar a inserção e a regulação de novos sistemas, dispositivos e negócios. Além disso, padrões elevados para a proteção de dados pessoais aumentam a compatibilidade entre sistemas jurídicos, possibilitando melhor fluxo de informações, maior segurança nas transações e relações cada vez mais complexas.

A Lei Geral de Proteção de Dados se anuncia, nessa direção, como passo indispensável no caminho da proteção efetiva e do pleno exercício da autodeterminação existencial e informacional da pessoa humana. Cuida-se de ferramenta que se propõe, em boa hora, à proteção do indivíduo e ao controle específico da circulação de informações, trazendo a segurança jurídica necessária ao desenvolvimento de renovada cultura de tutela de dados pessoais.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 25, p. 83-116, jul./set. 2020.

Recebido em: 16.01.2020
1º parecer em: 30.03.2020
2º parecer em: 11.06.2020