Tratamento de dados pessoais na LGPD: estudo sobre as bases legais

Chiara Spadaccini de TEFFÉ*

Mario VIOLA**

RESUMO: O presente artigo visa analisar as bases legais para o tratamento de dados pessoais na Lei Geral de Proteção de Dados brasileira (LGPD – Lei n. 13.709/18). Diante da necessidade, como regra, de se enquadrar todo tratamento de dados em uma base legal determinada, mostra-se relevante estudar as possibilidades positivadas nos artigos 7º e 11 da LGPD e, especialmente, as hipóteses do consentimento e do legítimo interesse. Entender a aplicação de cada base legal é fundamental para se garantir segurança nas relações e evitar que os direitos e liberdades dos titulares sejam ameaçados ou sofram danos. Para tanto, serão analisadas principalmente doutrina brasileira e referências que versam sobre o regulamento europeu de proteção de dados.

PALAVRAS-CHAVE: Dados pessoais; tratamento de dados; bases legais; privacidade.

TITLE: Processing of Personal Data according to LGPD: a Study about the Legal Basis

ABSTRACT: This article aims to analyze the legal basis for the processing of personal data in the Brazilian General Data Protection Law (Law n. 13.709/18). Considering the need to have a valid lawful basis in order to process personal data, it is relevant to study the possibilities established in articles 7 and 11 of the LGPD and, especially, the figures of consent and legitimate interest. Understanding the application of each legal basis is essential to ensure security in the relationships and processes carried out, as well as to avoid risks and damages to the rights and freedoms of the data subject. For this purpose, Brazilian doctrines and references on the European data protection regulation will be analyzed.

KEYWORDS: Personal data; data processing; legal basis; privacy.

---

* Doutoranda e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Atualmente, é professora de Direito Civil 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" da Pós-Graduação do Instituto New Law. Associada ao Instituto Brasileiro de Estudos em Responsabilidade Civil (IBERC). Foi professora substituta de Direito Civil na Universidade Federal do Rio de Janeiro (UFRJ). Advogada e consultora em proteção de dados. Contato: chiaradeteffe@gmail.com.

** Doutor em Direito pelo *European University Institute* (Florença, Itália), Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro. É pesquisador associado do *Centre for Media Pluralism and Media Freedom* do *European University Institute*, *Acting Data Protection Officer* também do *European University Institute*, *Certified Information Privacy Professional/Europe* (CIPP/E) e advogado. E-mail: mviolaac@gmail.com.

1. Hipóteses legais para o tratamento de dados: controle e garantias ao titular

Na Lei Geral de Proteção de Dados (Lei n. 13.709/18 –LGPD), parte-se da ideia de que todo dado pessoal tem importância e valor. Por essa razão se adotou conceito amplo de dado pessoal, assim como estabelecido no Regulamento europeu (GDPR–*General Data Protection Regulation*),[1] sendo ele definido como informação relacionada a pessoa natural identificada ou identificável. Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo informações inclusive de caráter sensível sobre ela, conforme já observou o *Bundesverfassungsgericht* (Tribunal Constitucional Federal Alemão) no emblemático julgamento sobre a lei do censo de 1983.[2]

Diante do cuidado com o tema, foi estabelecido como regra geral (Art. 1º) que qualquer pessoa que trate[3] 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 os tratamentos de dados pessoais que realizar. Isso importa dizer que não haverá necessidade de identificação de uma base legal apropriada apenas nos casos que se enquadrarem nas hipóteses de exclusão de aplicação da lei previstas no Art. 4º da

[1] A disposição brasileira segue o previsto no GDPR: "Artigo 4.º 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;".

[2] "Um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados insignificantes no contexto do processamento eletrônico de dados" (MARTINS, Leonardo (org.). *Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005, p. 244-245. Disponível em: <www.kas.de/wf/doc/26200-1442-1-30.pdf>. Acesso em: 01.08.19).

[3] Cabe recordar a noção de "tratamento" disposta na Lei: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". Há, assim, um amplo rol de ações dispostas na lei e sob o guarda-chuva da ideia contida em tratamento de dados pessoais.

LGPD.[4] Mas, ainda assim, o tratamento de dados pessoais previsto no Art.4º, inciso III (para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais) "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". Para tanto, já foi criada no âmbito da Câmara dos Deputados comissão de juristas responsável pela elaboração de anteprojeto de lei sobre essa matéria.[5]

Portanto, não sendo uma hipótese de exclusão, deverá ocorrer o encaixe do tratamento realizado em pelo menos uma das hipóteses legais para que ele seja considerado legítimo e lícito, sendo possível inclusive cumular as mesmas, assim como no GDPR. Essas bases foram estipuladas de forma geral e variada, devendo detalhes e adequações serem realizados especialmente pela Autoridade nacional de proteção de dados (ANPD), pelo Legislativo e Judiciário.

---

[4] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. §1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. §2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no §4º deste artigo. §3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público (Redação dada pela Lei nº 13.853, de 2019).

[5] Câmara dos Deputados. Ato do Presidente de 26/11/2019. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/conheca-a-comissao/criacao-e-constituicao/ato-de-criacao>. Acesso em: 03.05.20.

Entende-se que tanto o rol do Art. 7º quanto o do Art. 11 são taxativos,[6] apesar de dotados de hipóteses chamadas de "coringas", ou seja, hipóteses mais abertas e com certo grau de subjetividade (como, por exemplo, o legítimo interesse). Há, entretanto, autores que defendem a existência de uma outra base legal para o tratamento de dados pessoais no Art. 23 da LGPD para o exercício geral das competências ou o cumprimento de atribuições legais da Administração Pública.[7] Contudo, entendemos que o tratamento de dados pessoais para tais atividades já estaria contemplado nas hipóteses relativas ao cumprimento de uma obrigação legal (Art. 7º, II, e Art. 11, II, 'a'), já que a atuação da Administração Pública decorreria de um mandamento legal, e ao tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7º, III, e Art. 11, II, 'b').

De forma a se evitar abusos no tratamento de dados e garantir os direitos do titular, ele poderá revogar o seu consentimento, conforme será visto no item 2, ou pleitear o direito à oposição, que significa que o titular poderá se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (Art. 18, §2º). Além disso, encontra-se positivado o direito à explicação (Art. 20), que dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões

[6] No regulamento europeu de proteção de dados (GDPR), utiliza-se a mesma sistemática para a aplicação das bases legais para o tratamento de dados pessoais: "The principle of 'lawful processing', which is one of several data protection principles under Article 5 GDPR, requires that every processing operation involving personal data must have a legal basis. Article 6(1) stipulates what may constitute such a legal basis. At the same time, it must be kept in mind that legally sound processing of personal data will necessitate fulfilling also all other of the core principles for processing personal data set out by Article 5(1). The list of legal grounds for processing contained in Article 6(1) must be understood as exhaustive and final – it can neither be supplemented nor otherwise amended by interpretation. As far as Member States' legislators are, at all, allowed to act under Article 6(1),1 all legislative activities must keep within the strict boundaries it sets. The elements in the list must be seen to be legally equal. There is no ranking between Article 6(1)(a) to (f) in the sense that one ground has normative priority over the others.3 However, in the private sector, consent (Article 6(1)(a)) may in practice play a salient role as a potential substitute whenever there is no contractual context, no detailed legal rules about a fitting legal basis, or the scope of 'legitimate interests of the controller or of a third party' is particularly difficult to assess. This may also be the reason why it was deemed necessary in the GDPR to define valid consent more extensively than the other legal grounds for processing and - compared to the DPD – to add two articles (Articles 7 and 8) dealing with specific aspects of consenting" (KOTSCHY, Waltraut. Lawfulness of processing. In: *2018 Draft commentaries on 10 GDPR articles* (from Commentary on the EU General Data Protection Regulation, OUP 2019). Oxford University Press, 2018, p. 37. Disponível em: <https://works.bepress.com/christopher-kuner/1/>. Acesso em: 22.07.19).

[7] MENDES, Laura Schertel; DONEDA, Danilo. "Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil". *Revista de Direito do Consumidor*, v. 120, p. 555, 2018.

destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.[8-9]

O sistema legal desenvolvido para o tratamento de dados representa para o titular instrumento de controle sobre as suas informações pessoais e de garantia de direitos. Nesse sentido, no presente artigo, busca-se analisar em detalhe os requisitos para o tratamento de dados na LGPD, com ênfase nas bases legais relativas ao consentimento e ao legítimo interesse e nas diferenças de tratamento estabelecidas para dados que sejam considerados sensíveis.

2. O consentimento do titular

O consentimento do titular dos dados recebeu tutela destacada na LGPD, ainda que não seja, vale lembrar, a única hipótese legal para o tratamento de dados pessoais nem hierarquicamente superior às demais contidas no rol do Art. 7º. Aliás, em determinados casos, a obtenção do consentimento poderá ser até mesmo inadequada, tendo em vista a existência de outra base legal contida no rol do Art. 7º, ou mesmo do Art. 11, aplicável. Nesses casos, parece mais adequado e seguro que ela seja utilizada e não o consentimento do titular do dado, ainda que seja possível obtê-lo.

Uma análise minuciosa dos princípios – que têm grande parte de seu centro gravitacional baseado no ser humano – revela a preocupação do legislador com a participação do indivíduo no fluxo de suas informações. Como será exposto, no texto legal, a caracterização do consentimento segue a linha do Regulamento europeu e das normas mais atuais sobre o tema. Há também uma série de disposições que oferecem regramento específico para concretizar, orientar e reforçar o controle dos dados através do consentimento.[10]

---

8 Debate-se, aqui, se deveria haver uma obrigatoriedade da revisão humana de decisões automatizadas. Sobre o assunto, conferir: MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?* Artigo estratégico 39. Instituto Igarapé. Dezembro de 2018. FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. *Jota,* publicado em 09 de julho de 2019. MULHOLLAND, Caitlin; FRAJHOF, I. Z. Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação frente à tomada de decisões por meio de machine learning. In: Ana Frazão; Caitlin Mulholland (Org.). *Inteligência Artificial e Direito*: Ética, Regulação e Responsabilidade. 1. ed. Rio de Janeiro: Revista dos Tribunais, 2019, v. 1, p. 265-287.

9 Art. 20 (...) § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

10 Cf. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: Ana Frazão, Gustavo Tepedino e Milena Donato Oliva (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Editora Revista dos Tribunais, 2019, p. 287-322.

No que diz respeito ao tratamento dos dados, o consentimento deverá ocorrer, como regra, de acordo com a hipótese estabelecida no artigo 7º, I, da LGPD, sendo certo que no caso de dados sensíveis foram positivadas normas mais rígidas (Art. 11, I), conforme se verá mais adiante, e que em se tratando de criança, além de o consentimento ser reforçado,[11] foi acrescentada hipótese adicional de tratamento de dados sem o consentimento de um dos pais ou responsável legal (Art. 14, §3º).[12-13]

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 dados por parte de uma série de sujeitos e situações de pouca transparência e informação no que tange ao tratamento de dados pessoais de usuários de serviços online. Nesse sentido, defende-se que a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados para outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa.

---

[11] "What is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR. Trusted third party verification services may offersolutions, which minimise the amount of personal data the controller hasto process itself" (European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. Adotada em 04 de maio de 2020, p. 26-27).

[12] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (...) § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

[13] Cf. TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: proteção e consentimento. In: *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.47-54. TEFFÉ, Chiara Spadaccini de. Proteção de dados de crianças e de adolescentes. *Revista do advogado*, n. 144, nov. 2019, p. 54-59. "Como se depreende da Lei, o consentimento é uma das bases legais para o tratamento de dados, mas não a única. Acerca do tratamento de dados de menores de idade, não foi estabelecido rol especial para o tratamento de suas informações, devendo ser aplicadas, como regra, as disposições dos artigos 7º e 11, que trazem as hipóteses previstas pela LGPD para o tratamento de dados pessoais. Entende-se que o art. 14 da LGPD traz em si especificidades quanto ao consentimento e mais algumas possibilidades legais de tratamento de dados. Dessa forma, como complemento às hipóteses de autorização legal para o tratamento de dados, afirma-se no parágrafo 3º, do artigo 14, que poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o parágrafo 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 § 1º". No mesmo sentido, European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. Adotada em 04 de maio de 2020, p. 26. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>. Acesso em: 06.05.2020: "127. It is clear from the foregoing that Article 8 shall only apply when the following conditions are met: The processing is related to the offer of information society services directly to a child. The processing is based on consent".

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.[14] Ele promove a personalidade, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações.[15]

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). Dialoga, portanto, com a definição positivada no GDPR: "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco,[16] que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".[17]

Livre significa que o titular pode escolher entre aceitar ou recusar a utilização de seu bem, sem intervenções ou situações que viciem o seu consentimento. Nessa linha, estabeleceu-se de forma expressa a vedação ao tratamento de dados pessoais mediante vício de consentimento. A respeito dessa característica, mostra-se relevante que se

[14] 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 ser o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento".
[15] DONEDA, Danilo, op. cit., p. 379.
[16] "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. Springer, 2017, p. 94).
[17] Recomenda-se a leitura de: Article 29 Data Protection Working Party - Guidelines on consent under Regulation 2016/679. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 29.04.20.

analise a assimetria entre as partes e eventual vulnerabilidade de algum contratante,[18] para se garantir a efetiva validade do consentimento dado. 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".[19]

No sentido de fortalecer o indivíduo, a Lei também estabelece que (Art. 9º, §3º), 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. Regula-se, assim, a lógica binária das chamadas políticas de tudo ou nada, em que o usuário ou aceita todas as disposições e termos do serviço ou não pode utilizá-lo.[20] Dessa forma, visa-se oxigenar processos de tomada de decisão, além de incentivar

[18] "Recital 43 clearly indicates that it is unlikely that *public authorities* can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. WP29 considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities (...) An imbalance of power also occurs in the *employment* context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1a)) due to the nature of the relationship between employer and employee" (*Guidelines on Consent under Regulation 2016/679*, p. 07-08).

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

[20] "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*. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.76)

configurações de privacidade personalizáveis e a possibilidade da manifestação do consentimento de forma granular.[21]

Na linguagem legislativa, o vocábulo *informado* significa que o titular do dado 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, direcionado a tratamento específico, para determinado agente e sob determinadas condições. Destaca-se, aqui, a importância dos princípios da transparência, adequação e finalidade para restringir tanto a generalidade na utilização dos dados quanto tratamentos opacos. Para diminuir a assimetria técnica e informacional existente entre as partes, exige-se que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados.[22]

Na lógica do consentimento informado, o artigo 9º da LGPD dispõe que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da: finalidade específica do tratamento (I); forma e duração do tratamento, observados os segredos comercial e industrial (II);[23] identificação do controlador (III); informações de contato do controlador (IV); informações acerca do uso compartilhado de dados pelo controlador e a finalidade (V); responsabilidades dos agentes que realizarão o

---

[21] "When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose. Example 7: Within the same consent request a retailer asks its customers for consent to use their data to send them marketing by email and also to share their details with other companies within their group. This consent is not granular as there is no separate consents for these two separate purposes, therefore the consent will not be valid. In this case, a specific consent should be collected to send the contact details to commercial partners. Such specific consent will be deemed valid for each partner (see also section 3.3.1), whose identity has been provided to the data subject at the time of the collection of his or her consent, insofar as it is sent to them for the same purpose (in this example: a marketing purpose)" (European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. Adotada em 04 de maio de 2020, p. 26).

22 "When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether or not to consent may not be hidden in general terms and conditions" (European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. Adotada em 04 de maio de 2020, p. 15).

[23] "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*, publicado em 12 de setembro de 2018).

tratamento (VI); e direitos do titular, com menção explícita aos direitos contidos no art. 18 (VII).[24-25]

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 ocorrer de forma clara. O consentimento do titular apresenta-se no Art. 7º como a primeira possibilidade para a realização do tratamento de dados, 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, o consentimento não poderá ser extraído da omissão do titular, mas tão somente de atos positivos que revelem claramente sua real vontade.[26] Outro cuidado expresso na norma é a disposição que estabelece que caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei, observando-se o princípio da responsabilização e prestação de contas.[27]

[24] 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.

[25] "Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm".). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given" (European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. Adotada em 04 de maio de 2020, p. 18).

[26] Como, por exemplo, por meio de click em botão, marcação de opção em caixa (que deve vir desmarcada) ou gravação confirmando a aceitação.

[27] Tomando como base o art. 224 do CC, recomenda-se que termos de uso, políticas de privacidade e demais informações sobre produtos e bens sejam sempre traduzidas para o português. Art. 224. Os documentos redigidos em língua estrangeira serão traduzidos para o português para ter efeitos legais no País.

A *finalidade* da coleta dos dados deve ser sempre previamente conhecida, seja qual for a base legal utilizada. Essa diretriz[28] diz respeito à relação entre os dados colhidos e a finalidade perseguida pelo agente. Apresenta 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.[29] Defende-se 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. Isso viria através da lógica do consentimento granular.

No caso de dispensa da exigência do consentimento previsto no Art.7º, §4º, para os dados "tornados manifestamente públicos pelo titular",[30] os agentes de tratamento continuarão obrigados a observar os direitos do titular e os princípios previstos na Lei. Assim como na hipótese dos dados de acesso público,[31] 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 sejam considerados públicos, não deixam de ser pessoais, sendo necessário considerar sempre a finalidade da circulação e o que justifica sua disponibilização.[32] Vale recordar, aqui, dados cuja divulgação pública é obrigatória por lei: como o fato de alguém ser proprietário de um imóvel ou sócio de uma empresa ou os dados acerca de determinadas atividades de órgãos públicos. Outro exemplo é a consulta de CPFs no site da Receita Federal com o propósito de mera confirmação da titularidade para operações financeiras.

Nesse sentido, 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

---

[28] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (...).

[29] RODOTÀ, Stefano, op. cit., p. 59.

[30] A doutrina oferece dois 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, op. cit., p. 271).

[31] 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.

[32] BIONI, Bruno, op. cit., p. 269-270.

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.[33-34] 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.

De forma geral, dispôs a Lei que eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas na Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular (Art. 7º, § 6º).

---

[33] Essa previsão, aliás, encontra semelhança no art. 9º, § 2º, alínea 'e' do GDPR, que reconhece como possível base legal para o tratamento de dados pessoais - no caso do GDPR dados sensíveis - quando tiverem sido manifestamente tornados públicos pelo seu titular. Isso não quer dizer, contudo, que basta que o dado pessoal tenha sido, por exemplo, disponibilizado online por seu titular. Para que um dado seja considerado como tornado manifestamente público pelo seu titular, deve restar inequívoco que ele pretende e espera que seus dados pessoais sejam tratados ulteriormente. Além disso, como previsto no próprio § 4º do Art. 7º da LGPD, devem ser observados os direitos do titular e os princípios previstos na LGPD.

[34] "On the other hand, such data would have to be made public by the data subject, and more than that, manifestly made public, so as to indicate that they wish and expect such data to be further processed. No need to mention that all other provisions, including the principles and the Article 6, still apply, and also the personal data may be processed only if the purpose of the processing could not reasonably be fulfilled by other means" (FOITZIK, Piotr. Publicly available data under the GDPR: Main considerations. Disponível em: <https://iapp.org/news/a/publicly-available-data-under-gdpr-main-considerations/>. Acesso em: 03.05.20). No mesmo sentido v. Information Commissioner's Office (ICO). What are the conditions for processing? Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/>. Acesso em: 03.05.20. O ICO apresenta algumas questões a serem respondidas para se verificar se determinado dado pessoal pode ser considerado como tendo sido tornado manifestamente público por seu titular: "So to use this condition, you should consider some specific questions: Is the special category data already in the public domain – can a member of the public realistically access it in practice? Who made the data public – was it the individual themselves or was it someone else? In what context was it made public – for example was it due to them giving an interview, standing for public office, or writing a book, blog or social media post? Did the individual deliberately take the steps which made this special category data public, or was it accidental or unintentional? Did they make a clear decision? Is the individual likely to have understood that their action means that their special category data is in the public domain?".

Quanto à eficácia subjetiva, o consentimento está vinculado ao controlador para o qual foi dado. O controlador que obteve o consentimento referido no inciso 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 na Lei. A partir dessa disposição, afirma-se que existiria dever que não se restringiria apenas ao controlador originário, devendo ser observado por todos aqueles que tenham acesso aos dados, dos quais se exigiria o dever de verificar a licitude do procedimento de acesso ou compartilhamento, inclusive no que tange ao consentimento específico do titular.[35]

Outra disposição relevante afirma que o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Logo, o consentimento será temporário. 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, entre cujos atributos se encontra 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, podendo o intérprete guiar-se por mecanismos como o *venire contra factum proprium*. 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,[36] resguardado o interesse público (Art. 15, III). Como o consentimento pode ser dado e depois revogado pelo titular, muitas vezes será

[35] BIONI, Bruno, op. cit., p. 269-270.
[36] 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.

melhor para as empresas terem uma base legal alternativa para legitimar o tratamento de dados.[37]

3. Aplicação do legítimo interesse

O legítimo interesse é hipótese legal que visa a possibilitar tratamentos de dados importantes, vinculados ao escopo de atividades praticadas pelo controlador, e que encontrem justificativa legítima. Diante da flexibilidade dessa base legal, as expectativas do titular[38] dos dados têm peso especialmente relevante para sua aplicação, devendo ser consideradas também a finalidade, a necessidade e a proporcionalidade da utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse.

Incluem-se, aqui, tratamentos em que a obtenção do consentimento do titular poderia criar óbice para a exploração regular de dados pessoais, que atenda a interesses legítimos do controlador ou de terceiros, ou quando se constatar que outras bases legais

---

[37] "(...) in practice, entities often based their processing activities on several legal bases. For example, where an entity processed personal data based on their necessity for the performance of a contract, said entity would often also obtain the data subject's consent. This preventive approach aimed at securing the lawfulness of the processing operations in case one or several of the used legal bases would lose their legitimacy. This approach can be upheld under the GDPR. However, entities should choose a primary legal permission among the available options. This is advisable as, under the Regulation, the conditions for obtaining valid consent, as well as those regarding other legal bases for processing, have been specified and tightened. Therefore, entities should—prior to processing—evaluate which legal basis might be most suitable for their processing activities. Under the principle of accountability (see Sect. 3.1), entities must be able to prove that the legal bases they use are fulfilled, e.g., when processing personal data based on their prevailing legitimate interests, entities must be able to demonstrate their interests, as well as the legitimacy of the latter" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A Practical Guide. Springer, 2017, p. 101).

[38] Como exemplos de legítima expectativa de tratamento dados, vale trazer o seguinte exemplo: "An individual uploads their CV to a jobs board website. A recruitment agency accesses the CV and thinks that the individual may have the skills that two of its clients are looking for and wants to pass the CV to those companies. It is likely in this situation that the lawful basis for processing for the recruitment agency and their clients is legitimate interests. The individual has made their CV available on a job board website for the express reason of employers being able to access this data. They have not given specific consent for identified data controllers, but they would clearly expect that recruitment agencies would access the CV and share with it their clients, indeed, this is likely to be the individual's intention. As such, the legitimate interest of the recruitment agencies and their clients to fill vacancies would not be overridden by any interests or rights of the individual. In fact, those legitimate interests are likely to align with the interests of the individual in circulating their CV in order to find a job". Outro exemplo a se mencionar seria: "An individual creates a profile on a social networking website designed specifically for professional networking. There is a specific option to select a function to let recruiters know that the individual is open to job opportunities. If the individual chooses to select that option, they would clearly expect those who view their profile might use their contact details for recruitment purposes and legitimate interests may be available (subject to compliance with other legal requirements, and PECR in particular). However, if they choose not to select that option, it is not reasonable to assume such an expectation. The individual's interests in maintaining control over their data – particularly in the context of the PECR requirement for specific consent to receive unsolicited marketing messages – overrides any legitimate interests of a recruitment agency in promoting its services to potential candidates". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test>. Acesso em: 10.02.20.

não são adequadas para lidar com o tratamento realizado no contexto da internet das coisas e do Big Data. Em muitas situações, pode ser desnecessário coletar novo consentimento para outros usos implícitos dentro de uma relação já preestabelecida. Além disso, quando o interesse for de terceiro, a base poderá ser aplicada em situações em que eles não tiverem meios para obter tal tipo de autorização ou se esse tipo de interação inviabilizar o próprio tratamento dos dados.[39]

Mostrar que há um interesse legítimo significa que o controlador (ou um terceiro) deve ter algum benefício ou resultado claro e específico em mente. Não basta afirmar a existência de interesses comerciais vagos ou genéricos. Deve-se pensar detalhadamente no que se está tentando alcançar com a operação de tratamento específica. Embora determinado objetivo possa ser potencialmente relevante, ele deverá ser "legítimo". Qualquer interesse ilegítimo, antiético ou ilegal não será um interesse legítimo para a LGPD.

Exemplos de aplicação da base legal do legítimo interesse são: a) o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle de fraudes[40] ou para garantir a segurança da rede e da informação nos sistemas informáticos de determinada instituição; b) fornecimento de imagens de câmeras de segurança para fins de seguro;[41] c) segurança e melhoria de produtos e serviços; d) tratamentos de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar; e) no caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando apenas os dados estritamente necessários para tal;[42] f) envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compras, tomando como base seu histórico de compras; g) lembrar ao usuário que ele deixou itens no carrinho online, mas não

---

[39] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 232.

[40] "Algo bastante comum é a criação de perfis comportamentais dos consumidores para combater fraudes e incidentes de segurança, pelos quais se diagnosticam atividades que fogem do padrão para tratá-las como suspeitas. É por esse motivo que serviços de e-mail, rede social e instituições financeiras alertam seus clientes e, em muitos casos, bloqueiam automaticamente acessos e transações financeiras. Por exemplo, se o acesso a uma conta parte de um dispositivo diferente, se a compra supera valores e é realizada em locais que não aqueles usuais. Todos esses dados informam ações de combate a fraudes e incidentes de segurança" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p. 241).

[41] Nesse exemplo, também, a finalidade é a prevenção e controle das fraudes, só que na esfera securitária.

[42] "*marketing* direto: há situações nas quais o titular do dado já mantém uma relação com o controlador, como no caso de ele já ter adquirido seus produtos e serviços. A partir desse histórico de compras, é possível lhe direcionar anúncios publicitários condizentes com o seu padrão de consumo. Por exemplo, é o que uma loja de vinhos faria com consumidores que gostassem mais de uma determinada uva, o que livrarias fariam com clientes que gostassem mais de um determinado autor, e assim por diante" (BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 250).

finalizou a compra; e h) reunião de informações sobre determinado candidato em processos seletivos. Por ser um conceito em construção, caberá principalmente a Autoridade Nacional de Proteção de Dados (ANPD) e ao Poder Judiciário preenchê-lo no caso concreto.[43]

Na LGPD, essa hipótese legal não foi disponibilizada para o tratamento de dados sensíveis, devendo a atividade ser encaixada nas demais bases legais dispostas no art. 11 da lei, que traz entre elas a possibilidade de tratamento para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, e o exercício regular de direitos em contrato.

Diante da necessidade de se trazer maior concretude para tal requisito, tanto a LGPD quanto a experiência internacional, notadamente a europeia, propõem alguns parâmetros interpretativos para sua aplicação. O antigo Grupo de Trabalho do Artigo 29 (*Working party 29*),[44] em seu parecer sobre o requisito do legítimo interesse, que serviu de base para o texto do GDPR, propôs a utilização de um teste: o *legitimate interest assessment* (LIA) ou teste da ponderação.[45] Busca-se, assim, balancear os direitos do titular dos dados e de quem faz uso das suas informações, verificando-se tanto se há um interesse legítimo de quem trata os dados quanto se estão sendo respeitadas as legítimas expectativas e os direitos e liberdades fundamentais dos titulares.

Destaca-se que o *legitimate interest assessment* apresenta quatro fases que devem ser cumpridas de modo a se verificar o preenchimento do requisito do legítimo interesse. São elas: (i) a avaliação dos interesses legítimos; (ii) o impacto sobre o titular do dado; (iii) o equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado.[46-47]

---

[43] Cf. BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Editora Revista dos Tribunais, 2019.

[44] No texto da GDPR (art. 68 e ss)., o colegiado foi transformado no *European Data Protection Board*.

[45] Grupo de trabalho do artigo 29.º para a proteção de dados. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. Adotado em 9 de abril de 2014. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf>. Acesso em 14.08.19.

[46] PEREIRA DE SOUZA, Carlos Affonso; VIOLA, Mario; PADRÃO, Vinicius. Considerações iniciais sobre os interesses legítimos do controlador na lei geral de proteção de dados pessoais. *Direito Público*, v. 16, n. 90, dez. 2019.

A LGPD igualmente estabelece parâmetros, em um rol exemplificativo, para a utilização do interesse legítimo como requisito autorizativo para o tratamento de dados sem o consentimento do titular, conforme se depreende de seu artigo 10:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Os dispositivos da LGPD que tratam dos interesses legítimos (arts. 7º, IX, e 10) possibilitam a transposição de parte do mencionado teste para avaliar a existência de legítimo interesse no caso concreto.

---

47 Tratando da aplicação do legítimo interesse e do teste de ponderação, o Guide to the General Data Protection Regulation - desenvolvido pelo Information Commissioner's Office (ICO) do Reino Unido - afirma que: "It makes most sense to apply this as a test in the following order: Purpose test – is there a legitimate interest behind the processing? Necessity test – is the processing necessary for that purpose? Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms? This concept of a three-part test for legitimate interests is not new. In fact the Court of Justice of the European Union confirmed this approach to legitimate interests in the Rigas case (C-13/16, 4 May 2017) in the context of the Data Protection Directive 95/46/EC, which contained a very similar provision. This means it is not sufficient for you to simply decide that it's in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test>. Acesso em: 10.02.20.

O Art. 10, em seu *caput* e inciso I, traz a necessidade de avaliação da existência de uma finalidade legítima e de uma situação concreta. Segundo Bioni,[48] o primeiro passo é verificar se o interesse do controlador é legítimo (finalidade legítima), ou seja, se ele não contraria, por exemplo, outros comandos legais (leis esparsas e legislação infralegal). Deve-se observar se está presente algum benefício ou vantagem com o uso dos dados por parte do controlador. A partir disso, analisa-se se tal interesse está claramente articulado, para que não chancele um uso genérico de dados. É necessário também perquirir se há uma situação em concreto (bem definida e articulada) que lhe dê suporte.

Em seguida, o §1º do Art. 10 traz a ideia do princípio da necessidade/minimização. Verifica-se, nessa etapa, se os dados coletados são realmente necessários para se atingir a finalidade pretendida e se o tratamento dos dados não seria coberto por outras bases legais da LGPD.

No inciso II do art. 10, há a ideia do balanceamento de interesses, trabalhando com a legítima expectativa do titular do dado e seus direitos e liberdades individuais. Essa é a principal fase do teste de proporcionalidade em que se balanceia os interesses do controlador e de terceiros diante dos do titular dos dados. Analisa-se, aqui, se o novo uso atribuído ao dado está dentro das legítimas expectativas do titular: "Isso é parametrizado pela noção de *compatibilidade* entre o uso adicional e aquele que originou a coleta dos dados. Eles devem ser próximos um do outro, demandando-se uma análise *contextual* para verificar se esse uso secundário seria esperado pelo titular dos dados".[49] Adicionalmente, deve-se verificar como os titulares serão impactados, principalmente se poderão sofrer discriminações. No caso de ser o legítimo interesse de terceiro, isto é, de alguém que não mantém uma relação já preestabelecida com o titular dos dados, afirma Bioni que: "a noção de legítima expectativa mostra-se mais difícil de ser demonstrada e o risco da aplicação dessa base legal é ainda maior".[50]

Por fim, nos §§2º e 3º do art. 10 são encontradas as salvaguardas, como exigências de transparência e mecanismos de oposição (*opt out* - podendo o cidadão optar por estar fora do que considerar ser incompatível com as suas legítimas expectativas) e de mitigação de riscos aos titulares dos dados (por exemplo, pseudonimização).[51]

---

[48] BIONI, Bruno. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020
[49] BIONI, Bruno, op. cit., p. 237.
[50] BIONI, Bruno, op. cit., p. 238.
[51] BIONI, Bruno, op. cit., p. 253 e ss.

Vale destacar, contudo, que esse requisito apenas legitima o tratamento de dados pessoais no limite necessário para a finalidade a qual ele se propõe e que o agente de tratamento deverá manter registro das operações de tratamento de dados que realizar, especialmente quando baseado no legítimo interesse (Art. 37). Justamente pela maleabilidade do legítimo interesse, recomenda-se a feitura de relatório de impacto à proteção de dados pessoais,[52] de forma a se minimizar os riscos para os dois lados da relação.

Segundo Leonardi, o teste acima mencionado deverá ser documentado, com base no par. 3º, do art. 10, da LGPD, já que o relatório "poderá" ser solicitado pela ANPD ao controlador, o que significa que ele já deverá ter sido preparado no momento da decisão pela utilização do legítimo interesse e antes que qualquer tratamento com base nessa hipótese ocorra.[53] Situação diversa encontra-se no art. 38 da lei, deixando claro o legislador que neste caso não se espera a prévia feitura do documento: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial".

É importante salientar que uma utilização adequada e inteligente dessa base legal proporciona e incrementa novos modelos de negócios e diversas estratégias comerciais,

[52] "Art. 5º (...) XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;" "Art. 38 (...) Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados".

[53] LEONARDI, Marcel. Legítimo interesse. *Revista do Advogado*, v. 39, 2019, p. 70.

de segurança e inovação, sendo necessário realizar um balanço perfeito entre interesse legítimo e legítimas expectativas e direitos dos titulares.[54]

Conforme dispõe o art. 7º, IX, os interesses legítimos poderão ser do controlador ou de terceiro, de forma que se pode incluir "interesses comerciais, individuais ou mesmo interesses da coletividade e da sociedade amplamente considerados".[55] Ponto interessante a se destacar é que o art. 10 da LGPD faz referência apenas ao controlador, devendo a doutrina e a ANPD esclarecerem se sua interpretação deverá ser ampliada. O termo "terceiro" não se refere apenas a outras organizações, podendo também ser um indivíduo não envolvido inicialmente de forma direta na relação ou o público em geral. Por exemplo, uma companhia de seguros deseja processar dados pessoais com base em interesses legítimos para identificar reivindicações fraudulentas. Em primeiro lugar, ela considera o teste de finalidade. É do interesse legítimo da empresa garantir que seus clientes não realizem fraudes contra ela. Adicionalmente, os clientes da empresa e o público em geral também têm interesse legítimo em garantir que a fraude seja evitada e detectada.[56]

---

[54] Nesse sentido, vale destacar os considerandos 47 e 48 do GDPR: "(47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta (48) Os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro mantêm-se inalterados".

[55] LEONARDI, Marcel. Legítimo interesse. *Revista do Advogado*, v. 39, 2019, p. 70.

[56] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test>. Acesso em: 10.02.20.

Outro exemplo interessante de aplicação do legítimo interesse oferecido pela Autoridade de proteção de dados do Reino Unido[57] é o seguinte: uma empresa financeira não consegue localizar um cliente que parou de efetuar pagamentos referentes a um contrato de compra e venda. O cliente mudou de residência sem notificar a empresa de seu novo endereço. Diante disso, a empresa deseja contratar uma agência de cobrança de dívidas para encontrar o cliente e solicitar o pagamento da dívida. Para tanto, deseja divulgar os dados pessoais do cliente à agência para essa finalidade. No caso, a empresa financeira tem interesse legítimo em recuperar a dívida que é devida e, para atingir esse objetivo, é necessário que ela use uma agência de cobrança de dívidas para rastrear o cliente. Na situação, mostra-se razoável que seus clientes esperem que ela tome medidas para buscar o pagamento de dívidas pendentes. Ainda que os interesses possam ser opostos entre cliente e empresa, sua atuação estaria dentro do razoavelmente esperado para a situação narrada, restando o saldo em favor da empresa financeira.

Dessa forma, podem ser concluídos alguns pontos em relação ao legítimo interesse: a) pode ser a base mais apropriada em diversas hipóteses, devendo, porém, ser aplicada de forma proporcional e limitada, quando trouxer benefício claro e determinado para o controlador e/ou terceiro; b) poderá ser aplicado quando não causar um impacto elevado aos direitos e garantias do indivíduo; c) o indivíduo – titular dos dados – deverá esperar razoavelmente que seus dados sejam usados dessa maneira; e d) poderá ser aplicado quando não for possível ou não se desejar dar ao titular dos dados total controle ou, ainda, quando o controlador não quiser incomodá-lo com solicitações de consentimento para tratamentos que muito provavelmente seriam aceitos pelo titular.

4. Demais bases legais para o tratamento de dados pessoais

Ao longo do artigo 7º da LGPD são apresentadas outras hipóteses legais para o tratamento de dados pessoais, não havendo, aqui, nenhuma superior às demais, conforme destacado em tópico específico (item 2). Entende-se que, ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a base mais *adequada* e *segura* para a situação concreta.

[57] Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test>. Acesso em: 10.02.20.

Logo após a previsão relativa ao consentimento, afirma-se que o tratamento de dados pessoais poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador, como obrigações trabalhistas, deveres oriundos da lei anticorrupção e a guarda de registros por determinados provedores na forma do Marco Civil da Internet. Outro exemplo são as empresas do setor de seguros ou do mercado financeiro, as quais estão submetidas a várias regras legais e regulatórias e devem cumprir obrigações que eventualmente poderão exigir o tratamento de dados pessoais de seus clientes. Uma política de privacidade e tratamento de dados bem desenhada e transparente pode ajudar a melhor esclarecer o uso dessa base legal pela instituição.

Em seguida, aborda-se o tratamento de dados pessoais pela administração pública, para o tratamento e uso compartilhado[58] de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da lei, que regula o tratamento de dados pessoais pelo Poder Público. As políticas em questão podem envolver, por exemplo, a implementação de saneamento básico, de auxílios a cidadãos em situação de vulnerabilidade ou de projetos voltados à educação de crianças e adolescentes.

Execução de políticas públicas é uma das justificativas para que o setor público realize tratamentos de dados. Esse requisito encontra-se intimamente ligado à previsão estabelecida no artigo 23 da LGPD que dispõe que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único, do art. 1º, da Lei nº 12.527/11 (Lei de Acesso à Informação)[59] deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público,[60] desde que: a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam

[58] Art. 5º, XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

[59] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

[60] Doneda e Mendes defendem que o caput do art. 23 da LGPD traz uma base legal adicional para o tratamento de dados pela administração pública, além daquelas previstas no art. 7º. Cf. MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555, 2018.

o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e b) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais. Parece-nos que a previsão contida no art. 23 traz requisitos adicionais para o tratamento de dados pessoais por parte da Administração Pública, já que, conforme destacamos no item 1, entendemos que a base legal relativa ao tratamento de dados pessoais pela Administração Pública na execução de suas competências legais ou no cumprimento das atribuições legais do serviço público é o cumprimento de uma obrigação legal ou a própria execução de políticas públicas, na forma do que preveem os artigos 7º e 11 da LGPD.

Pode-se também tratar dados para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Dispõe a lei, em seu Art. 5º, XVIII, que órgão de pesquisa representa "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". Em relação à anonimização[61] — utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo —, entende a Lei que essa situação seria mais protetiva para os titulares, vez que dado anonimizado é o dado relativo a titular que não possa ser identificado, ou seja, uma vez anonimizado, o dado deixa de ser pessoal, segundo o art. 12 da LGPD.

[61] "Para proteger a privacidade dos indivíduos as bases de dados anonimizadas podem se valer de vários expedientes, como ocultar algumas informações, generalizar outras e assim por diante. Então ao invés de saber quem exatamente visitou o meu estabelecimento eu sei que essa pessoa é homem ou mulher e que tem uma idade entre 40-50 anos, só para continuar com o exemplo. Somando todas as entradas na base de dados eu consigo gerar uma visualização de quantos % do meu público é de cada faixa etária, gênero e assim por diante. Acontece que quanto mais informações eu jogo nessa base, mais fácil fica reidentificar a pessoa cujo dado foi anonimizado. Chegamos então em uma encruzilhada: como criar uma base de dados anonimizados que possa atingir o equilíbrio entre utilidade para quem se vale dela e ao mesmo tempo não saia por aí revelando a identidade de todo mundo? (...) para o dado ser considerado como anonimizado eu preciso olhar para dois fatores: um objetivo e outro subjetivo. Por fatores objetivos no conceito de "esforços razoáveis" a própria lei menciona "o custo e o tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis" (art. 12, §1º). Já os fatores subjetivos olham para quem fez o processo de anonimização e para quem está tentando quebrá-lo (SOUZA, Carlos Affonso. Eles sabem quem é você? Entenda o monitoramento de celulares na quarentena. Disponível em: <https://tecfront.blogosfera.uol.com.br/2020/04/17/eles-sabem-quem-e-voce-entenda-o-monitoramento-de-celulares-na-quarentena/>. Acesso em: 03.05.20). Conferir também: Paul Ohm. Broken promises of privacy: responding to the surprising failure of anonymization. 57 *UCLA Law Review* 1701 (2010); BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. Direito Digital e proteção de dados pessoais. *Cadernos Jurídicos*. Ano 21 - Número 53 - Janeiro-Março/2020, p. 191-201.

Por exemplo, prática utilizada pelos órgãos de pesquisa com o intuito de anonimizar os dados é quando em uma pesquisa para apuração de intenção de votos em uma eleição as informações são alocadas levando em conta sexo, escolaridade, região geográfica e classe social dos indivíduos de maneira agregada. A partir dessas distinções, verifica-se a proporção de votação para cada candidato. O resultado da pesquisa é resumido ao ponto que se torna praticamente impossível saber quem foram as pessoas que expressaram aquelas intenções, devendo a instituição garantir a segurança desses dados e sua anonimização nos bancos de dados.

Vale lembrar também que, de acordo com o art. 13, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização[62] dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. Acrescenta-se que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Outra hipótese autorizativa do tratamento de dados está presente quando for necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. A disposição em questão é mais ampla do que aquela prevista no art. 11, II, "d",[63] da LGPD, podendo o agente tratar, sem consentimento, os dados que são necessários para a contratação, bastando que o titular seja parte ou esteja em tratativas para um contrato. É possível trabalhar, aqui, dois exemplos: a) nas situações em que o titular adquira produtos ou serviços para entregá-los será preciso conhecer o nome completo, o endereço e outras

[62] Art. 13 § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
[63] Art. 11, II, d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).

informações de contato do consumidor;[64] e b) levantamentos realizados por instituições financeiras em relação a determinada pessoa, anteriormente à concessão de crédito a ela. No campo dos seguros, essa base apresenta importância pois é necessário realizar análises preliminares para subsidiar a contratação (conhecimento do risco), como também para cumprir o contrato, como no caso da regulação de um sinistro, do fornecimento de assistência 24 horas, da inspeção de risco etc.[65]

Essa hipótese se assemelha em alguma medida ao tratamento de dados via consentimento. Todavia, como traço distintivo marcante, ressalta-se que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a execução do contrato. No mesmo sentido, foi estabelecida base legal no Regulamento europeu de proteção de dados, em seu art. 6º: se o tratamento for necessário para a execução de um contrato do qual o titular dos dados seja parte ou para diligências pré-contratuais a pedido do titular dos dados.[66-67] Nessa base legal fica clara a distinção entre "consentimento" para se tornar parte de um contrato e "consentimento" para fins de tratamento de seus dados pessoais.

---

[64] No entanto, o *profiling* dos interesses e preferências de um indivíduo com base nos itens adquiridos não é necessário para a execução do contrato e o responsável pelo tratamento não pode confiar nessa base legal como referência para esse processamento. Mesmo que esse tipo de publicidade direcionada seja uma parte útil do relacionamento com o cliente e seja uma parte necessária do modelo de negócios desse fornecedor, não é necessário executar o contrato propriamente dito. Isso não significa que o processamento que não é necessário para o contrato seja automaticamente ilegal, mas que você precisa procurar uma base legal diferente e outras salvaguardas. Fonte: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/>. Acesso em: 29.04.20

[65] Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.26. Disponível em: <http://cnseg.org.br/data/files/AF/63/3B/7E/B8B6F610373532F63A8AA8A8/GBPMS_ONLINE_ok.pdf>. Acesso em: 29.04.20

[66] "When is the lawful basis for contracts likely to apply? You have a lawful basis for processing if: you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract. you have a contract with the individual and you need to process their personal data so that they can comply with specific counter-obligations under the contract (eg you are processing payment details). you haven't yet got a contract with the individual, but they have asked you to do something as a first step (eg provide a quote) and you need to process their personal data to do what they ask. This applies even if they don't actually go on to enter into a contract with you, as long as the processing was in the context of a potential contract with that individual". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/> Acesso em: 29.04.20.

[67] Para esta hipótese, doutrina aponta o seguinte exemplo: "Entity X runs an online shop, and a customer purchases X's products. X is permitted to process the customer data based on Art. 6 Sec. 1 phrase 1 lit. b GDPR to the extent necessary for the performance of the contract with the customer. In this example, in order to deliver the products to the customer and, thus, fulfil its obligations under the purchase agreement, X has to process the name and address of the customer, the types and amount of articles purchased, the method of payment and shipping information. Based on the method of payment, X might have to process the bank account details of the customer. For example, if the customer will pay on a cash-on-delivery basis, X will not need the bank account details in order to make the delivery. Other personal data should not be necessary unless the purchased articles are subject to statutory distribution conditions (such as age restrictions, subsequent to which X has to process the customer's age)" (VOIGT, Paul; BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR)*. A Practical Guide. Springer, 2017. p.102)

O tratamento também pode ter como base o exercício regular de direitos em processo judicial, administrativo ou arbitral (nos termos da Lei nº 9.307/96). Há, aqui, base legal ampla que autoriza o uso de dados pessoais em processos para garantir o direito de produção de provas de uma parte contra a outra. O exercício regular de direitos compreende ações do cidadão comum autorizadas pela existência de direito definido em lei e condicionadas à regularidade do exercício desse direito. Dentro dessa hipótese, não pode haver conduta abusiva ou o desempenho disfuncional de certa posição jurídica pela parte. Afirma a doutrina que, nos casos em que se entender que determinados dados poderão servir como elementos para o exercício de direitos em demandas, eles poderão ser armazenados, desde que havendo real necessidade e para essa finalidade.[68] Entende-se que não seria razoável que uma parte ficasse privada de legitimamente se defender, tendo que depender do consentimento da parte adversa para apresentar determinadas provas ou informações para a defesa de seus interesses. Protege-se, assim, a ampla defesa e o contraditório.

No rol de possibilidades, tutela-se ainda a proteção da vida ou da incolumidade física do titular ou de terceiro. A aplicação da hipótese parece ser razoável em situações excepcionais e pontualmente, não sendo cabível para justificar ações genéricas. Recorda-se o seguinte exemplo: obtenção de dados de geolocalização de celulares visando encontrar pessoas desaparecidas em desastres e escombros ou que possam ter sido sequestradas ou estar perdidas.[69] Outra aplicação dessa base poderia ser para o tratamento de dados importantes para se conter o avanço de epidemias, como o recente caso do COVID-19.

Em seguida, autoriza-se o tratamento para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. A saúde enquanto direito fundamental recebeu tutela específica na Lei, de onde se pode tirar alguns questionamentos: quem seriam os profissionais de saúde e quais serviços seriam considerados de saúde? Um plano de saúde por exemplo poderá utilizar de forma ampla tal base legal? Quais riscos à pessoa isso implicará? A tutela da saúde nesse dispositivo seria especificamente da pessoa a quem esses dados dizem respeito ou poderia envolver uma coletividade ou grupo específico? O cuidado com a mencionada base deve existir entre outras razões porque, a partir da solicitação de exames ou da análise de dados de saúde, é possível inferir inclusive situações sensíveis

[68] LIMA, Caio César C. Seção I - Dos Requisitos para o Tratamento de Dados Pessoais. MALDONADO, Viviane Nóbrega; BLUM, Renato (Coord.). *LGPD Lei Geral De Proteção De Dados*. Revista dos Tribunais, 2019, p. 184.
[69] LIMA, Caio César C., op. cit., p. 185.

sobre determinada pessoa e, se utilizados de maneira inadequada, podem dar ensejo a discriminações ilegítimas ou abusivas (Art. 6º, IX). Em relação à autoridade sanitária, recorda-se a Lei nº 9.782/99, que define o Sistema Nacional de Vigilância Sanitária e cria a Agência Nacional de Vigilância Sanitária.

Como penúltima base, dispõe a Lei que o tratamento de dados poderá ser realizado quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, conforme tratado no item de número 3 do presente artigo.

Por fim, a última base legal para o tratamento de dados [não sensíveis] refere-se à proteção do crédito. Espera-se que, por meio dela, os tratamentos realizados busquem ampliar e facilitar a concessão de crédito, melhorar as análises de risco e impulsionar o mercado de consumo. Nesse caso, a base deverá restar em constante diálogo com normas como o Código de Defesa do Consumidor (Lei nº 8.078/90), a lei do cadastro positivo (Lei nº 12.414/11) e portarias do Ministério da Justiça.[70]

Informação e transparência são direitos básicos do consumidor, devendo ele ter acesso de forma clara e objetiva a todos os aspectos da relação contratual e a forma como seus dados são tratados. Como mencionado no Recurso Especial nº 1.348.532, a partir da exposição de dados financeiros do consumidor abre-se possibilidade para intromissões diversas em sua vida: "Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas".[71]

Tema que diretamente se relaciona com a base legal acima envolve o *credit scoring*, que pode ser compreendido como um sistema de pontuação utilizado pelas instituições que operam com relações comerciais ou creditícias, que tem como finalidade auxiliar na tomada de decisões relativas à concessão de crédito a determinado consumidor. Essa pontuação toma como base diversas variáveis, como idade, sexo, estado civil, profissão, renda, histórico de adimplemento de outras operações de crédito, entre outras. Essa prática comercial foi considerada lícita pelo STJ, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei nº 12.414/11.

---

[70] Como, por exemplo: Portaria SDE nº 005, de 27 de agosto de 2002 (Complementa o elenco de cláusulas abusivas constante do art. 51 da Lei nº 8.078, de 11 de setembro de 1990.). Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/legislacao> Acesso em: 21.04.19.
[71] STJ. REsp 1.348.532 – SP. Rel. Min. Luis Felipe Salomão. DJe: 30/11/2017.

Todavia, no Recurso Especial nº 1.419.697[72] foi estabelecido que na avaliação do risco de crédito devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, como disposto no CDC e na Lei 12.414/11. Além disso, no tocante ao sistema *scoring* de pontuação, afirmou-se que, "Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas".[73]

Segundo a lei do cadastro positivo, ficam proibidas anotações de informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor, e informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (Art. 3º, §3º). A vedação do uso de dados sensíveis busca evitar a utilização discriminatória da informação e garantir o dever de respeito à privacidade do consumidor. Como decidido no REsp 1.419.697, não podem ser valoradas pelo fornecedor do serviço de *credit scoring* informações sensíveis, ficando caracterizado abuso do direito pela utilização de informações sensíveis, excessivas, incorretas ou desatualizadas. Destaque-se que, no referido Recurso, o STJ entendeu que dentre as informações consideradas "excessivas" estão as referentes aos gostos pessoais e, até mesmo, filiação a clube de futebol.[74]

Após a análise das dez bases que compõem o rol do Art. 7º, encerra-se esse item recordando as hipóteses estabelecidas no GDPR para a licitude do tratamento. Seu artigo 6º ressalta que o tratamento só será lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) o tratamento for necessário para a execução de um contrato do qual o titular dos dados seja parte ou para diligências pré-contratuais a pedido do titular dos dados; c) o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) o tratamento for

[72] STJ. REsp 1.419.697/RS (submetido ao regime dos recursos repetitivos), Rel. Min. Paulo de Tarso Sanseverino. DJe 17/11/2014.
[73] Súmula 550 do STJ: "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo" (Segunda seção, julgado em 14/10/2015, DJe 19/10/2015)
[74] Veja-se, a esse título, *Transparência e Governança nos algoritmos: um estudo de caso sobre o setor de birôs de crédito*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf>. Acesso em: 30.07.19.

necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; ou 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.

5. Tratamento de dados sensíveis

Os dados pessoais qualificados como sensíveis se encontram presentes em todos os conjuntos informacionais do ser humano. Na LGPD — assim como no GDPR —, entendeu o legislador que a melhor forma de os proteger seria trazendo exemplos claros de dados assim considerados.[75] Portanto, segundo o art. 5º, inciso II, da LGPD, dados sensíveis versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São também sensíveis aqueles referentes à saúde ou à vida sexual e dados genéticos[76] ou biométricos.[77]

Cuida-se de dados especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, cujo contexto propicia riscos significativos para seu titular.[78] Eles integram o "núcleo duro" da privacidade, tendo em vista que, pelo tipo e natureza de informação que trazem, apresentam informações cujo tratamento pode ensejar a

[75] "(...) 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).

[76] 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".

[77] Importante salientar que a definição de "informação sensível" não era estranha ao legislador pátrio, visto que tal definição - à exceção da referência a dados biométricos - já constava na Lei do Cadastro Positivo (Lei n. 12.414/11): Art. 3º, § 3º Ficam proibidas as anotações de: (...) II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

[78] No GDPR, em seu art. 9º, esses dados foram considerados como 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".

discriminação de seu titular, devendo, por conseguinte, ser protegidos de forma mais rígida.[79]

A respeito dessa especificação, vale questionar: em se tratando de informações pessoais, não seria mais adequado se trabalhar com um rol exemplificativo de dados sensíveis? Tendo em vista as diversas possibilidades de utilização e cruzamento de dados pessoais, haverá algum dado não potencialmente sensível?[80] Todos os dados considerados sensíveis pelo legislador se encontram na mesma esfera particular/ íntima do seu titular? Em que medida a criação de novas categorias de dados beneficiaria a pessoa humana?

Nessa direção, entende-se que essencial para se determinar se um dado é sensível ou não é verificar o contexto de sua utilização, além das relações que podem ser estabelecidas com as demais informações disponíveis e a potencialidade de seu tratamento servir como instrumento de estigmatização ou discriminação.[81] Como destaca doutrina: "(...) deve-se admitir que certos dados, ainda que não tenham, a princípio, essa natureza especial, venham a ser considerados como tal, a depender do uso que deles é feito no tratamento de dados".[82]

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; ou II – quando sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para determinadas situações expressas nas alíneas desse artigo: a) cumprimento de

[79] RODOTÀ, Stefano, op. cit., 78 e 96.
[80] "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*, n. 2, junho, 2019, ano 11, p. 12).
[81] Cf. 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 e ss.
[82] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, nov. 2019, p. 47-53, p. 49.

obrigação legal ou regulatória pelo controlador;[83] b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;[84] 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[85]; f) tutela da saúde,[86] exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos,[87] 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. Nessa situação, devem todos os cuidados já previstos para o tratamento dos dados ser aplicados de forma ainda mais intensa, já que para os dados sensíveis se espera um padrão ainda mais rigoroso de proteção.

Da leitura do dispositivo [Art. 11 da LGPD], verifica-se que ele mantém várias das bases já previstas no art. 7º para o tratamento de dados pessoais, deixando de fora do

[83] Exemplo: Os dados de prontuários médicos com até 20 anos devem ser mantidos pelo hospital, em razão de obrigação legal imposta pela Lei nº 13.787/18: Art. 6º Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados.
[84] Art. 11, II, § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
[85] Exemplo: pessoa inconsciente é levada para um hospital (onde nunca esteve), após sofrer grave acidente. Nesse caso, o novo hospital precisará de todo o histórico médico do paciente para atendê-lo de forma adequada. A partir dessa base legal, entende-se que poderá o médico que irá atendê-lo requisitar documentação a outro hospital onde o paciente já esteve ou ao médico de confiança dessa pessoa (se essa informação estiver disponível).
[86] "O tratamento de dados sensíveis na área de saúde recebe regramento diferenciado em diversos países, observando-se regras rígidas para a segurança dos dados. Em 1997, diante do alargamento do National Health Service do Reino Unido, foram desenvolvidos os princípios para a segurança das informações e dados pessoais na área médica, estabelecidos no Relatório Caldicott, encomendado por Dame Fiona Caldicott, a National Data Guardian for health no Reino Unido. Os "Princípios Caldicott" são essenciais no desenho da governança da segurança da informação na área de saúde e, também, em todas as outras áreas que tratem dados sigilosos, haja vista que são extremamente objetivos. Em uma tradução livre, são os seguintes: 1) justifique o propósito para a utilização da informação confidencial; 2) não use o dado pessoal confidencial a não ser que seja absolutamente necessário; 3) utilize o dado pessoal confidencial o mínimo necessário; 4) o acesso ao dado pessoal confidencial deve ser restrito àquelas pessoas que necessitam conhecê-lo; 5) toda pessoa com acesso ao dado pessoal confidencial deve estar ciente de suas responsabilidades; 6) o acesso ao dado pessoal confidencial deve estar de acordo com a legislação; 7) a obrigação de compartilhamento do dado confidencial pode ser tão importante quanto a obrigação de proteger a confidencialidade dos dados do paciente. A LGPD traz estes princípios na sua essência. Na área de saúde terá de ser desenvolvido um eficiente programa de governança, de compliance e de treinamento de pessoas para proteção dos dados sensíveis do paciente e a eficiência passa antes de mais nada pela conscientização das responsabilidades de cada um que participar da intrincada relação que se forma para a prestação da assistência à saúde" (RAEFFRAY, Ana Paula Oriola de. *A proteção de dados pessoais na área de saúde*. Estadão. Publicado em 20 de abril de 2019).
[87] Exemplo: A utilização de dados biométricos para fins de validação de operações bancárias realizadas em caixas eletrônicos.

tratamento de dados sensíveis as hipóteses de atendimento aos interesses legítimos do controlador ou de terceiro (Art. 7º, IX) e de proteção do crédito (Art. 7º, X).

No lugar da hipótese relativa ao legítimo interesse, o Art. 11, II, "g", trouxe base mais específica, que visa à prevenção de fraudes e garantir a segurança do titular, restando vinculada aos interesses dos titulares e determinadas entidades. Como exemplo de aplicação, aponta-se a seguinte situação: instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária por meio de um caixa eletrônico, por exemplo. Adicionalmente, pode-se mencionar a exigência para atendimento médico-hospitalar, com a utilização de seguro ou plano de assistência à saúde, que o segurado/beneficiário coloque seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilize a cobertura securitária em seu lugar.

Além disso, a norma acrescentou a possibilidade de exercício regular de direitos também em relação a um contrato (Art. 11, II, "d"), mas não replicou a disposição do Art. 7º, V.[88] Nesse caso, como exemplo, recorda-se a situação de um seguro saúde ou seguro de vida necessitar coletar informações sensíveis, com base no exercício regular de direitos, pois, sem o tratamento de tais dados, poderá não ser possível entregar a prestação que lhe compete decorrente da relação contratual, como o ressarcimento de despesas médicas no seguro saúde ou o pagamento de indenização por algum tipo de invalidez decorrente de acidente ou doença nos seguros de pessoas.[89] Afirma-se que, aqui, a seguradora não teria apenas o dever de cumprir a obrigação contratual, mas também o direito de adimpli-la. Da mesma forma, a doutrina europeia tratando de dispositivo similar no GDPR reconhece a possibilidade de uma seguradora – com base no exercício regular de direitos decorrentes de um contrato – tratar dados de saúde de

[88] Art. 7º, V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; (...).
[89] Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.31. Disponível em: <http://cnseg.org.br/data/files/AF/63/3B/7E/B8B6F610373532F63A8AA8A8/GBPMS_ONLINE_ok.pdf>. Acesso em: 29.04.20.

um segurado para verificar a regularidade de uma reclamação de indenização oriunda de um sinistro de seguros de pessoas.[90]

Retornando às hipóteses autorizativas para o tratamento de dados sensíveis, a primeira delas (Art. 11, I) refere-se ao consentimento do titular ou seu responsável legal, que deverá ser dado de forma específica e destacada, para finalidades específicas. Oferece-se na Lei camada adicional de proteção para que tais dados não sejam utilizados contra seus titulares, o que poderia lhes causar restrições a bens e serviços ou mesmo ao exercício de direitos.[91] Parte da doutrina encontra, nesse dispositivo, a existência de certa preferência a tal hipótese legal, com base na 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 ali estabelecidas nas alíneas. Interpretação essa com a qual discordamos e que já encontra crítica na doutrina:

> (...) tanto na hipótese de tratamento de dados sensíveis por meio do consentimento do titular quanto naquelas que se referem às demais situações que independem desta manifestação de autonomia, previstas nos incisos I e II do art. 11 da LGPD, reconhece-se na técnica legislativa utilizada uma posição de igualdade entre estas hipóteses, e não a de prevalência do consentimento.[92]

Um dos desafios será compreender a dimensão e o real significado do consentimento caracterizado como específico e destacado. Segundo doutrina, deve-se "enxergá-lo como um vetor para que haja mais *assertividade* do titular com relação a esses

[90] "Using sensitive data may also be necessary for a controller to establish, exercise or defend legal claims. Reliance on this criterion requires the controller to establish necessity. That is, there must be a close and substantial connection between the processing and the purposes. One example of an activity that would fall under this criterion is processing medical data by an insurance company in order to determine whether a person's claim for medical insurance is valid. Processing such data would be necessary for the insurance company to consider the claim brought by the claimant under their insurance policy" (USTARAN, Eduardo. *European Data Protection Law and Practice*. Portsmouth: IAPP, 2018, p. 88).

[91] "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*, publicado em 26 de setembro de 2018).

[92] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei geral de Proteção de Dados Pessoais. *Revista do Advogado*, n. 144, nov. 2019, p. 47-53, p. 52.

movimentos 'específicos' de seus dados".[93] A noção, no caso, aproxima-se da ideia de consentimento expresso, por exigir maior atuação do titular dos dados, além de cuidado mais elevado com o tratamento da informação pelo agente.

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 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.

Segundo a LGPD, será aplicada a proteção disposta no artigo 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, aprioristicamente, não sejam sensíveis podem assim se tornar quando, em determinado contexto fático, levarem a informações sensíveis a respeito dos titulares.[94] Um exemplo sempre recorrente na doutrina envolve a análise do histórico de compras de uma pessoa em um supermercado ou farmácia, ou ainda o acesso a fatura do principal cartão de crédito dela, uma vez que, a partir disso, seria possível inferir dados sensíveis, como convicções religiosas ou políticas, estado de saúde[95] ou orientação sexual.

---

[93] BIONI, Bruno, op. cit., 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 (...). 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, op. cit., p. 203).

[94] Sobre o ponto, anota 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, como resultado final, a informações sensíveis a respeito das pessoas" (FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *Jota*, publicado em 26 de setembro de 2018).

[95] Caso famoso envolve a empresa *Target* e o uso de dados para a realização de previsão de gravidez de clientes. Mais informações em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI317687-17579,00-A+CIENCIA+QUE+FAZ+VOCE+COMPRAR+MAIS.html> e <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>. Acesso em: 11.04.19.

Sobre o ponto acima, é necessário contextualizá-lo com a problemática atual: a COVID-19.[96] Diante do avanço da pandemia, o debate em torno de medidas que utilizam dados pessoais e sistemas de vigilância para combater o vírus tornou-se ainda mais importante. Até onde o interesse coletivo pode avançar sobre o individual? Quais mecanismos de rastreamento e coleta de dados serão aplicados e por quanto tempo? Quem terá acesso aos bancos de dados criados? Serão eles algum dia descartados? O que se mostra justificável diante de um cenário de pandemia global e qual legado isso deixará para o tema da proteção de dados? Perguntas apresentadas globalmente, mas ainda sem respostas.

Stefano Rodotà em "A Vida na Sociedade da Vigilância: a Privacidade Hoje" nos lembra que, em relação aos dados de saúde, "a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações".[97] Não há dúvida de que o conhecimento por parte de empregadores, companhias seguradoras, planos de saúde ou mesmo governos de informações sobre pessoas que foram infectadas – se não observadas salvaguardas adequadas – poderá causar discriminações, além de prejudicar determinadas contratações. Nesse cenário, dados de geolocalização, mesmo a princípio não sensíveis, podem ser facilmente manipulados para usos lesivos a seu titular e para verificação de informações íntimas.

Caso a LGPD já estivesse em vigor, ela ofereceria respaldo e segurança para o tratamento de dados (inclusive sensíveis) necessário, bem como disposições específicas para o Poder Público atuar. Atrasar sua entrada em vigor sem um compromisso por parte do Poder Público com a estruturação em curto prazo da Autoridade Nacional de Proteção de Dados, para que ela possa regulamentar os dispositivos da LGPD que dela dependem, apenas traz opacidade e maior intranquilidade para a conjuntura atual. Entende-se que ter uma Autoridade Nacional de Proteção de Dados em pleno funcionamento no Brasil seria de grande relevância para a orientação de profissionais, empresas, cidadãos e governo nessa situação de emergência.

---

[96] Trecho extraído de: TEFFÉ, Chiara Spadaccini de. A saúde na sociedade da vigilância: como proteger os dados sensíveis? Migalhas, publicado em 14 de abril de 2020. Disponível: <https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia-como-proteger-os-dados-sensiveis>. Acesso em: 03.05.20.

[97] RODOTÀ, Stefano. *A vida na sociedade da vigilância:* a privacidade hoje. Coord. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.106.

Em momentos excepcionais que exigem maior acesso e tratamento de dados, a fim de se proteger interesse maior, a disciplina da proteção de dados (nas dimensões individual e coletiva) não deve ser compreendida como empecilho ou despesa. É a partir dela, especialmente de seus princípios, que a utilização de informações pessoais poderá ter legitimidade e que limites e procedimentos específicos serão estabelecidos de acordo com o princípio da dignidade da pessoa humana e *standards* reconhecidos internacionalmente para a tutela de dados.

A adoção de medidas emergenciais, de forma proporcional e justificada, que restrinjam a liberdade individual para garantir a saúde pública pode ser necessária na conjuntura atual. Todavia, os agentes públicos e privados que tratarem informações pessoais deverão agir em conformidade com os limites fixados no ordenamento, evitando medidas arbitrárias que extrapolem a proporcionalidade na restrição de direitos individuais, sob pena de responsabilidade.

Voltando para os parágrafos do Art. 11 da LGPD, a comunicação ou o uso compartilhado de dados pessoais 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. Segundo a Lei, 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.

Enfim, o § 5º do Art. 11 dispõe que 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. Esse dispositivo deve ser lido em consonância com o que dispõe a Lei nº 9.656/98 (que versa sobre os planos e seguros privados de assistência à saúde) e seu art. 14, o qual estabelece que, em razão da idade do consumidor, ou da condição de

pessoa portadora de deficiência, ninguém pode ser impedido de participar de planos privados de assistência à saúde.[98]

Os dados sensíveis necessitam mais do que nunca de uma tutela diferenciada e especial, de forma a se evitar que informações dessa natureza sejam vazadas, usadas indevidamente, comercializadas ou sirvam para embasar preconceitos e discriminações ilícitas em relação ao titular. Todavia, a mera proibição do tratamento de dados sensíveis é inviável, pois, em alguns momentos, o uso de tais dados será legítimo e necessário, além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações desse gênero, como, por exemplo, algumas entidades de caráter político, religioso ou filosófico.[99]

Dessa forma, entende-se que o tratamento de dados sensíveis é possível e, inclusive, pode ser necessário em determinadas circunstâncias. Contudo, deverá ser pautado estritamente nos ditames legais, pela relevância dos valores em questão, e legitimado apenas quando tal tratamento não servir para a realização de discriminações ilícitas ou abusivas. Esse entendimento restou reforçado com o princípio da não discriminação, previsto no inciso IX, do art. 6º, da LGPD, que estabeleceu a impossibilidade de realização de tratamento de dados para fins discriminatórios ilícitos ou abusivos.[100] Por outro lado, o tratamento de dados que gerar diferenciação de titulares para fins lícitos, como, por exemplo, para a segmentação de riscos de crédito ou securitários, poderá ser admitido, ainda que envolva dados sensíveis, desde que presente alguma das hipóteses

---

[98] "Esse dispositivo, porém, deve ser lido em consonância com o que dispõe a Lei nº 9.656/98 (que versa sobre os planos e seguros privados de assistência à saúde) e aqui merece ser feita uma distinção entre seleção de riscos e análise de risco para fins de subscrição e precificação. A Lei nº 9.656/98 veda a seleção de riscos, ou seja, a possibilidade de recusa de oferecimento de cobertura a determinado proponente, porém a mesma lei reconhece a possibilidade de precificação e de análise de riscos para fins de subscrição ao admitir que, na presença de doença preexistente, deverá ser ofertada ao proponente a cobertura parcial temporária ou o agravo do prêmio durante o período no qual seria aplicável a cobertura parcial temporária. Portanto, é nessa linha que deve ser interpretado esse dispositivo da LGPD. Logo, é fundamental que se ponha em perspectiva que nem toda discriminação é prejudicial e ilícita, como não é, por exemplo, aquela diretamente relacionada a subsidiar a contratação de um seguro" (Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados pessoais. CNseg. p.14. Disponível em: <http://cnseg.org.br/data/files/AF/63/3B/7E/B8B6F610373532F63A8AA8A8/GBPMS_ONLINE_ok.pdf>. Acesso em: 29.04.20). "Portanto, seleção de riscos para fins de não oferecimento de cobertura em seguro saúde é vedada pelo dispositivo em questão, mas não a análise de risco para fins de precificação (agravo do prêmio) ou para o estabelecimento de cobertura parcial temporária, no caso de identificação de preexistência de alguma doença, o que, como consequência, autoriza o tratamento de dados sensíveis referentes à saúde do beneficiário ou do segurado para essas finalidades" (p. 34).

[99] 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.

[100] Cf. O'NEIL, Cathy. *Weapons of Math Destruction*. New York: Crown Publishers, 2016. PASQUALE, Frank. *The Black Box Society:* The secret algorithms that control money and information. Massachusetts: Harvard University Press, 2015. Transparência e Governança nos algoritmos: um estudo de caso sobre o setor de birôs de crédito. Publicado em: ITS Rio, 2017, p. 13. Disponível em: <https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf>. Acesso em 11/11/2019.

autorizativas previstas nos já citados artigos 7º e 11 e havendo pleno respeito às normas da LGPD.

Considerações finais

A Lei Geral de Proteção de Dados representa o marco de uma nova cultura de tutela da privacidade e dos dados pessoais no Brasil. Caminhando ao encontro do Regulamento europeu, a norma institui modelo preventivo de proteção de dados, baseado na ideia de que todo dado pessoal possui relevância e valor, por representar projeção da pessoa humana.

Entende-se que o sistema desenvolvido tem como pilares centrais: a) amplo conceito de dado pessoal; b) necessidade de que qualquer tratamento de dados tenha uma base legal; c) rol taxativo de hipóteses legais para o tratamento de dados; d) caracterização detalhada do consentimento do titular e preocupação com sua manifestação; e) legítimo interesse como uma das hipóteses autorizativas e necessidade de realização de um teste de balanceamento de interesses para a sua regular aplicação; f) amplo rol de direitos do titular; e g) densa carga principiológica.

Busca-se implementar instrumentos para a proteção e garantia da dignidade humana. Para tanto, a LGPD facilita o controle dos dados tratados, impõe deveres e responsabilidades aos agentes de tratamento e proporciona segurança para que as informações circulem. Visa-se antecipar os riscos de violação à privacidade, como também evitar tratamentos abusivos de informações e vazamentos de dados.

civilistica.com

Recebido em: 10.12.2019

Publicação a convite.

Como citar: TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Data de acesso.