OAB RIO GRANDE DO SUL ESA

REVISTA ELETRÔNICA DA ESA/RS

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

CONSENTIMENTO: PRIMEIRA BASE LEGAL DO ROL TAXATIVO DO ART. 7º DA LEI Nº 13.709/18 E ÚLTIMA ALTERNATIVA PARA TRATAMENTO DOS DADOS PESSOAIS EM VIRTUDE DA SUA FRAGILIDADE

CONSENT: FIRST LEGAL BASIS OF THE RESTRICTIVE ROLL FROM ART. 7 OF LAW No. 13.709/18 AND LAST ALTERNATIVE FOR THE TREATMENT OF PERSONAL DATA BY VIRTUE OF ITS FRAGILITY

***Mônica Tais Medeiros Lopes Scariot*[1]**

***Renata Dalla Santa de Carvalho*[2]**

RESUMO

A proteção à privacidade foi objeto de norma especial com a promulgação da Lei Geral de Proteção de Dados – LGPD em 2018, a Lei nº 13.709/18. A norma possui uma série de princípios que permeiam o tratamento dos dados pessoais, assim como estabelece dez hipóteses que permitem o tratamento dos dados pessoais, também chamadas de bases legais. O consentimento é uma das hipóteses de tratamento, contudo, trata-se de uma base legal vulnerável, já que possui uma série de requisitos para que seja considerado válido, bem como pode ser revogado a qualquer momento a pedido do titular de dados, razão pela qual sugere-se, dentre as opções legais, utilizá-lo como última hipótese.

Palavras-chave: Lei Geral de Proteção de Dados. Bases Legais. Consentimento. Fragilidade

ABSTRACT

Privacy protection was the subject of a special rule with the enactment of the General Data Protection Law - LGPD in 2018, Law No. 13.709 / 18. The standard has a series of principles that permeate the processing of personal data, as well as establishing ten hypotheses that allow the processing of personal data, also called legal bases. Consent is one of the treatment hypotheses, however, it is a vulnerable legal basis, since it has a series of requirements for it to be considered valid, as well as it can be revoked at any time at the request of the data subject, which is why which it is suggested, among the legal options, to use it as a last hypothesis.

Key-words: General Data Protection Law. Legal bases. Consent. Fragility

[1]Especialista em Direito Civil, Negocial e Imobiliário pela LFG – Anhanguera UNIDERP e Especialista em Direito Digital e Proteção de Dados pela Escola Brasileira de Direito - EBRADI, e-mail: monica@lopesepauletto.com.br. Advogada, inscrita na OAB/RS 81.345.

[2] Especialista em Direito Digital pela Fundação Escola Superior do Ministério Público, e-mail: renata@dallasanta.adv.br. Advogada, inscrita na OAB/RS 101.683

INTRODUÇÃO

Em uma época em que a conhecida frase *Data is the new oil* (Dados é o novo petróleo) proferida por Clive Humby tem o poder de sintetizar o novo produto de valor agregado no mercado, e que determina o sucesso de negócios de diferentes segmentos, há de se intensificar a atenção para delimitar com regras que coíbam excessos daqueles que exploram o uso de dados em relação ao cidadão. Na contemporaneidade, apesar de existirem diversas leis que definem e determinam o limite entre o que deve ser de conhecimento público e o que é de exclusividade do indivíduo, sabe-se que a intimidade, por meio do comércio de dados pessoais, tem sido objeto de violação para fins de exploração econômica, sem a ciência de quem possui a sua tutela. Nesse contexto, o consentimento surge como uma das hipóteses legais que visa a proteção do referido direito.

É relevante recapitular que o consentimento teve importante destaque no Código de Nuremberg que em 1947, (JADOSKIA, 2017, p. 117), entre outras determinações que corroboraram para questões de bioética, incluiu a necessidade de consentimento livre e esclarecido pelo paciente, para a utilização e o fornecimento de suas informações em pesquisas. Não obstante, a Declaração de Helsinque, 1965 (Mundial, 1964) avança no sentido de estabelecer critérios na coleta e no uso do consentimento. Entretanto, de forma mais ampla, foi por meio da *General Data Protection Regulation* – GDPR - que revogou o considerando 171 da Diretiva 93/13/CEE (Europeu, 2020, p. 38) - que o consentimento passou a ocupar fundamental importância como uma das hipóteses para o tratamento de dados pessoais por meio de critérios direcionados à proteção dos titulares de dados em virtude das relações econômicas entre instituições, pessoas jurídicas, e consumidores, pessoas físicas.

Assim, considera-se atual, necessário e pertinente o presente estudo acerca do consentimento, uma vez que, apesar de já vigorar a Lei Geral de Proteção de Dados no Brasil, ainda há muitos desafios a serem superados, diante da desinformação e da relativização ponderada pelos controladores - que ainda desacreditam acerca da real necessidade de conformação de seus processos à referida Lei, motivo pelo qual titulares de dados tem sido submetido a experiências de anuência em termos de consentimento absolutamente duvidáveis sob à luz da nova norma.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

1. LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A proteção à privacidade possui previsão legal no art. 5º, X, XI e XII da Constituição Federal de 1988, bem como nos artigos 20 e 21 do Código Civil Brasileiro dentre outros artigos esparsos em leis especiais.

A partir da promulgação da Lei Geral da Proteção de Dados – LGPD, os brasileiros passaram e ter essa proteção à privacidade disciplinada por meio de norma especial, momento que marca uma nova fase no que diz respeito aos direitos dos titulares dos dados pessoais.

Políticas de privacidades foram instituídas, *cookies* para permitir navegação e rastreio simbolizam uma nova fase, em que há uma preocupação com as consequências da coleta indevida dos dados pessoais, mormente em virtude das elevadas e notórias sanções previstas na referida norma.

A Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2020 após uma série de prorrogações legislativas ocorridas em 2019 e 2020.

Trata-se de uma norma especial de natureza principiológica, sendo que conforme previsão no art. 6º, além da boa-fé, as atividades de tratamento de dados pessoais deverão observar os princípios abaixo indicados:

> 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;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Um dos pontos chaves da norma é a proteção à privacidade do titular dos dados, visto que o tratamento dos dados pessoais está permitido apenas nas hipóteses discriminadas no art. 7º, intituladas de bases legais, quais sejam: consentimento, legítimo interesse, execução de Contrato, cumprimento de obrigação legal, defesa e interesses vitais dos titulares, interesse público ou de autoridade, tutela da saúde (procedimentos realizados por profissionais da saúde ou por entidades sanitárias), realização de estudos por órgão de pesquisa (desde que anonimizados), exercício regular de direitos em processo judicial, administrativo ou arbitral e proteção do crédito.

As bases legais são hipóteses que autorizam o tratamento de dados. Em outras palavras, pode-se dizer que são condições determinadas pela Lei Geral de Proteção de Dados para que seja possível fazer a coleta de dados pessoais e o seu tratamento.

Em que pese alguns pensem que a LGPD seja uma cópia do GDPR (*General Data Protection Regulation* – Regulamento Europeu), cumpre informar que não se tratam da mesma legislação, embora de fato a norma brasileira tenha sido inspirada no regulamento europeu e possua inúmeras semelhanças principiológicas.

A título de exemplo, nota-se que o regulamento europeu dispõe acerca de seis bases legais para o tratamento de dados pessoais dos titulares dos dados, enquanto a norma brasileira dispõe de dez. As bases legais do Regulamento europeu são mais restritivas, podendo ocorrer o tratamento de dados pessoais somente nas hipóteses a seguir indicadas: consentimento, interesse legítimo, execução de contrato, cumprimento de obrigação legal, defesa e interesses vitais dos titulares, interesse público ou de autoridade.

A principal diferença entre as bases legais é que a norma brasileira possui quatro bases legais a mais que o regulamento europeu, quais sejam: tutela da saúde, realização de estudos por órgão de pesquisa (desde que anonimizados), exercício regular de direitos em processo judicial, administrativo ou arbitral e proteção do crédito. Cumpre informar que o consentimento – base legal tema do presente artigo - encontra-se presente em ambas legislações, possuindo inclusive critérios semelhantes para validade conforme adiante será explanado.

2. ASPECTOS GERAIS DO CONSENTIMENTO

O consentimento é uma das bases legais previstas no artigo 7º da Lei Geral de Proteção de Dados, e pode-se dizer que é uma das bases legais mais populares, já que antes mesmo da vigência da LGPD, o Marco Civil da Internet (Legislação que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil - Lei nº 12.965, de 23 de abril de 2014) já trazia expressamente hipóteses em que o tratamento de dados pessoais somente poderia ocorrer mediante consentimento, com base no direito e garantia dos usuários, nestes termos *in verbis:*

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> [...]
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Conforme anteriormente mencionado o artigo 7ª da LGPD dispõe acerca das hipóteses de tratamento de dados pessoais, também intituladas de bases legais, sendo que o consentimento encontra previsão no inciso I do referido artigo, nestes termos, *in verbis:*

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado 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 desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> 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;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - 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; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O consentimento é a manifestação livre, informada, e inequívoca do titular para que seja realizado o tratamento dos seus dados pessoais. (BLUM, 2020, p. 26). Já o tratamento diz respeito a toda operação realizada com os dados pessoais, tais como coleta, armazenamento, compartilhamento, eliminação etc.

Vale ressaltar que não existe prevalência sobre as bases legais, de forma que nenhuma base legal possui maior peso ou relevância sobre a outra. A análise sobre a base adequada deve ser efetuada com cautela e de acordo com cada caso específico, já que a escolha da base legal inadequada, especialmente em decorrência de má-fé pode resultar em incidências de multas, como vêm ocorrendo na Europa.[3]

2.1 Casos de nulidade do consentimento

O consentimento, para sua plena validade, deve atender aos princípios relacionados no art. 5º da Lei Geral de Proteção de Dados, que define tal expressão como:

> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Não obstante tal conceito, é relevante frisar que o consentimento deve ser específico e cumprir com as finalidades indicadas, visto que ele sendo genérico, incorrerá na possibilidade das nulidades, nos termos do §4, *in verbis:*

> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 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.
> § 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.

Isso significa dizer que a validade do consentimento está submetida a existência de requisitos que devem ser preenchidos, os quais estão relacionados no art. 5º, XII, quais sejam ser inequívoco, livre e manifestado.

[3] Nesse sentido, segue site utilizado para consulta de multas aplicadas (Rastreador de aplicação de GDPR) no qual é possível verificar vários casos em que houve aplicação de multas por utilização da base legal incorreta: I*nsufficient legal basis for data processing* – Acesso em: 11/05/2021 – Disponível em: https://www.enforcementtracker.com/

Outro ponto importante é que não pode ser considerado válido o consentimento manifestado como "tudo ou nada", ou seja, é necessário observar a granularidade do consentimento (BLUM, 2020, p. 28). Significa, portanto, que para cada finalidade deve-se coletar um consentimento específico, ainda que sejam as mesmas partes (controlador e titular dos dados), já que o que determina a observância da granularidade é a finalidade do tratamento e não as partes envolvidas.

Não menos importante, o dever de guardar o comprovante do ato, no caso o consentimento, seja ele físico ou eletrônico, recai sobre o controlador, que faz a coleta dos respectivos dados pessoais. Tal obrigação, em uma primeira análise parece ser um documento de simples guarda, contudo, quando se trata de uma organização com um grande fluxo de dados a guarda não automatizada se torna inviável. Em contrapartida, incluir consentimento pré-pronto ou preenchido previamente poderá ensejar a nulidade do mesmo, razão pela qual é de extrema importância o cuidado e zelo no que concerne a escolha do conteúdo do termo de consentimento, bem como quanto a forma de guarda do mesmo.

Trata-se de exemplo claro de consentimento, aquele decorrente de relação de trabalho. De forma genérica, a relação empregado x empregador tem em si, de forma intrínseca uma relação de desequilíbrio, onde o empregado é a parte vulnerável. *In casu*, o entendimento harmônico atualmente é o de que o consentimento coletado em sua origem é nulo.

Exceção a essa regra seria o consentimento obtido pelo empregador para finalidades dentre as quais não seja possível a observância de outra base legal, tomando-se por base o princípio da boa-fé. A título de exemplo, pode-se mencionar as empresas que divulgam em seus boletins internos os aniversários dos colaboradores juntamente com fotos pessoais. Nessa hipótese, tal relação não estaria abarcada pela base legal de obrigação legal por fugir do escopo de relação inicial, mas igualmente não se poderia considerar, ao menos em uma primeira análise, a nulidade de um consentimento, caso tenha sido obtido especificamente para divulgação interna, bem como preenchidos os demais requisitos de validade.

Diante dessas breves considerações, extrai-se que a combinação de um ou outro elemento discriminado à lei, em um ato realizado pelo titular de dados para ter acesso a um produto ou serviço, não configurará o consentimento. Isso porque, nesse caso a lei visa proteger o titular de dados, resguardando a ele o direito e o poder de controlar os seus próprios dados.

Assim, se o controlador no momento da coleta de dados apenas informar que tal dado será utilizado para uma finalidade específica – não estando tal finalidade dentro do rol taxativo disposto no artigo 7º e incisos II a X da referida Lei – porém não motivar que o titular se manifeste acerca dele, optando por anuir de forma autônoma, não condicionada, não premeditada – como os casos dos *checkbox* já marcados (MURINO, 2018) - e sem descrever o tipo de tratamento que será dados a eles – pois poderão ser objetos de compartilhamento, transferência, entre outros – bem como informar acerca de eventuais riscos a que ele está submetido (VAINZOF, 2018, p. 71-81), restará evidente o descumprimento fidedigno aos elementos necessários e constituintes do ato de consentir explicitado na lei. Portanto, tal ato viciado será considerado nulo, visto que inexistentes os requisitos que formam o consentimento.

Antes mesmo da publicação da Lei Geral de Proteção de Dados, o uso do consentimento foi objeto de importante discussão nos tribunais brasileiros, através da invocação dos preceitos legais em defesa do Direito do Consumidor Brasileiro. Uma delas, foi decidida pelo Superior Tribunal de Justiça, no ano de 2017, invocando a Diretiva 95/46/CE, 35ª Conferência de Privacidade da Associação Alemã de Proteção de Dados e Segurança de Dados, o Regulamento (EU) 2016/679 (GDPR), do Parlamento e do Conselho, que respaldou o entendimento de que o consentimento para ser válido deve preencher requisitos e na falta de algum deles há configuração de cláusula abusiva:

> RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. **CLÁUSULAS ABUSIVAS**. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. (...) 3. **É abusiva e ilegal** cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, **sem que seja dada opção de discordar daquele compartilhamento**. 4. A cláusula posta em contrato de serviço de cartão de crédito **que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança**. 5. **A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada**. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e Documento: (...) 9. A orientação fixada pela jurisprudência da Corte Especial do STJ, em recurso repetitivo, no que se refere à abrangência da sentença prolatada em ação civil pública, é que "os efeitos e a

> eficácia da sentença não estão circunscritos a lindes geográficos, mas aos limites objetivos e subjetivos do que foi decidido, levando-se em conta, para tanto, sempre a extensão do dano e a qualidade dos interesses metaindividuais postos em juízo (arts. 468, 472 e 474, CPC e 93 e 103, CDC)".(...) (Salomão, 2017) (***grifo nosso)***

Reforça-se que nessa decisão o Ministro motivou seu relatório também com base em artigo produzido pelo Dr. Jorge Barros Mendes em que traz o entendimento de que "ao consentimento, a partir do novo documento, deve ser dado de forma expressa, clara, de modo inteligível, de fácil acesso e numa linguagem clara."

No que tange às nulidades do consentimento, conclui-se que qualquer condição que contraste ao conceito impresso na lei, o tornará nulo, uma vez em que para a constituição do consentimento em sua essência, qualquer inobservância aos elementos básicos que compõem o referido termo se converterá em aceite qualquer, pois se distancia do entendimento da lei acerca do ato de consentir, o que importa em sua nulidade por sua própria inexistência, visto que o rol de elementos constitutivos do consentimento necessariamente deve primar por todos os seus requisitos em conjunto e não de forma excludente ou optativa pelo controlador.

3. O CONSENTIMENTO NA GDPR – *GENERAL DATA PROTECTION REGULATION*

O Regulamento Europeu – *General Data Protection Regulation* se trata de uma evolução da legislação de privacidade proteção de dados europeia, em especial a Diretiva 95/46/CE e é a atual norma relativa a proteção de privacidade que vigora na Europa. A norma entrou em vigor 25 de maio de 2018 e possui disposição diversa da Lei Geral de Proteção de Dados, tendo em vista que é dividida inicialmente em 173 (cento e setenta e três) considerandos – arcabouço de definições e previsões com o objetivo de assegurar o cumprimento da norma – e posteriormente em 99 (noventa e nove) efetivos artigos.

Na referida norma existem várias diretrizes especificas acerca do consentimento, sendo que inúmeros requisitos sobre a validade foram absorvidos pela norma brasileira.

Nesse sentido, o artigo nº 4.º, item 11, do GDPR define consentimento como: "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"

Já o artigo 7º dispõe acerca das condições aplicáveis ao consentimento, nestes termos, *in verbis:*

> Artigo 7.o
> Condições aplicáveis ao consentimento
> 1.Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
> 2.Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
> 3.O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.
> 4.Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento

Não obstante a norma europeia seja mais rigorosa acerca do tratamento dos dados pessoais (possui apenas seis bases legais), também coloca o consentimento como uma opção bastante rígida, uma vez que para ser válido, o consentimento deve ser livre, manifesto, específico, informado e explícito.

Considerando que a norma está em vigor desde 2018, bem que existem inúmeras Autoridades Reguladoras de Proteção de Dados, constantemente são publicadas *Guideline*s (Diretrizes), montadas a partir das atualizações e casos práticos que vão surgindo. Nesse sentido, a *Guideline* nº 05/2020, datada de 04 de maio de 2020 dispõe especificamente sobre o consentimento, elencando uma série de diretrizes práticas, tais como: validade da manifestação inequívoca, consentimento granularizado dentre outras.

A título de exemplo, em determinado trecho da *Guideline* há expressa indicação para avaliar se o consentimento em questão foi obtido de forma livre, nestes termos, *in verbis:*

> O elemento «livre» implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido13. Se o consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente. Assim sendo, não se considera que o consentimento foi dado de livre vontade se o titular dos dados não o puder recusar nem o puder retirar sem ficar prejudicado14. A noção de desequilíbrio entre o responsável pelo tratamento e o titular dos dados também é tida em consideração no RGPD.14. Ao avaliar se o consentimento é dado livremente, importa ter em conta a

> situação específica em que o consentimento está subordinado à execução de um contrato ou à prestação de um serviço, tal como descrito no artigo 7.º, n.º 4. O artigo 7.º, n.º 4, foi redigido de forma não exaustiva com palavras como «designadamente», significando que pode haver uma variedade de outras situações que se enquadram nesta disposição. Em termos gerais, qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.[4]

E na sequência, a referida *Guideline* traz uma situação hipotética para que se possa visualizar especificamente a questão indicada:

> Exemplo 1: Uma aplicação para telemóvel de edição de fotografias solicita aos utilizadores que ative a localização por GPS para fins de prestação dos serviços. A aplicação também os informa de que utilizará os dados recolhidos para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, indo além da concretização do serviço principal prestado. Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre.

Diante disso, verifica-se que para se obter um consentimento válido à luz da legislação as etapas são bastante rigorosas e seguem exigindo novas diretrizes e atualizações, razão pela qual dentre as opções de bases legais disponíveis para tratar os dados pessoais, certamente deve ser utilizado como última opção, diante da sua fragilidade.

4. HIPÓTESES DA OBRIGATORIEDADE DO CONSENTIMENTO PARA TRATAMENTO DE DADOS E DADOS SENSÍVEIS

Apesar de figurar como base legal de elevada importância, o consentimento figura entre uma das dez hipóteses de conformidade para que o controlador esteja adequado à Lei Geral de Proteção de Dados. Sendo hipótese, logo não é obrigatório, nas situações elencadas ao artigo 7º incisos II a X. (BLUM, 2020, p. 26)

Oportuno enfatizar que frente a referida lei, o titular de dados é a parte hipossuficiente da relação e por decorrência de sua vulnerabilidade (VAINZOF, 2018, p. 54-72) é que se deve imprimir mais transparência ao titular de dados para que este de fato exercite seu direito de

[4]Guideline 05/2020 – Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf - Acesso em 19/05/2021

consentir ou não o tratamento de dados para a finalidade proposta pelo controlador, conforme sugere o professor Vainzof:

> Considerar sempre os titulares vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais, é um caminho aconselhável para o atendimento dos referidos princípios. (VAINZOF, 2018, p. 54-72)

Portanto, em se referenciando relações comerciais entre iniciativas privadas – controladores – e titulares de dados, sejam eles ocupando o papel de consumidor, empregado, fornecedor, entre outras posições pertinentes ao negócio, sugere-se que o tratamento de dados seja fundamentado em consentimento apenas se verificada a ineficácia das outras hipóteses de tratamento.

Reforça-se que o controlador poderá respaldar o tratamento dados por outras nove bases legais previstas na LGPD, quais sejam: legítimo interesse; cumprimento de obrigação legal ou regulatória; tratamento pela administração pública; realização de estudos e de pesquisa; execução ou preparação contratual; exercício regular de direitos; proteção da vida e da incolumidade física; tutela de saúde do titular; proteção de crédito.

Motiva-se a referida sugestão pelo fato de que o consentimento só é necessário se não houver respaldo de tais bases supracitadas para o tratamento de dados que o controlador intenciona realizar. Dessa forma, o consentimento se torna base legal a ser utilizada de forma complementar, o que facilitará ao controlador na gestão do consentimento, sendo mais favorável sua utilização no esgotamento das outras bases legais.

5. TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E DE ADOLESCENTES – CONSENTIMENTO COMO EXCEÇÃO À REGRA

Diferentemente das demais hipóteses de conformidade à Lei Geral de Proteção de Dados, o tratamento de dados pessoais de crianças e adolescentes com base no consentimento, é uma necessária exceção à regra.

Entende-se que o menor, não possui compreensão da extensão dos riscos a que estão expostos e de suas garantias para as situações de tratamento de dados pessoais, portanto, tal permissão fica sob tutela dos responsáveis legais da criança e do adolescente. Nesse sentindo a

Lei 13.709/18 segue o mesmo entendimento do Regulamento Geral da União Europeia – GDPR, tratado no considerando 38:

> As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

A legislação brasileira de proteção de dados, em seu art. 14; §3º, prevê, no que tange à autorização para tratamento de dados, como única hipótese de exclusão do consentimento o caso em que a coleta seja necessária para contatar pais ou responsável legal, entretanto, tal coleta não poderá ser armazenada, sendo permitida sua utilização uma única vez:

> § 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.

A referida lei, no art. 14, §1º, determina, entretanto que para todas as outras situações, se faz imprescindível a aplicação do consentimento, como única base legal válida:

> 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.

Oportuno destacar que no §4º da referida lei brasileira, inspirado na GDPR, inclui em seu texto a necessidade do respectivo consentimento para jogos e aplicativos de internet.

Entretanto, vale ressalvar que a lei brasileira, pura e simples, não condiciona os atos do controlador, definindo um escopo apropriado para validar o consentimento. Cita-se como exemplo a metodologia editada pelo COPPA/1998 – *Children's Online Privacy Protection Act* -, nos Estados Unidos da América, para fins de proteção de dados de menores de 13 anos, que determina uma sequência de atos necessários a serem cumpridos para fins de eficácia do consentimento de quem possui a responsabilidade legal sobre a criança, conforme pode-se conferir:

> (...). (2) Os métodos existentes para obter o consentimento verificável dos pais que satisfaçam os requisitos deste parágrafo incluem:
> (i) Fornecer um formulário de consentimento a ser assinado pelos pais e devolvido à operadora por correio postal, fax ou digitalização eletrônica;
> (ii) Exigir que um pai, em conexão com uma transação monetária, (...)
> (iii) fazer com que um dos pais ligue para um número de telefone gratuito com pessoal treinado;
> (iv) Ter um pai conectado (...) por meio de videoconferência;
> (v) Verificar a identidade dos pais, comparando uma forma de identificação emitida pelo governo em bancos de dados de tais informações, onde a identificação dos pais é excluída após a verificação ser concluída; ou
> (vi) (...) usar um e-mail juntamente com etapas adicionais para fornecer garantias de que a pessoa que fornece o consentimento é o pai. Essas etapas adicionais incluem: Enviar um e-mail de confirmação para os pais após o recebimento do consentimento, ou obter um endereço postal ou número de telefone dos pais e confirmar o consentimento dos pais por carta ou telefonema. (...)

Confia-se, portanto no papel importantíssimo de regulamentação que a Autoridade Nacional de Proteção de Dados exercerá, merecendo sua atenção especial para fins de ajustamento das interações a serem realizadas pelo controlador quando do tratamento de dados pessoais de crianças e adolescentes a fim de trazer legitimidade e validade para os atos do controlador no intuito de consolidar segurança jurídica aos direitos tutelados ao menor.

6. GESTÃO DO CONSENTIMENTO

A adoção do consentimento como base escolhida pelo controlador, ainda que preenchidos todos os seus requisitos para possuir validade, não é suficiente em si. Isso porque a lei obriga o controlador a determinados processos necessários até que o consentimento possa ser eliminado. Um dos pontos críticos do consentimento é o fato de que ele pode - e deve - ser revogado, se houver pedido do seu titular, por isso esta é entendida como uma das bases legais mais complexas, já que possui uma evidente fragilidade.

Consequentemente, importa que o controlador deverá se valer de alguns processos (VIEIRA, 2019, p. 89) que garantam a eficácia do consentimento que devem ser observados desde a coleta de dados até sua exclusão. Ou seja, não basta que o consentimento seja uma manifestação livre, informada e inequívoca com finalidade específica de tratamento de dados. Ele precisa estar sob o controle do seu titular.

Para tanto, faz sentindo integrar inteligência da área de administração para facilitar o entendimento e criar um processo que evidencie o ciclo de vida do consentimento e, por

consequência o fluxo de dados decorrente do consentimento. Para ilustrar, utiliza-se uma das diversas ferramentas possíveis para o desenho do ciclo de vida dos dados, nesse caso opta-se por demonstrar com a metodologia baseada no 5W2H, conforme explicita-se abaixo:

> 1 - *Who?* Quem é o titular de dados
> *2 - What?* Que dados serão necessários
> *3-Where?* Onde será armazenado, compartilhado ou para quem será transferido
> *4 - When?* Quando foi coletado, quando se encerrará e/ou quando foi solicitada a sua exclusão ou transferência pelo titular.
> *5 - Why?* Para quê finalidade será consentido o tratamento
> *6 - How?* (Como?) De que forma ele será armazenado, disponibilizado e como o titular poderá requerer sua exclusão
> *7 - How Much?* Para essa questão específica, a lei já determina que o requerimento de exclusão, bem como de relatório dos dados que permanecem em posse do controlador deverá ser respondido a título não oneroso ao titular, ou seja, gratuito.

Em alguns programas de conformidade com a LGPD, também se utiliza a nomenclatura de política de consentimento, e a doutrina indica que é necessário ter uma lista que todas as notificações de consentimento de privacidade devem atender se há coleta de dados, nestes termos, *in verbis:*

> Os dados devem incluir a identidade do controlador e do responsável pela proteção de dados, por quanto tempo será mantido, os direitos que o consumidor tem, o direito de registrar uma reclamação, os destinatários e as transferências de dados, uma declaração de que o consumidor tem o direito de retirar o consentimento a qualquer momento e também uma explicação de porque você ou um terceiro deseja coletar os dados. (MALDONADO, 2019, p.162)

A norma dispõe ainda que o consentimento deve ser destacado das demais cláusulas:

> 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.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

Dessa forma, resta evidente que, se o controlador não possui até o presente momento atenção focada na proteção e privacidade de dados, e vir a fundamentar tratamento de dados com base no consentimento, urgirá incluir em sua organização processo de gestão do consentimento.

Por fim, cabe recomendar que, havendo disponibilidade financeira pelo controlador, é interessante a adoção de recursos tecnológicos e automatizados para a gestão do consentimento, frente a dificuldade de gerenciamento do referido documento de forma híbrida, em ambiente físico e virtual, visto que além de os documentos precisarem estar disponíveis, acessíveis e redundantes, o que importa investimento de recursos nas duas formas de armazenamento,

também viabiliza agilidade nas rotinas e nos processos, o que imprime qualidade às políticas de proteção e privacidade da organização.

7. CONCLUSÃO

O rol taxativo do art. 7º da Lei Geral de Proteção Dados que possui dez hipóteses de tratamento dados de dados certamente é fundamental para a proteção à privacidade, já que a limitação das hipóteses de tratamento restringe as ideias pretéritas de que os bancos de dados podiam ser repletos de informações desnecessárias – e inclusive vendidos ilegalmente – sem qualquer penalidade ou consequência.

A partir da modalidade de tratamento de dados, é imprescindível que seja efetuado um estudo adequado, normalmente iniciado por meio de mapeamento dos dados pessoais, a fim de verificar qual é a base legal mais adequada – e que justifique – o tratamento em questão, ressalvado os casos em que o consentimento é obrigatório, tais como o tratamento de dados de criança e adolescente.

Dentre as bases legais previstas, certamente o consentimento é uma das hipóteses de maior suscetibilidade, uma vez que possui uma série de requisitos formais de validade, bem como pode ser revogado a qualquer momento a pedido titular, ou seja, possui um caráter bastante vulnerável.

Não obstante, a gestão do consentimento também é considerada uma tarefa árdua, mormente quando aplicada a um grande fluxo de dados, já que para ser considerado válido, o consentimento obtido deve ser livre, informado e inequívoco. Ademais, deve ser individual para cada finalidade, também chamado de granular, o que certamente potencializa de forma significativa a gestão anteriormente mencionada.

Em consideração a isso, por consequência de todos os requisitos formais de validade, bem como o fato de que o titular dos dados pode revogá-lo a qualquer momento, consoante previsão expressa do art. 8º, §5 e do art. 18 da Lei Geral de Proteção de Dados – LGPD, sugere-se que a opção pela base legal do consentimento seja empregada como última predileção em um rol de dez hipóteses legais, pela fragilidade para configurar sua validade – em primeira análise – bem como em face da vulnerabilidade para manutenção do consentimento em virtude da iminência de revogação por parte do titular dos dados.

REFERÊNCIAS BIBLIOGRÁFICAS

BLUM, Renato Ópice; **Proteção de dados**: Desafios e Soluções na Adequação à lei, Rio de Janeiro, Forense, 2020

BLUM, Renato Ópice; MALDONADO, Viviane Nóbrega, **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Européia.** São Paulo: Thomosom Reuters, 2018.

JADOSKIA, Rafael MOSTARDEIRO, Sofia Rech, EXTERKOETTERA, Júlia d´Avila, GRISARDA, Nelson HOELLER, Alexandre Ademar. O consentimento livre e esclarecido: do código de Nuremberg. Vittalle – **Revista de Ciências da Saúde 29 n. 2**, 2017
.
MALDONADO, Viviane Nóbrega, **LGPD**: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. 3. Ed, Thomson Reuters Brasil, São Paulo, 2019.

MURINO, Thiago Barrizzelli. **O consentimento válido nas novas leis de proteção de dados**. Migalhas, 2018. Disponível em: < https://www.migalhas.com.br/depeso/286214/o-consentimento-valido-nas-novas-leis-de-protecao-de-dados >. Acesso em 21/05/2021

VAINZOF, Rony. **Dados Pessoais**, Tratamento e Princípios. BLUM, Renato Ópice (Org); MALDONADO, Viviane Nóbrega (Org), Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Européia. São Paulo: Thomosom Reuters, 2018
.
BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 19/05/2021

BRASIL. **Marco Civil da Internet**. Lei nº 12.965, de 23 de Abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 19/05/2021

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.348.532/SP**. Relator Luis Felipe Salomão – Quarta Turma. Disponível em: < https://processo.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202108054>Acesso em 21 de maio de 2021.
GUIDELINE 05/2020 – Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf > - Acesso em 19/05/2021

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: < https://www.privacy-regulation.eu/pt/r38.htm>. Acesso em: 23/05/2021.