Novo regulamento europeu reforça a proteção dos dados pessoais?

 Na primeira parte desta coluna, apresentamos uma visão geral do

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia, conhecido como GDPR (*General Data Protection Regulation*).

Enquanto finalizávamos esta segunda parte, foi aprovado no Senado brasileiro, na última terça-feira, dia 10 de julho, o Projeto de Lei da Câmara dos Deputados 53 de 2018, que institui o marco regulatório para proteção de dados no Brasil[1]. Esse projeto tem forte inspiração no direito europeu e, apesar de suas especificidades, e das particularidades do sistema jurídico brasileiro, a discussão aqui apresentada torna-se imprescindível para iniciar o debate sobre a regulação nacional da matéria[2].

Vimos que o GPDR, seguindo os passos da Diretiva 96/45/CE, marco normativo da proteção de dados antes da vigência do novo regulamento, tem por objetivo explícito conciliar a livre circulação dos dados, considerada imperativa nas sociedades atuais, com a proteção das pessoas em relação a seus dados.

Apesar de sua conexão de origem com o direito à privacidade, o direito à proteção de dados passa a ser considerado direito fundamental autônomo, de forma expressa, na Convenção Europeia de Direitos Humanos. E como tal é acolhido no regulamento europeu, que pretende reforçar esse direito, ao conferir a seu titular uma gama de poderes em relação a seus dados pessoais.

Um dos pontos de convergência entre essa ampliação da proteção dos dados pessoais e a outra finalidade explícita do GDPR, a facilitação da sua circulação, é o poder de autocontrole sobre os próprios dados assegurado a seu titular. O consentimento, ao mesmo tempo que se dirige à proteção do titular dos dados pessoais, viabiliza sua circulação lícita.

O GDPR põe o consentimento do titular no centro da proteção de dados pessoais, ao torná-lo requisito de licitude do tratamento de dados em geral, salvo hipóteses expressas, conforme seu artigo 6º[3]. Esse alargamento das hipóteses de exigência do consentimento é reforçado pelo previsto no artigo 7º, que requer daqueles que realizam o tratamento de dados pessoais a comprovação desse consentimento.

Esse mesmo artigo impõe o dever de informar qualificado, ao determinar que a cláusula de consentimento para tratamento de dados pessoais seja inteligível, de fácil acesso e em linguagem clara e simples. E assegura o direito de revogação do consentimento a qualquer momento, garantindo-se a

mesma facilidade para retirada quanto para sua concessão.

O consentimento do titular está sempre atrelado ao princípio da finalidade, que deve ser determinada, explícita e legítima (artigo 5º). Neste ponto, fica claro que do direito à autodeterminação informativa resulta que o consentimento do titular para acesso e tratamento de determinados dados pessoais não implica renúncia ao controle sobre os destinos ulteriores dessas informações.

Assim, a tutela da privacidade e dos dados pessoais não opera mais, unicamente, na lógica da informação sigilosa em contraposição à informação revelada pelo titular. O consentimento para que determinados dados sejam recolhidos e utilizados de certa maneira autoriza apenas e tão somente o tratamento para as finalidades autorizadas. Os dados a serem tratados devem ser pertinentes e necessários para atingir a essa finalidade e seu armazenamento está condicionado a sua utilidade para tal fim (artigos 5º, "b" e 9º ,"i")[4].

A autodeterminação pessoal é especialmente garantida em relação a uma categoria especial de dados, denominados "dados sensíveis" na Diretiva 95/46/CE. Conforme o artigo 9º do GDPR, esses dados são os que revelam a "origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical" do titular, bem como seus "dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, os dados relativos à saúde ou os dados relativos à sua vida sexual ou sua orientação sexual".

Em princípio, o tratamento dessas categorias especiais é vedado. Entretanto, o próprio artigo elenca dez diferentes hipóteses em que tal vedação é excluída. Os dados sensíveis podem ser objeto de tratamento, primeiro, nos casos em que haja consentimento explícito do seu titular, ou em que este tenha os tornado, previamente, públicos (artigo 9º, 2, "a" e "e").

A par da iniciativa do titular para consentir no tratamento ou publicar dados sensíveis, esses dados podem ser tratados em caso de interesse público ou social relevante (artigo 9º, 2, "b", "f", "g", "h", "i" e "j"), de interesse legítimo de entidades sem fins lucrativos, em relação a seus membros, ou antigos membros, ou pessoas que mantenham com elas contato regulares relativos a seus objetivos (artigo 9º, "d"), e de proteção de interesses vitais do próprio titular ou de outra pessoa, se o titular estiver impossibilitado física ou legalmente de manifestar sua vontade (artigo 9º, "c").

A dispensa do consentimento do titular não exime o responsável pelo tratamento do cumprimento das demais normas protetivas previstas no regulamento. Tampouco priva o titular de seus demais direitos, como o de acesso e informação, da restrição do uso às finalidades para os quais se destinam, de retificação, de segurança e confidencialidade.

Mesmo nos casos em que o consentimento não é condição de licitude do tratamento de dados pessoais, o regulamento busca mecanismos de controle do titular sobre seus dados. O GDPR prevê, nesse sentido, em seu artigo 21, o direito de oposição do titular em relação ao tratamento de seus dados, que tenha por base o interesse público ou interesse legítimo do responsável (artigo 6º, 1, "e" e "f"), ou nas hipóteses de alargamento das finalidades originais, sem consentimento do titular (artigo 6º, 4)[5].

O consentimento do titular de dados é, igualmente, necessário para permitir o tratamento voltado à

tomada de decisões automatizadas, inclusive a definição de perfis, que afete significativamente o titular ou sua esfera jurídica (artigo 22º, 1 e 2, “c”). Autoriza-se o tratamento de dados para esse fim, se a decisão for necessária para conclusão de contrato entre o titular dos dados e o responsável pelo tratamento, ou se expressamente autorizada pela lei nacional. Em relação aos dados sensíveis, salvo consentimento expresso, só se admite decisão automatizada ou definição de perfil, em casos excepcionais de interesse público relevante (artigo 22º, 4).

O quadro geral do regulamento nos permite concluir que o consentimento do titular ocupa lugar central na proteção de dados pessoais, mas não esgota a regulação jurídica da matéria. Há dados que não estão incluídos no âmbito de tutela do direito à proteção dos dados pessoais, tais como os anônimos, os relativos a investigação e persecução criminal, e os que digam respeito à segurança pública, nacional e comunitária.

Mesmo em relação aos dados protegidos pelo regulamento, estão previstas hipóteses de dispensa do consentimento para tratamento de dados, voltado ao atendimento do interesse público relevante (por exemplo, para formulação de políticas públicas, gestão e fornecimento de serviços públicos, segurança), ou que seja justificado pelo interesse legítimo de quem realiza o tratamento (como é caso dos serviços de proteção ao crédito, cadastros de consumidores, dentre outros).

Além disso, nem todo tratamento consentido é lícito, pois é preciso observar os demais requisitos do artigo 6º. A isso se soma a previsão de uma autoridade independente, responsável por fiscalizar e garantir sua aplicação efetiva (artigo 51º).

De qualquer modo, é evidente que o GDPR privilegia o consentimento, fortalecendo-o com a exigência de sua comprovação, do fornecimento de informações, vinculação com finalidades específicas, explícito em caso de dados sensíveis.

Esse poder de controle sobre as próprias informações pessoais reafirma a garantia jurídica de uma autodeterminação informativa, por meio da qual se garante, juridicamente, o poder de decidir sobre os destinos de seus dados pessoais.

A construção jurídica em torno da privacidade e a proteção dos dados pessoais procura dar respostas às exigências de circulação de informações pessoais, sobretudo digitais, nas sociedades contemporâneas. Ao se constatar a impossibilidade de manter uma esfera de intimidade intocada, os juristas, e os textos legais, mudam o foco para a tentativa de garantir algum controle sobre o fluxo das informações, fundado, sobremaneira, na autonomia individual, ainda que temperada por limites estatais.

Apesar da relevância evidente do direito à proteção de dados pessoais, já há algum tempo, o debate teórico em torno do tema aponta para a existência do chamado “paradoxo da privacidade”, para explicitar que, ao mesmo tempo em que se atribui grande valor à privacidade e à autodeterminação, se aceita revelar informações pessoais rotineiramente, nas redes sociais e páginas da internet, em troca de algum benefício[6]. Assim como é, de larga aceitação, a ingerência na intimidade por órgãos estatais e empresas privadas, em nome da segurança[7].

A fragilidade dessa construção jurídica não é novidade. A ideia de uma autodeterminação ou de uma

autogestão da privacidade está ancorada no pressuposto de que o indivíduo pode tomar decisões racionais, com a devida avaliação de riscos e benefícios, em especial do ponto de vista econômico. Pressupõe, igualmente, que a manifestação da vontade individual corresponde, baseada nessa avaliação racional, às preferências individuais[8].

Se, por um lado, o regulamento europeu prevê uma série de salvaguardas para o indivíduo que buscam superar o modelo de proteção baseado unicamente no consentimento; de outro, a ênfase na autonomia individual como mecanismo de acesso lícito aos dados pessoais põe em relevo as complexidades do paradoxo da privacidade em nossas sociedades.

A par de uma série de obstáculos à concretização desse modelo de proteção da privacidade, que privilegia o consentimento, a predisposição em consentir no fornecimento, uso e tratamento de dados pessoais, baseada em uma racionalidade econômica — ainda que nem sempre expresse uma decisão racional — pode levar à erosão da discussão sobre a importância da proteção de dados pessoais em sua dimensão coletiva e pública.

Como nos alerta Rodotà, nas sociedades contemporâneas, a privacidade e a proteção dos dados pessoais devem ser entendidas como direitos atinentes, também, à esfera de liberdade pessoal e política, com repercussões coletivas[9].

Essa aproximação entre privacidade, proteção de dados e liberdade na esfera pública enfrenta o desafio de subverter a lógica do modelo do autogerenciamento da privacidade, fundado em um cálculo individual de riscos e benefícios, para pensar o controle do tratamento de dados como um valor fundamental tanto para a liberdade individual como para efetivação de uma sociedade democrática.

**Esta coluna é produzida pelos membros e convidados da Rede de Pesquisa de Direito Civil Contemporâneo (USP, Humboldt-Berlim, Coimbra, Lisboa, Porto, Girona, UFMG, UFPR, UFRGS, UFSC, UFPE, UFF, UFC, UFMT e UFBA).*

---

[1] Cf. Senado aprova projeto de lei que regulamenta proteção de dados pessoais. Acesso em: 10 jul. 2018. Disponível em: https://www.conjur.com.br/2018-jul-10/senado-aprova-projeto-regulamenta-protecao-dados.
[2] Em uma visão geral, o projeto aprovado pelo Senado consagra princípios e garantias semelhantes ao Regulamento europeu, também, reforçando o controle do titular sobre seus dados pessoais, pela exigência do consentimento, o direito ao acesso e à informação, o direito de retificação e apagamento, dentre outros. A íntegra do projeto pode ser consultada em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&ts=1531318615899&disposition=inline&ts=1531318615899
[3] O artigo 8º dispõe expressamente sobre a necessidade de o consentimento para o tratamento de dados pessoais de crianças com menos de dezesseis anos ter sido dado ou autorizado por seus representantes legais.
[4] O GDPR excepciona a obrigatoriedade do consentimento, resguardadas as demais garantias, para o fim de investigações científicas (artigo 9º, 2, ”j”). A utilização massiva de dados de saúde nas pesquisas científicas põe em questão o consentimento do titular e a vinculação a uma finalidade específica para

tratamento de dados nessa área (Cf. MOSTERT, M. et allii. *From Privacy to Data Protection in the EU: Implications for Big Data Health Research*. In: *European Journal of Health Law*, Volume 25, Issue 1, 2017, pp. 43–55. Sobre o tema, conferir: CORRÊA, A. E. *O corpo digitalizado: bancos de dados genéticos e sua regulação jurídica*. Florianópolis: Conceito Editorial, 2010.
[5] Do mesmo modo, o regulamento consagra o direito à limitação de tratamento, nas hipóteses previstas no artigo 18º.
[6] HULL, Gordon. *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data* (December 2, 2014). *Ethics and Information Technology*. Disponível em: http://ssrn.com/abstract=2533057 orhttp://dx.doi.org/10.2139/ssrn.2533057. Acesso em: 11 ago. 2016.
[7] CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005, p. 83.
[8] Há uma evidente e insuperável assimetria entre as informações detidas pelas empresas que vão manejar os dados e o indivíduo que consente em seu uso; além disso, a efetivação das preferências de privacidade, por uma série de razões técnicas, é bastante difícil. Por fim, recusar a liberação de dados é inviável, em muitos casos, pois constituem pressuposto de acesso a bens e serviços essenciais (HULL, ob. cit.).
[9] RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 44.

Referências bibliográficas

CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.
CORRÊA, A. E. *O corpo digitalizado: bancos de dados genéticos e sua regulação jurídica*. Florianópolis: Conceito Editorial, 2010. EDELMAN, Bernard. L'homme numérique: question d'image. In: *L'individu face aux nouvelles Technologies: surveillance, identification et suivi*. Université de Lausanne. Paris: Schulthess, 2005, p. 39-49.
HULL, Gordon. *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data* (December 2, 2014). Ethics and Information Technology,: Disponível em: http://ssrn.com/abstract=2533057 orhttp://dx.doi.org/10.2139/ssrn.2533057. Acesso em: 11.ago.2016.
RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

Date Created
23/07/2018