Proteção de dados e expectativas para 2020

Recentes decisões do STJ e do DPDC mostram que a proteção de dados já começa a ser uma realidade no Brasil

Ana Frazão

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do CADE.

Apesar de ainda faltarem alguns meses para que a LGPD entre em vigor, decisões do final do ano passado mostram que a proteção de dados já começa a ser uma realidade no Brasil. Há evidências de que o sistema de proteção previsto pela LGPD já começa a ter efetividade, ainda que transversalmente, por meio da aplicação de regras do Marco Civil da Internet, da Lei 12.414/2011 e do Código de Defesa do Consumidor.

Dois recentes e importantes exemplos ajudam a compreender de que maneira a proteção de dados vem sendo implementada. O primeiro deles diz respeito a recurso especial julgado em novembro do ano passado pela 3ª Turma do Superior Tribunal de Justiça[1], oportunidade em que se entendeu que a existência de banco de dados sem o conhecimento do consumidor ensejaria dano moral *in re ipsa*, por violação ao dever de informação.

Nesta oportunidade, o STJ teve o cuidado de diferenciar a questão dos bancos de dados da hipótese do *credit scoring*[2], situação na qual se afastou a exigência de prévio e expresso consentimento do consumidor, por não se tratar propriamente de cadastro ou banco de dados, mas sim de modelo estatístico.

Entretanto, na hipótese específica, entendeu o STJ que "A gestão do banco de dados impõe a estrita observância das exigências contidas nas

[1] REsp 1758799/MG, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 12/11/2019, DJe 19/11/2019.

[2] A questão foi julgada em recurso repetitivo (REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014).

respectivas normas de regência - CDC e Lei 12.414/2011 - dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele."

Embora não se baseie na LGPD, o acórdão dialoga com vários dos direitos por ela previstos, como o direito de acesso aos dados armazenados e o direito à retificação de informações incorretas, até porque a Lei 12.414/2011 apresenta várias normas semelhantes às da LGPD, algumas das quais atualizadas recentemente por meio da Lei Complementar 166/2019. Da mesma maneira, o STJ deixou claro que tais deveres permeiam todas as etapas do tratamento, incidindo sobre a coleta, o armazenamento e a transferência de dados dos consumidores a terceiros.

Daí ter concluído o STJ que "Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais."

O princípio da finalidade específica do tratamento de dados também foi explorado, na medida em que o STJ considerou que "O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais."

O STJ ainda tocou em importantes discussões relativas ao alcance do consentimento do usuário, bem como em relação às situações de dados tornados públicos pelos usuários. Daí ter concluído que "o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos."

Como se pode observar, ainda que sem aplicar a LGPD – até porque obviamente isso não poderia ser feito -, a fundamentação adotada pelo STJ ao interpretar os dispositivos legais já existentes reflete uma série de discussões que foram positivadas pela LGPD, tornando a argumentação mais densa e consentânea com os propósitos e referenciais atuais da proteção de dados.

Outro interessante exemplo é a decisão do Departamento de Proteção e Defesa do Consumidor - DPDC do final de dezembro do ano passado, que condenou o Facebook à multa de R$ 6.600.000,00 (seis milhões e seiscentos mil reais)[3]. É preciso registrar que se trata de processo administrativo aberto *ex officio*, o que revela a mobilização espontânea das instituições oficiais em favor da proteção de dados no Brasil.

O problema que deu ensejo ao processo administrativo diz respeito ao famoso caso *Cambridge Analytica* e seus desdobramentos, diante das suspeitas do uso indevido de dados de cidadãos brasileiros, cujo número seria superior a 444.000.

Em interessante decisão, o DPDC deixou claro que " Dentre as alegações e provas colacionadas aos autos, ficou claro que, no âmbito da plataforma Facebook, prevalece um modelo de obtenção do consentimento do usuário no sentido de promover, como *default*, o compartilhamento automático de dados desse usuário com os desenvolvedores de aplicativos aos quais os amigos desse usuário tenham subscrito." Ou seja, "Dito de outra forma, como regra, se uma pessoa compartilha os seus dados com o desenvolvedor de um aplicativo (p. ex., quando passa a usá-lo), automaticamente (segundo as configurações-padrão da plataforma), esse desenvolvedor tem acesso aos dados dos amigos dessa pessoa."

Além disso, considerou o DPDC que o Facebook utilizou-se de um *nudge,* ou seja, de um estímulo de comportamento, a fim de que o compartilhamento instantâneo de informações de amigos de usuários que aderiram a determinado aplicativo ocorresse por meio de um mecanismo *opt-out*, em vez de *opt-in*. Tal questão foi considerada crucial para o DPDC, como se

---

[3] Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ. PROCESSO Nº 08012.000723/2018-19. Representante: Departamento de Proteção e Defesa do Consumidor - ex officio. Representados: Facebook Inc. e Facebook Serviços Online do Brasil Ltda. Decisão de 27/12/2019.

observa por trecho importante de sua fundamentação, que esclarece as implicações do modelo sobre o alcance da prática e o número de afetados:

> "Isso colocado, no presente caso, a simples adoção de um sistema de *opt-out*, em vez de um sistema de *opt-in,* tem implicações significativas. Afinal de contas, num sistema de *opt-in*, a quantidade de potenciais afetados no presente caso teria se limitado a oitenta e quatro usuários ou a um quantitativo não muito superior a isso (justamente aqueles usuários brasileiros que subscreveram o aplicativo *thisisyourdigitallife*), enquanto o sistema de *opt-out* implicou em um quantitativo superior a quatrocentos e quarenta mil usuários com seus dados expostos a tal aplicativo. Afinal de contas, é inverossímil acreditar que, num sistema em que sejam adotadas configurações-padrão de *opt-in*, os amigos de alguém que passasse a usar um aplicativo respondessem afirmativamente a cada solicitação de compartilhamento de dados que esse aplicativo fizesse a esses amigos. Ainda, é de se esperar que, caso esse fosse o modelo de negócios adotado pelas Representadas, a plataforma Facebook dificilmente teria a dimensão e porte (em capital, investimento e em capilaridade e quantidade de usuários) que possui atualmente."

Diante dessas circunstâncias, considerou o DPDC, acertadamente, que a responsabilidade do provedor não poderia ser afastada nem mesmo no contexto de total transparência, embora esse não fosse o caso do Facebook. Com efeito, a autorização dos usuários teria ocorrido de forma genérica, já que dois pontos permaneciam em aberto no momento em que houve o consentimento: (i) quem teria acesso a esses dados e (ii) qual a finalidade do tratamento das informações fornecidas pelos usuários. Daí concluir o DPDC que "dizer que houve consentimento específico para uma finalidade indefinida *ex ante* é o mesmo que dizer que não houve consentimento para finalidade nenhuma, uma vez que não se encontra presente o atributo da especificidade."

Tais aspectos foram devidamente contextualizados com os estudos que mostram a vulnerabilidade dos consumidores em situações nas quais precisam dimensionar adequadamente as consequências futuras de decisões presentes, motivo pelo qual não se pode imaginar que o consentimento possa ser visto como um cheque em branco.

Daí por que a decisão aborda a interessante discussão sobre o alcance do dever de informação e as suas limitações para, sozinho, assegurar a proteção dos dados, já que oferecer informações completas ou simples pode não ser suficiente para a total compreensão do contrato por parte dos consumidores. Daí a importância do dever de monitoramento e da proteção das legítimas expectativas dos consumidores no que se refere ao seu direito à proteção dos dados pessoais.

É necessário destacar que o DPDC foi bastante cauteloso na análise do consentimento a partir dos *nudges*, deixando claro que não se trataria de ilícitos *per se*. Entretanto, considerou que tais práticas exigiriam, no mínimo, maior nível de monitoramento sobre os desenvolvedores de aplicações na plataforma diante dos maiores riscos à privacidade dos usuários e da própria magnitude do modelo de negócios adotado.

Ponto interessante da decisão foi a questão do ônus da prova, ficando claro que caberia ao Facebook o ônus de comprovar que tais dados não foram indevidamente compartilhados com os responsáveis pela *Cambridge Analytica*, até porque, diante do modelo de *opt-out* adotado, é a plataforma que dispõe de maior capacidade de monitorar o que os desenvolvedores de aplicativos estão fazendo.

Por fim, entendeu o DPDC que o fato de a LGPD estar em *vacatio legis* não impediria o exame da questão, já que o direito à proteção de dados dos envolvidos já estaria assegurado por outros diplomas legislativos notadamente o Código de Defesa do Consumidor, naquilo em que exige o reconhecimento da vulnerabilidade do consumidor, a boa-fé, o equilíbrio entre consumidores e fornecedores e o respeito ao direito dos consumidores à privacidade:

> "Em que pese haver atualmente a Lei Geral de Proteção de Dados brasileira em período de *vacatio legis*, havia legislação específica aplicável ao caso, cuja interpretação deve se dar em consonância com o Código de Defesa do

> Consumidor. Também é importante deixar claro que os arts. 4o, caput, I, III e IV; 6o, II, III, IV e VI, art. 18, art. 31; art. 37, *caput*, e art. 39, na medida em que tal prática se aproveita da vulnerabilidade do consumidor acima narrada e o expõe a método desleal nos serviços e produtos que lhe são ofertados."

Consequentemente, e também com base nas regras do Marco Civil da Internet, entendeu o DPDC que houve prática abusiva em desfavor da coletividade consumerista, consubstanciada na falha no dever de fornecimento aos usuários de informações claras e adequadas quanto à política de privacidade do Facebook, bem como na falha no dever de custódia adequada dos dados fornecidos pelos usuários.

Ainda que optando por uma visão pouco intervencionista do Estado, o que reflete claramente a política econômica do atual governo, entendeu o DPDC que, no caso concreto, estariam presentes os fundamentos para a intervenção excepcional do Estado.

Como se pode observar, também o DPDC, apesar de não aplicar a LGPD, mostrou claramente o seu interesse em dar eficácia aos dispositivos já existentes sobre a matéria, trazendo rica argumentação que adianta várias das discussões que são tratadas diretamente pela LGPD, tais como a finalidade específica do tratamento de dados, os limites e pressupostos do consentimento, bem como o alcance dos deveres de informação e monitoramento.

Esses dois exemplos, somados a diversas outras iniciativas do Ministério Público e dos órgãos de defesa dos consumidores, mostram não só que já existe respaldo legal para a adoção de uma série de medidas em favor da proteção de dados no Brasil, como também que tais iniciativas, mesmo quando baseadas nos dispositivos legais atualmente existentes, estão em total convergência com a LGPD.

Não seria exagero dizer, portanto, que decisões como as mencionadas no presente artigo estão criando uma cultura e um ambiente institucional propício para a proteção de dados e, dessa maneira, pavimentando o caminho para que a LGPD, ao entrar em vigor, possa ter o máximo possível de eficácia.

Logo, as expectativas para 2020, em termos de proteção de dados, parecem ser promissoras, de forma que há boas razões para que os agentes econômicos se adaptem o mais rápido possível às normas da LGPD, bem como às normas já existentes sobre o assunto.

Link https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/protecao-de-dados-e-expectativas-para-2020-12022020

Publicado em 12/02/2020