

Bases compartilhadas de dados pessoais e os riscos para a proteção dos titulares

A redução de assimetria informacional pode ter um alto preço para os titulares de dados

Ana Frazão

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

Fomos treinados a ver a plena informação como um dos pilares para a existência de mercados competitivos e funcionais. Um dos pontos comuns de diversas teorias econômicas é precisamente a ideia de que, quanto mais informação, melhor funciona o mercado. Conseqüentemente, todos os esforços devem ser feitos para reduzir a assimetria informacional.

Nesse sentido, a economia atual caminha para várias iniciativas que, buscam, por meio da redução das assimetrias informacionais, trazer mais competitividade e benefícios aos consumidores por meio de bases comuns de dados. De fato, o elemento comum a iniciativas como o *open banking*, o *open insurance* e o *open health* é de que o acesso comum aos dados dos usuários possibilitará redução de assimetria informacional e conseqüente aumento de rivalidade entre agentes econômicos, que passarão a disputar o melhor interesse do usuário, inclusive para o fim de lhe proporcionar propostas sob medida.

É inequívoco que todas essas iniciativas, até por envolverem dados altamente sensíveis, advertem para a necessidade de observância da LGPD, inclusive realçando que a proteção do usuário deve estar no centro de todos esses sistemas. A grande questão é saber se, de fato, temos alguma garantia ou segurança de que será possível avançar em tais propósitos com a efetiva proteção de dados.

Para além dos riscos de vazamento e outros incidentes de segurança, o ponto fundamental é assegurar que os dados pessoais não apenas só poderão ser utilizados para a finalidade específica que justificou o tratamento, sempre em benefício do titular, mas jamais para o prejudicar, criando-se uma verdadeira ideia de dever fiduciário nesse sentido.

É por essa razão que a questão vai muito além da necessidade do consentimento por parte do usuário. O grande problema é como garantir que não haverá desvios de finalidade, ainda mais quando se sabe que sistemas de inteligência artificial não atendem ao requisito da explicabilidade e não raro operam sob a mais absoluta obscuridade.

Daí por que grande parte das salvaguardas que são cogitadas para a proteção de dados apresentam falibilidades e mesmo quando se insere um agente independente para cuidar dos dados – que pode ser o regulador ou não – a grande questão é como se controla o controlador.

Acresce que, para avançar no tema, é importante considerar o verdadeiro hiato entre o regime normativo previsto pela LGPD e a prática atual. Podemos falar que a transparência e a *accountability* têm sido a regra nos negócios de dados? Podemos falar que o direito à explicação de decisões automatizadas e o direito ao apagamento são realmente eficazes? Podemos falar que não há utilização discriminatória de dados pessoais?

Em muitos desses casos, os titulares de dados não têm nem como obter uma prova de que seus direitos estão sendo efetivamente respeitados. Como se comprovar que o agente de tratamento não utilizou dados para finalidades distintas ou não permitidas? Como se comprovar que o agente de tratamento apagou os dados que ilicitamente obteve sobre um determinado titular?

Para além da ausência de respostas a várias dessas perguntas, ainda há evidências que apontam para o descumprimento de todas essas regras mesmo sem a existência de uma base comum de dados que facilite o acesso à informação por parte dos agentes econômicos. No tocante à discriminação, esta já tem se tornado uma prática em relação a consumidores, mesmo no varejo de bens e serviços, para produtos que aprioristicamente não dependem de uma precificação personalizada, como é o caso do crédito e do seguro.

Mesmo nos setores que exigem essa precificação personalizada, o capitalismo de vigilância apresenta inúmeros desafios que não podem ser negligenciados. Que dados podem ser coletados dos usuários para as análises de risco? Que prognoses ou inferências não podem ser admitidas, sob pena de violação aos direitos? Mesmo em negócios que envolvem precificação individualizada, que discriminações são admissíveis e que discriminações são consideradas abusivas ou ilícitas?

A rigor, as tensões que se potencializam no capitalismo de vigilância requerem não apenas a avaliação de que dados pessoais podem ser utilizados ou não nas avaliações de risco, mas também como podem ser utilizados, inclusive no que diz respeito ao peso proporcional que o dado apresenta para a tomada de decisão por parte do agente econômico.

Veja-se, por exemplo, o interessante exemplo mencionado por Cathy O’Neil¹ sobre o que vem ocorrendo na indústria do seguro de automóveis. A autora traz situações em que motoristas ricos com péssimo histórico de direção têm preços mais favoráveis do que consumidores pobres com ótimo histórico de direção. Tal diferenciação seria justificável ou pode ser considerada uma discriminação abusiva contra os pobres?

Esse tipo de situação nos coloca diante de questões que inclusive transcendem a discussão sobre assimetria informacional, pois dizem respeito à pertinência dos critérios de avaliação de risco e o sopesamento de cada um deles, sob pena de se perpetuar discriminações contra mulheres, negros, pobres e outros grupos vulneráveis.

Shoshana Zuboff² também mostra que o acesso amplo a dados pessoais pode comprometer inclusive a própria ideia do contrato como instrumento de alocação de riscos. Afinal, quando um agente econômico sabe tudo da contraparte – e, em muitos casos, além da base comum de dados, o agente econômico poderá ter acesso a outros dados pessoais dos titulares por diversas outras fontes - ele age na premissa de certeza e não mais de risco, o que coloca o outro contratante em uma posição de extrema fragilidade e compromete a própria funcionalidade da economia de mercado.

¹ O’NEIL, Cathy. *Weapons of math destruction. How big data increases inequality and threatens democracy*. EUA: Crown, 2016.

² ZUBOFF, Shoshana. *The age of surveillance capitalism. The fight for a human future at the new frontier of power*. New York: Public Affairs, 2019.

Todos esses aspectos são ora expostos para se demonstrar que, sob vários fundamentos, a preservação dos dados pessoais é fundamental não apenas para a proteção dos usuários, como igualmente para a própria manutenção do mercado e do contrato como instrumento de alocação de riscos minimamente equilibrado para ambas as partes.

Daí por que a busca por informação, no atual contexto, precisa ser compatível com o regime de proteção de dados pessoais, o que nos desperta para duas questões fundamentais:

- (i) há que se buscar mecanismos efetivos para que informações coletadas para determinados fins não sejam utilizadas para outros fins, o que enseja discussões que vão desde a natureza das obrigações dos agentes de tratamento – como a questão dos deveres fiduciários – até questões sobre ônus da prova quanto ao cumprimento de tais requisitos;
- (ii) há que se buscar regras mais transparentes e objetivas para disciplinar a atuação de agentes econômicos que precisam precificar individualmente o risco, inclusive para se saber que dados podem ser utilizados e como podem ser utilizados, a fim de se evitar a discriminação ilegal ou abusiva ou outras violações aos direitos dos titulares.

Como se vê, os desafios do capitalismo de vigilância não são triviais, o que contrasta com o otimismo normalmente presente na defesa do acesso compartilhado a dados. Nesses casos, embora ninguém questione a necessidade de observância à LGPD, dificilmente são apresentadas propostas concretas de como será assegurada a eficácia da lei e como serão administrados vários dos *tradeoffs* já apontados, até porque o aumento da competição não pode se dar às custas da desproteção dos titulares de dados pessoais.

Uma coisa é certa: é preciso reconhecer que a proteção efetiva de dados pessoais impõe efetivamente a manutenção de uma zona indevassável do indivíduo, o que precisa ser considerado diante de todas as iniciativas que envolvem bases comuns de dados. Para assegurar os direitos dos titulares de dados e a própria funcionalidade do mercado, a manutenção da assimetria informacional nessa área pode ser uma opção preferível à tentativa de reduzir tal assimetria sem os devidos cuidados e salvaguardas.

Publicado em 06/09/2023

Link: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/bases-compartilhadas-de-dados-pessoais-e-riscos-para-a-protecao-dos-titulares-06092023>