Requisitar dados não é suficiente para a proteção da privacidade. É preciso tratar a assimetria de informação.

Elvino de Carvalho Mendonça & Rachel Pinheiro de Andrade Mendonça

A disruptura digital pelo qual passa o mundo não tem sido sem dor. As "maravilhas" da tecnologia materializadas nos smartphones cobram o seu preço e esse preço é o ataque frontal a privacidade e a liberdade do ser humano.

Estas pequenas "maravilhas" transferem dados pessoais a cada acesso ou transação para as *Big techs*, que, a partir de infinitos acessos e/ou transações realizadas por cada detentor de smartphone, são capazes de construir bases de dados gigantescas com informações pessoais as mais variadas possíveis e em um nível de detalhe tão pequeno quanto se possa imaginar.

O passo seguinte é a utilização destas informações pela empresa para fazer negócios sem o consentimento do ser humano, na medida em que captam, armazenam, classificam, precificam e alienam os comportamentos, pensamentos e sentimentos de cada ser humano sob o manto de um "capitalismo de vigilância", cujos reais interessados nesse grande mercado de predição de comportamentos futuros são as empresas de marketing e publicidade e o real valor desse modelo de negócios não são mais os usuários e sim os seus comportamentos, pensamentos e sentimentos.

Segundo Shoshana Zuboff:

> "o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais.

> Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro." [1]

Prossegue a Autora Shoshana Zuboff aduzindo que,

[1] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. Tradução George Schlesingerr. Rio de Janeiro: Intrínseca, p. 23.

> "[p]or enquanto, digamos que os usuários não são produtos, e sim que são as fontes de suprimento de matéria-prima." [2]

No entanto, o que é ainda mais grave é a utilização destas informações para atuar em um nível abaixo da consciência humana, fazendo com que o ser humano seja induzido/manipulado digitalmente a consumir não o que deseja, mas sim aquilo que a empresa deseja. Neste ponto, vale citar Byung-Chul Han que, parafraseando Walter Benjamin, aduz ao *inconsciente óptico* a seguinte estrutura:

> "Os pensamentos de Benjamin sobre o inconsciente óptico podem ser transpostos ao regime da informação. Big Data e inteligência artificial constituem uma *lupa digital* que explora o inconsciente, oculto ao próprio agente, atrás do espaço da ação consciente. Em analogia ao consciente óptico, podemos chamá-lo de inconsciente digital. O *Big Data* e a Inteligência Artificial levam o regime de informação a um lugar em que é capaz de influenciar nosso

[2] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. Tradução George Schlesingerr. Rio de Janeiro: Intrínseca.

> comportamento em um nível que fica embaixo do liminar da consciência."[3]

A proteção de dados no Brasil se encontra tratada na Lei Geral de Propriedade de Dados (LGPD)[4], diploma legal que *dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural* (art. 1º) e que *cria a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal (art. 55-A).*

E um dos requisitos para o tratamento dos dados previstos na LGPD para fazer a proteção de dados individuais está previsto no caput do art. 9º, que pugna 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 de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.*

A garantia de acesso aos dados pelo usuário é uma condição necessária, mas não suficiente para que o tratamento de dados individuais atinja o objetivo da privacidade, principalmente porque há uma abissal assimetria de informação[5] entre a *big tech* e o usuário, assimetria que é potencializada pelo fato de que transparência dos dados para o usuário não pode ultrapassar a

---

[3] HAN, Byung-Chul. Infocracia: digitalização e a crise da democracia. Tradução de Gabriel S. Philipson. Petrópolis: Editora Vozes. 2022, p.23.

[4] L13709 (planalto.gov.br)

[5] VARIAN, HALL. Intermediate Microeconomics: A Modern Approach. Fifth Edition. W. W. Norton. 1999.

proteção dos segredos de empresa e industriais, conforme postula o art 6º, inciso VI[6], da mesma lei.

Acertadamente, a LGPD atribui à ANPD a competência para *articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação* (art. 55-J, inciso XXIII) e a competência para que [*a] ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental coordenem as suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei* (art. 55-J, § 3º).

A atuação conjunta da ANPD e das agências reguladoras permite chamar à atenção para o real problema que envolve a proteção de dados, que é a assimetria de informação existente entre as empresas (*Big techs*) que captam os dados, os usuários, as agências reguladoras setoriais e a ANPD, conforme mostra a figura 1.

No modelo exposto na figura 1, verifica-se que embora o usuário detenha a propriedade do dado, quem o utiliza e desenvolve políticas comerciais sem que o usuário tenha como identificá-las é a empresa. Da mesma forma, ainda que a agência reguladora, em parceria com a ANPD, detenha alguns instrumentos para a obtenção dos dados e dos sistemas de mineração de dados, o *core* da informação obtida é o segredo do

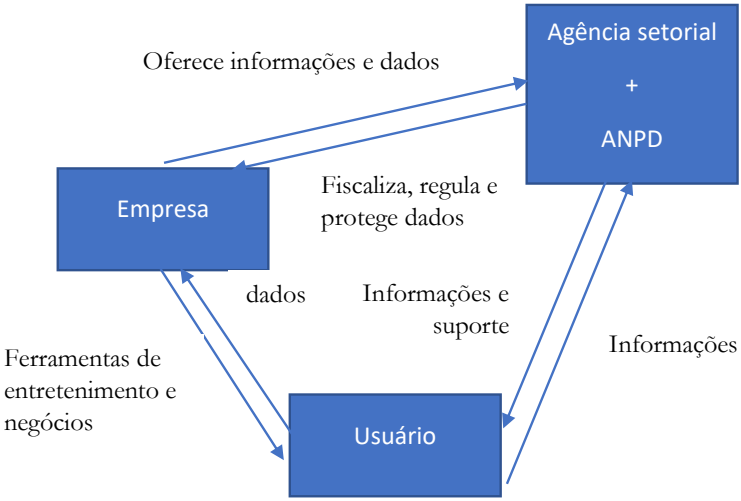
---

[6] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

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;

negócio da empresa e ela tem incentivos econômicos para não revelar a nenhum agente, sobretudo ao Estado.

Figura 1. O problema do agente-principal na proteção de dados



Elaboração: Autores

Conforme expresso anteriormente, a LGPD garante ao usuário o acesso a todas as suas informações, bastando, apenas, que o usuário as solicite à empresa. No entanto, o dado é só o insumo e tem pouca serventia se não vier acompanhado das informações geradas por ele e, sobretudo, de como a empresa utilização essa informação no mercado de predição de comportamentos futuros, com altíssimo lucro.

Portanto, é exatamente o que e como as *Big techs* utilizam os dados dos usuários que é o "X" da questão da proteção de dados. Solicitar dados, algoritmos e outras coisas que o valham não soluciona o problema da privacidade dos usuários, pois o abuso do

direito de privacidade por parte das empresas não está no dado, mas na informação gerada por este dado, e se essas empresas não estão dispostas a informá-las, a razão é que ela detém muito mais informações a respeito do seu negócio que o regulador.

O caminho para fazer com que as *Big techs* respeitem o direito de privacidade do usuário passa por fazer com que o retorno financeiro da empresa em respeitar o direito seja superior ao retorno financeiro de não o respeitar. Um caminho possível é gerar incentivos sobre o gerador do benefício para a empresa[7], que é o usuário.

A obrigação de apresentar dados não é suficiente para fazer com que a empresa pare de avançar sobre a privacidade dos usuários, pois repassar os dados para o usuário não altera o retorno esperado da empresa.

No entanto, é preciso que o usuário seja beneficiado pela agência reguladora (Estado) através de um mecanismo em que a *big tech* seja obrigada a revelar informações que não desejaria para o regulador. Esse é o árduo trabalho que deverá ser enfrentado pela regulação econômica envolvendo as agências reguladoras e a ANPD.

---

[7] Um exemplo importante a se considerar diz respeito a nota legal. Neste caso, ao colocar o CPF nas suas compras o consumidor fica automaticamente habilitado a participar de sorteio realizado pela Secretaria de Estado de Fazenda, onde são oferecidos descontos no pagamento de impostos (ex. IPVA), entre outras coisas. Ao solicitar que o consumidor solicite a inserção do seu cpf na nota fiscal, o estabelecimento comercial fica automaticamente obrigado a emitir a nota fiscal e, com isso, fica obrigado a recolher os impostos devidos. A obrigação de emitir nota fiscal por si só não é suficiente para fazer com que o comerciante de fato a emita, mas a oferta de benefício para o consumidor obriga a emissão da nota fiscal por parte do comerciante.