



Vulnerabilidade algorítmica do consumidor e hipertrofia do consentimento

17/09/2025

As empresas do ramo da tecnologia, as chamadas *big techs*, são detentoras do monopólio das plataformas digitais voltadas para as interações pessoais, como por exemplo, as redes sociais (Facebook, Instagram, X) e o WhatsApp. O usuário (consumidor), para poder ter acesso a tais plataformas, deve previamente aceitar os termos e condições de privacidade que lhe são impostos (os *cookies*), em cumprimento às normativas vigentes. Essa fórmula é conhecida de todos. Mas com relação a ela, queremos refletir sobre a seguinte questão: o atual modelo referente aos termos e condições de privacidade como requisito para o tratamento dos dados pessoais a quem beneficia? Esse modelo reduz ou acentua a vulnerabilidade algorítmica do consumidor que atua no mundo digital [1]?

Aceitar os *cookies* com um simples clique sem sequer ler os termos e condições já é parte do nosso cotidiano. Os mais distintos motivos, entre os quais “a falta de tempo”, “a falta de interesse”, “a dificuldade na compreensão”, revelam que a grande maioria dos usuários das plataformas digitais não lê as condições contratuais com as quais consentiu. O consentimento prestado desta forma, seria, portanto, válido? Estamos, sem lugar a dúvidas, diante de uma verdadeira “crise do consentimento”.

Evidentemente, não há como negar os benefícios que as redes sociais proporcionam; contudo, estas mesmas redes apresentam problemas que são invisíveis aos olhos do consumidor médio, e que se vinculam à vigilância que as *big techs* exercem sobre os seus usuários, a partir da coleta e tratamento de dados pessoais, que nada mais são que informações relacionadas à vida privada do particular. Basta que o usuário realize um único acesso ou uma única pesquisa, para que anúncios e propagandas, por exemplo, sejam disparados conforme o seu perfil, previamente estabelecido por algoritmos com base no acesso a esses dados, fomentando, assim, a sociedade de consumo e o consequente superendividamento.

A partir do exposto, percebe-se que muitos dos problemas da era tecnológica decorrem exclusivamente da crise que assola o atual modelo de consentimento. Um consentimento com o qual a sociedade não mais se preocupa, porque supostamente está sendo prestado por “livre e espontânea vontade”. Um consentimento que é requisito *sine qua non* para a utilização gratuita de um serviço digital. Um consentimento com relação ao qual na maior parte dos casos o usuário nem sequer compreende os termos e a extensão de seus efeitos na sua vida privada.

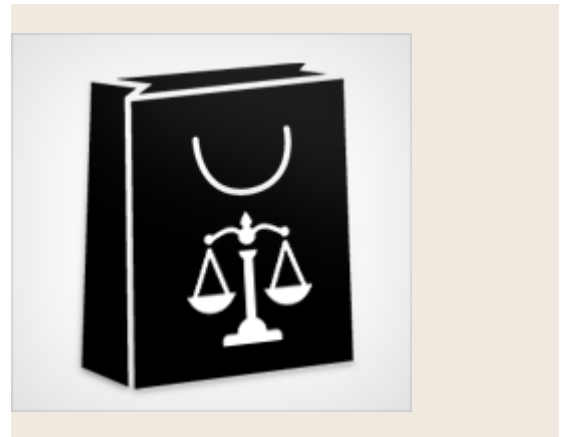
Como já referido, a crise do consentimento esbarra, em primeiro lugar, na vigilância [2] excessiva levada a cabo pelas *big techs*, que terminam por violar a privacidade de milhões de usuários com a finalidade de obter lucro a partir do acesso aos dados pessoais que foram fornecidos obrigatoriamente, já que para acessar as redes é preciso aceitar os termos pré-estabelecidos. Ou seja, as mesmas empresas que deveriam exercer o dever de cuidado,

garantindo segurança aos usuários, são as que promovem, por meio de suas práticas, o acirramento das vulnerabilidades inerentes ao mundo digital, que revelam uma assimetria técnica abissal entre o usuário titular dos dados, por um lado, e aqueles que realizam o tratamento destes dados, por outro.

A lógica das *big techs* é simples: quanto mais a sociedade ficar dependente das redes sociais, mais dados serão gerados e mais lucros serão obtidos, o que aumenta invariavelmente o valor de mercado deste ativo. Isso porque o tratamento de dados é extremamente lucrativo, em razão do baixo custo de seu processamento se comparado às informações que são coletadas a partir do aceite dos termos e condições de uso, que possibilitam uma incrível abertura de mercado.

Não obstante, essa situação revela a existência de um paradoxo. Sobre o tema, Byung-Chul Han, em sua obra *Infocracia: Digitalização e a Crise da Democracia*, destaca que na sociedade da informação e da hiperconexão, as pessoas não se sentem vigiadas, mas sim livres [3]. Em outras palavras, os usuários não se sentem controlados, pois os riscos do mundo virtual lhes são imperceptíveis até que ocorra, de fato, uma violação aos direitos personalíssimos. Diante desse cenário, será que ainda é possível falar de privacidade no mundo digital?

Outra variável que evidencia a vulnerabilidade algorítmica dos consumidores que atuam nas redes sociais se vincula à utilização de seus dados por parte destas plataformas, com o único intuito de fomentar o consumo. Esses *players* incitam o usuário a que compre, de forma compulsiva, para além de suas necessidades, o que é feito por meio de anúncios publicitários e propagandas veiculadas em campos específicos de *marketplace*, como no caso do Instagram e do Facebook, que originalmente foram criados apenas para interações sociais por meio de publicações pessoais.



Diante desse cenário caótico, no qual circulam bilhões de dados pessoais em prol do mercado, evidenciando a vulnerabilidade algorítmica a que está exposto o consumidor, qual seria o papel a ser desempenhado pelas organizações internacionais que atuam em âmbitos integrados e, conseqüentemente, pelos Estados como atores primários no campo da regulação?

A União Europeia, como importante *stakeholder* em matéria regulatória, já vem desenvolvendo estratégias, com a finalidade de estabelecer limites à atuação das plataformas digitais. Cita-se, por exemplo, a aprovação da Lei de Serviços Digitais (DSA, no acrônimo em inglês) [4], vigente desde novembro de 2022, e a Lei de Mercados Digitais (DMA, no acrônimo em inglês) [5], vigente desde setembro de 2023, as quais buscam estabelecer um espaço digital mais seguro aos usuários, atendendo às determinações da “Nova Agenda do Consumidor 2020-2025”, que estabeleceu como eixo prioritário da política europeia de proteção ao consumidor a transformação digital.

Nesse sentido, demonstrando o robustecimento da política de proteção ao consumidor no âmbito digital integrado, Christel Schaldemose, eurodeputada dinamarquesa líder para a

temática da Lei dos Serviços Digitais, em seu discurso, foi categórica ao dizer que *“Por muito tempo, as gigantes da tecnologia beneficiaram[-se] da ausência de regras. O mundo digital transformou-se num faroeste, com as [empresas] maiores e mais fortes a ditar as regras. Mas há um novo xerife na cidade – a DSA. A partir de agora, as regras e os direitos serão reforçados”* [6].

Mais regulamentações

Igualmente, merecem destaque outras normas da União Europeia, como o próprio Regulamento Geral de Proteção de Dados Pessoais (RGPD) [7], considerado uma das normativas mais disruptivas e inovadoras da atualidade, que vem influenciando a adoção de leis ao redor do mundo, como por exemplo, a criação da Lei Geral de Proteção de Dados (LGPD) [8], no Brasil. O RGPD, em seu artigo 6º, item 1, alínea “a” determina que o tratamento dos dados pessoais somente será lícito quando se verificar que o seu titular tenha prestado o seu consentimento para uma ou mais finalidades específicas.

Tal determinação fez com que em diversos países, inclusive fora do bloco europeu, começasse a ser exigido o consentimento do usuário, de forma expressa, através do aceite aos termos e condições de uso, como medida de licitude para o seu tratamento. Desse modo, percebe-se que embora o RGPD seja uma normativa de Quarta Geração, ele ainda se pauta no consentimento para determinar a licitude do tratamento de dados pessoais, não abordando o tema apenas de forma genérica, mas garantindo condições que lhe são aplicáveis, nos termos do artigo 7º do próprio Regulamento.

Em outras palavras, muito embora parem dúvidas sobre a real efetivação do consentimento, o bloco europeu segue reconhecendo-o como pressuposto essencial para a garantia da privacidade no ambiente *online*. Nesse sentido, o Parlamento Europeu e o Conselho, desde 2017, estão buscando remodelar a Diretiva 2002/58/CE [9] relativa à privacidade e às comunicações eletrônicas (Diretiva *ePrivacy*), para reformular os padrões pré-estabelecidos para os extensos termos de privacidade, justamente para gerar mais confiança e segurança no mundo digital. A diretiva objeto da reforma é de 2002 e não mais consegue suprir as necessidades atuais, já que as novas tecnologias se transformaram drasticamente desde então, assim como o seu impacto em quem as utiliza.

Outra grande inovação normativa da União Europeia é o Regulamento de Inteligência Artificial [10] (*EU IA ACT*), norma pioneira que se ocupa dos limites éticos para a utilização dos sistemas de IA, e que, portanto, possui relação direta com o tratamento de dados pessoais coletados a partir da interação dos usuários nas redes sociais. Essa regulamentação normativa igualmente tem servido de parâmetro para a criação de projetos de leis nos mais distintos países, entre os quais o Brasil, que já se valeu de suas determinações muito antes da própria aprovação do regulamento para a elaboração do Projeto de Lei nº 2338,[11] de 2023, já aprovado no Senado e que atualmente tramita na Câmara de Deputados, desde março de 2025.

Protagonismo do bloco e contexto brasileiro

Como se verifica, a União Europeia vem envidando esforços para buscar um ambiente digital mais seguro e igualitário *intra*zona, ao mesmo tempo em que tais medidas evidenciam o protagonismo regulatório do bloco europeu para além de suas fronteiras, fenômeno conhecido como “Efeito Bruxelas” [12]. Dessa forma, o processo de integração referido tem buscado promover a confiança do consumidor na economia digital, em razão de que cidadãos e empresas só utilizam serviços digitais em escala quando confiam na proteção de seus dados. Inclusive, tais medidas legislativas são de aplicação obrigatória, uniforme e preferente no âmbito do Direito interno dos Estados Membros.

Quanto ao cenário brasileiro, e sem filiar-se à corrente que identifica o protagonismo regulatório europeu como mais uma demonstração de colonialismo, compreende-se que os avanços normativos da União Europeia podem sim servir como fonte para os futuros passos da legislação brasileira voltada à proteção do usuário nas redes sociais. O Congresso Nacional já vem promovendo debates quanto à regulação destas plataformas, que precisam tomar uma maior robustez justamente para proteger efetivamente ao usuário e ao mesmo tempo acompanhar as mudanças que se operam rapidamente sobre a realidade tecnológica.

[1] Sobre o tema, ver: VERBICARO, Dennis. **Algoritmos de consumo**: discriminação, determinismo e solução online de conflitos na era da inteligência artificial. São Paulo: Revista dos Tribunais, 2023.

[2] ZUBOFF, Shoshana. **A ERA DO CAPITALISMO DE VIGILÂNCIA**: a luta por um futuro humano na nova fronteira de poder. Rio de Janeiro: Intrínseca, 2021.

[3] HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Tradução: Gabriel S. Philipson. Petrópolis: Editora Vozes, 2022. p. 13.

[4] UNIÃO EUROPEIA. Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho de 19 de outubro de 2016 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). **Jornal Oficial da União Europeia**, Luxemburgo, n. L 277/1, p. 1-102, 27 out. 2022. Disponível [aqui](#).

[5] UNIÃO EUROPEIA. Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais). **Jornal Oficial da União Europeia**, Luxemburgo, nº L 265/1, 1-66, 12 out. 2022. Disponível [aqui](#).

[6] PARLAMENTO EUROPEU. **A Lei dos Mercados Digitais e da Lei dos Serviços Digitais da UE em detalhe**. Bruxelas: Parlamento Europeu, 2025. Disponível [aqui](#).

[7] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva

95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Luxemburgo, n. L 119, 4 maio 2016. Disponível [aqui](#).

[8] BRASIL. **Lei nº 13.709/18**. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível [aqui](#).

[9] UNIÃO EUROPEIA. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações electrónicas). **Jornal Oficial da União Europeia**, Luxemburgo, n. L 201/37, 31 jul. 2002. Disponível [aqui](#).

[10] UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). **Jornal Oficial da União Europeia**, Luxemburgo, n. L, 12 jul. 2024. Disponível [aqui](#).

[11] Para mais detalhes sobre o projeto, ver: CÂMARA DOS DEPUTADOS. **PL 2338/2023**. Disponível [aqui](#).

[12] BRADFORD, Anu. The Brussels effect: how the European Union rules the world. New York: Oxford University Press, 2020.

Fonte: <https://conjur.jumps.com.br/2025-set-17/vulnerabilidade-algoritmica-do-consumidor-e-hipertrofia-do-consentimento-o-papel-dos-modelos-regulatorios-da-ue/>