A VULNERABILIDADE DOS TITULARES DE DADOS DIANTE DE GRANDES PLATAFORMAS E BIG TECHS: UM PARALELO ENTRE AS VIOLAÇÕES AO GDPR E À LGPD NO QUE TANGE À BASE LEGAL DO CONSENTIMENTO

THE DATA SUBJECTS' VULNERABILITY IN THE FACE OF BIG PLATFORMS AND BIG TECHS: A PARALLEL BETWEEN THE VIOLATIONS OF THE LGPD AND THE RGPD REGARDING THE LEGAL BASIS OF CONSENT

Isabela de Araújo Santos[1]

Data de Submissão: 09/03/2022
Data de Aceite: 13/06/2022

Resumo: O artigo se propõe a analisar as facetas da manipulação sub-reptícia utilizadas pelas grandes plataformas e *big techs* para coleta de dados pessoais de seus usuários e consumidores a partir da inobservância das salvaguardas e direitos relativos à base legal do consentimento para tratamento de dados. A partir de estudos documentais e de um paralelo entre a legislação europeia e brasileira, traçando semelhanças e distinções entre o Regulamento Geral de Proteção de Dados europeu e a Lei Geral de Proteção de Dados brasileira, foi possível averiguar a existência de ilicitudes e abusividades das práticas empregadas pelas grandes empresas de tecnologia, como controladoras, para obtenção de consentimento inválido a fim de tratar os dados pessoais coletados de seus consumidores no papel de titulares. Conclui-se que a vulnerabilidade dos usuários e consumidores de plataformas digitais é alarmante no contexto de uma economia capitalista fomentada por fluxo de dados pessoais, necessitando de urgente tutela e *enforcement* por parte de instituições competentes na defesa de seus direitos e garantias.

Palavras-chave: Consentimento. GDPR. LGPD. Grandes plataformas. *Big techs*.

1 Graduanda em Direito pela Universidade de Brasília e estagiária da área de proteção de dados e análise regulatória na Bioni Consultoria. Pesquisadora bolsista do CNPq e pesquisadora voluntária do Grupo Constituição Empresa e Mercado (GECEM), da Universidade de Brasília (UnB), e do Núcleo de Direito Concorrencial e Economia Digital (NUCED), da Universidade de São Paulo (USP). E-mail para contato: isabeladearj@gmail.com.

Abstract: The article proposes to analyze the facets of surreptitious manipulation used by big platforms and big techs to collect personal data of their users and consumers through the disregard of safeguards and rights related to the legal basis of consent for data processing. Based on documentary studies and a parallel between European and Brazilian legislation, drawing similarities and distinctions between the European General Data Protection Regulation and the Brazilian General Data Protection Law, it was possible to inquire that there are illicit and abusive practices employed by big technology companies, as controllers, to obtain invalid consent in order to process personal data collected from their consumers in the role of data subjects. It was possible to conclude that the vulnerability of users and consumers of digital platforms is alarming in the context of a capitalist economy fostered by the flow of personal data, requiring urgent protection and enforcement by competent institutions in defense of their rights and guarantees.

Keywords: Consent. GDPR. LGPD. Big platforms. Big techs.

1 - CONTEXTUALIZAÇÃO DE DISSIPAÇÃO DO LIVRE-ARBÍTRIO DOS TITULARES DE DADOS

> Minha ilusão de livre-arbítrio provavelmente vai se desintegrar à medida que eu me deparar, diariamente, com instituições, corporações e agências do governo que compreendem e manipulam o que era, até então, meu inacessível reino interior. (...) Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso, vamos perceber o universo inteiro como um fluxo de dados, considerar organismos pouco mais que algoritmos bioquímicos e acreditar que a vocação cósmica da humanidade é criar um sistema universal de processamento de dados — e depois fundir-se a ele.[2]

O trecho acima transcrito descreve a visão de Yuval Harari sobre um dilema que a sociedade contemporânea enfrenta diariamente: como se adaptar diante de tamanho fluxo de dados e constantes inovações proporcionadas pelo aprimoramento tecnológico, tendo repercussões em diversas searas da vida social, como a área jurídica e, especificamente, as salvaguardas referentes ao direito fundamental à proteção de dados pessoais e ao livre exercício do consentimento, as quais serão o foco deste artigo.

Essa perspectiva coaduna-se com a proposta trazida neste trabalho, na medida em que considera-se que a economia movida por dados mudou consideravelmente as relações sociais, mais notadamente no que concerne às práticas abusivas realizadas por plataformas digitais e *big techs* para coletar os dados pessoais de seus usuários e consumidores, burlando muitas vezes regras e normas asseguradas por leis referentes ao livre exercício do consentimento.

A regulação jurídica do tratamento de dados pessoais está amparada na ideia de que o indivíduo deve usufruir de autodeterminação informacional, ou seja, "deve ter o poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de livre desenvolvimento de sua personalidade"[3].

Logo, para que o indivíduo consiga exercer seu poder de autodeterminação informativa[4], torna-se necessário um instituto jurídico pelo qual possa expressar sua

---

2 HARARI, Y. N. **21 Lições para o Século 21**. São Paulo: Companhia das Letras, 2018, pp. 60-68.

3 MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 60

4 Termo trazido à doutrina brasileira por MENDES, L.S., Op. Cit., 2014.

vontade de autorizar ou não o processamento e tratamento de seus dados pessoais: o consentimento[5].

Desta feita, primeiramente, serão abordadas as mudanças decorrentes do uso de *Big Data* e de *big analytics* por grandes plataformas e *big techs* a fim de obter o consentimento de seus usuários e consumidores de maneira sub-reptícia. Posteriormente, o artigo se proporá a expor como a Lei Geral de Proteção de Dados (LGPD) brasileira e o Regulamento Geral de Proteção de Dados (GDPR) europeu definem o consentimento válido de titulares de dados, bem como a relevância da autodeterminação informativa para a licitude dessa base legal.

Por fim, será esclarecido como e por que as práticas atuais das grandes plataformas e *big techs* violam as disposições legais trazidas pelo GDPR e pela LGPD, tolhendo a capacidade decisória dos seus usuários e consumidores ao não proporcionar-lhes um consentimento válido dentro dos pré-requisitos estabelecidos pelas legislações. Assim, tornar-se-á demonstrada a vulnerabilidade dos titulares de dados face às essas empresas cujo poderio econômico sem precedentes cria uma possibilidade de manipulação comportamental que interfere diretamente no livre convencimento e na tomada de decisões de seus consumidores.

2 - O PODER DE TOLHER O LIVRE-ARBÍTRIO DE SEUS USUÁRIOS E CONSUMIDORES: COMO AS GRANDES PLATAFORMAS E AS BIG TECHS MANIPULAM A TOMADA DE DECISÕES DE SEUS USUÁRIOS

Em um contexto democrático, no qual estamos formalmente inseridos, a informação passa a ser um alicerce central para o exercício de direitos. Considerando, desta feita, a tecnologia contemporânea pela qual se propaga a informação, podemos notar uma grande importância do adequado fluxo e compartilhamento de dados para a autodeterminação informativa dos indivíduos.[6]

Com o escândalo da Cambridge Analytica, ocasião em que os dados de cerca de 87 milhões de pessoas foram extraídos ilicitamente, foi notado um investimento maciço das plataformas digitais em influenciar e manipular comportamentos por meio da coleta de informações de seus usuários[7]. Isso porque a obtenção de dados pessoais, como novo petróleo da economia contemporânea, tornou-se fundamental como **arma psicológica**, de maneira a fomentar e retroalimentar o capitalismo de vigilância[8].

---

5 MENDES, L.S., Op. Cit., 2014.

6 [referência ao(s) autor(es) suprimida]

7 [referência ao(s) autor(es) suprimida]

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

Esse termo, cunhado por Shoshana Zuboff, descreve uma nova ordem econômica que reivindica a experiência humana como matéria prima, a princípio gratuita, para práticas comerciais dissimuladas de extração, previsão e vendas. Diante disso, surgiu então uma nova lógica econômica parasítica na qual a produção é estreitamente vinculada a uma arquitetura global de influência na modificação comportamental[9].

Influenciar comportamentos, desta feita, passou a ser o objetivo central das grandes plataformas e das *big techs* dentro do capitalismo de vigilância, visto que a obtenção de dados pessoais, juntamente com sua análise - recorrentemente por meio da utilização de algoritmos -, permite às grandes plataformas digitais um poderio econômico sem precedentes e uma alta manipulação preditiva e captológica comportamental de seus usuários.

A partir das análises algorítmicas, torna-se possível entregar conteúdos personalizados aos usuários, utilizando técnicas de *profiling* e *microtargeting*, de modo a influenciar mais eficientemente suas tomadas de decisões dentro desse modelo capitalista datificado.

Logo, pode-se aferir dessa contextualização que os dados e sua capacidade de processá-los a fim de convertê-los em informações úteis guardam uma relação de interdependência entre si, só fazendo sentido diante um do outro, já que "a geração de valor depende do acesso simultâneo aos dois recursos", não podendo ser isolados[10].

Frank Pasquale defende que os controladores de dados pessoais não focam em tratar adequadamente os titulares de dados - respeitando suas garantias constitucionais e infraconstitucionais -, mas sim em **maximizar seus lucros**, independentemente das consequências negativas que essa conduta possa trazer àqueles cujos dados foram fornecidos.

Esse fenômeno de investimento em processos algorítmicos de captura, produção e análise de informação é denominado "**economia psíquica dos algoritmos**"[11]. O investimento se realiza em diversas áreas - tecnocientífica, econômica e social - e em diferentes dispositivos e serviços, a exemplo de redes sociais, aplicativos, serviços de streaming, plataformas de compartilhamento, entre outros; de maneira a modular comportamentos a fim de maximizar a lucratividade empresarial.

---

9 [referência ao(s) autor(es) suprimida]

10 FRAZÃO, A. **Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência**. In: Empresa, Mercado e Tecnologia, 2019, p. 182.

11 [referência ao(s) autor(es) suprimida]

Para compreendermos melhor esse modelo de negócios das plataformas digitais e sua influência nos mercados e consequente sobre seus consumidores, insta salientar a sua atuação nas diversas esferas do poder econômico.

A primeira esfera está representada no **poder de conexão** - *gatekeeper power* -, visto que as plataformas digitais põem em contato diversos agentes econômicos, consumidores e até mesmo governos[12], sendo muitas vezes a única opção de interação e intermédio possível entre esses *players*. Tornam-se, portanto, os centros de uma complexa teia de relações empresariais, cujo poder e suas repercussões na proteção de dados pessoais devem ser ponderados a fim de se evitar possíveis ilícitos.

Outra importante dimensão das plataformas é o **poder de alavancagem** (*leveraging power*), uma vez que passam a integrar os mesmos mercados de vários de seus usuários e, desse modo, fazem com que haja a possibilidade de que as plataformas digitais passem a **privilegiar seus próprios interesses em detrimento daqueles dos seus usuários**. Logo, o problema da formação de conglomerados e monopólios ganha uma nova perspectiva com essa esfera de poder, a partir do momento em que há o aumento de poder financeiro e riscos de fechamento de mercado decorrentes de concentração, vulnerabilizando o poder de escolha dos consumidores sobre os produtos e serviços ofertados no mercado.

Ademais, as plataformas detêm também o **poder de extração e exploração** de dados pessoais, já que podem monitorar seus usuários facilmente e associar um grande número de informações úteis sobre eles, obtendo, assim, diversas vantagens econômicas.

Uma outra dimensão importante a ser elucidada é a do **poder de comunicação**, a partir do momento em que se parte da premissa de Herbert Simon de que a riqueza de informação gera uma pobreza de atenção[13]. Dessa maneira, as plataformas digitais podem filtrar as informações e direcioná-las a seus usuários, moldando-as de acordo com o interesse de cada um deles, configurando a dimensão do chamado **poder de influência e de manipulação.**

Essas esferas de poder demonstram, portanto, um **acúmulo de poder econômico** maciço por parte dessas plataformas, de modo a muitas vezes ameaçar a autodeterminação informativa de seus usuários, bem como sua privacidade e o próprio direito à proteção de seus dados pessoais; sendo este, segundo Laura Schertel Mendes, um direito em "sua essência multidimensional, na medida em que busca

12 FRAZÃO, Op. Cit., 2019, p. 184.

13 SIMON, H. **Designing organizations for an information-rich world.** In: GREENBERGER, M. Computers, communications and the public interest. Baltimore: The John Hopkins Press, 1917.

equilibrar os variados interesses de usos e os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos"[14].

Além disso, Danilo Doneda expõe claramente o perigo que correm os titulares de dados hoje:

> **O tratamento de dados pessoais, em particular por processos automatizados, é, ao mesmo tempo, uma atividade que apresenta riscos cada vez mais claros. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais**; na eventualidade de esses dados não serem corretos e representarem erroneamente seu titular; na **sua utilização por terceiros sem o conhecimento ou autorização de seu titular; na eventualidade de serem utilizados para fins discriminatórios, somente para citar algumas hipóteses concretas**. Daí a necessidade de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que são, no fundo, expressão direta de sua própria personalidade. (...)
>
> **Os bancos de dados que contêm dados pessoais, tão comuns em nossos dias, proporcionam uma nova definição dos poderes e direitos sobre as informações pessoais e, consequentemente, sobre a própria pessoa**. Aumenta o número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo. (...)[15] - (grifos meus)

Diante do poder de manipulação das plataformas sobre os indivíduos, cabe destacar ainda a afirmação de Tim Wu de que o verdadeiro negócio de muitas delas é influenciar consciências[16], através de seu poder de comunicação, sendo capazes de modificar crenças e opiniões dos mais diversos cunhos: políticos, morais, religiosos e sociais.

As plataformas digitais adquiriram tamanha proporção no capitalismo de vigilância, que muitas delas possuem hoje posição dominante em diversos mercados,

---

14 MENDES, L.S., Op. Cit., 2014, p. 174.

15 DONEDA, D. **O Direito Fundamental à Proteção de Dados Pessoais**. In: MARTINS, G.M.; LONGHI, J. V. R. (Orgs.). Direito Digital: Direito Privado e Internet. 2. Ed. São Paulo: Editora Foco, 2019, p. 35-54.

16 WU, T. **The attention merchants**: the epic scramble to get inside our heads, New York; Kopf, 2016.

tornando-se inclusive o próprio mercado[17]. Surge daí o receio de uso desse poderio para proteger e fomentar ainda mais seu domínio, mesmo em detrimento dos consumidores – como titulares de dados –, especialmente diante do crescimento das barreiras à entrada nos mercados[18].

2.1 - MÉTODOS DE PERSUASÃO UTILIZADOS POR GRANDES PLATAFORMAS E BIG TECHS PARA COLETA DE DADOS DE SEUS USUÁRIOS

A psicologia comportamental tem mostrado que as pessoas apresentam limitações de racionalidade e influências de emoções e vieses[19] que comprometem drasticamente o livre exercício de seus direitos de liberdade, autodeterminação informativa, privacidade e proteção de dados pessoais, garantidos no ordenamento jurídico europeu e pátrio, corroborados com a vigência do Regulamento Geral de Proteção de Dados e da Lei Geral de Proteção de Dados.

Dentro da economia psíquica dos algoritmos, no campo do *Behavioral Economics*, há duas principais matrizes[20] que explanam os métodos de persuasão utilizados por grandes plataformas e *big techs* para coleta de dados de seus usuários: a matriz da predição e a matriz da captura.

A matriz preditiva de detecção de dados pessoais se constitui em métodos de detectar e reconhecer emoções medidas pela precisão do acerto, seja da personalidade do usuário ou consumidor, seja dos aspectos psicológicos e emocionais apresentados momentaneamente[21].

A predição de comportamentos hoje é baseada principalmente no método da psicometria preditiva de Kosinski, que, por sua vez, se inspirou no modelo do Big Five, cunhado por Lewis Goldberg em 1981. O Big Five, também chamado de Modelo dos Cinco Grande Fatores, se propõe a identificar cinco principais traços

17 THE ECONOMIST. **The new titans.** And how to tame them. 20 jan. 2018. Disponível em: <https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans>. Acesso em: 29 nov. 2020.

18 FRAZÃO, Op. Cit., 2019, p. 187.

19 FRAZÃO, A. **Proteção de dados pessoais e democracia**: a ameaça da manipulação informacional e digital. In: A Lei Geral de Proteção de Dados LGPD. Revista dos Tribunais, 2021, pp. 739-762.

20 BRUNO, F.G.; BENTES, A.C.F.; FALTAY, P. **Economia psíquica dos algoritmos e laboratório de plataforma: mercado, ciência e modulação do comportamento**. Revista FAMECOS, v. 26, n. 3, p. e33095, 27 dez. 2019.

21 [referência ao(s) autor(es) suprimida]

de personalidade por meio de hipótese lexical, empirismo, análise fatorial e universalidade[22].

Os cinco fatores trazidos por Goldberg são: abertura, consciencialidade, extroversão, neuroticismo e condescendência. Cada um desses fatores indicaria algum traço personalístico capaz de ser utilizado, a partir do modelo de psicometria de Kosinski, para prever comportamentos dos usuários de *big techs* a partir desse *profiling*, isto é, técnicas de perfilização[23].

O estudo de Kosinski demonstrou[24] que, quando combinadas várias características, em especial a extroversão, torna-se possível realizar previsões relativamente precisas em relação à personalidade de cada indivíduo. Analisando, portanto, as informações extraídas das redes sociais, seria possível perfilar esses usuários, dividindo-os automaticamente em diferentes segmentos e adaptando os anúncios a cada um deles, com base em sua personalidade[25].

Em outra pesquisa[26], Kosinski e sua equipe demonstraram que registros digitais de comportamento facilmente acessíveis, a exemplo dos likes no Facebook, podem ser utilizados para prever de forma automática e precisa uma variedade de atributos e informações pessoais altamente sensíveis, incluindo orientação sexual, etnia, religião, posicionamento político, traços de personalidade, felicidade, inteligência, idade e sexo[27].

Desse modo, a capacidade de detecção e algoritmização das expressões faciais por meio de *softwares* possibilitou às grandes plataformas e às *big techs* um enorme poder de influência e predição comportamental humana sobre seus usuários.

Porém o engajamento econômico corporativo não é o único almejado pelas grandes plataformas: o engajamento dos próprios usuários, no sentido de capturar sua atenção pelo máximo de tempo possível, se tornou um dos principais fatores de investimento no segundo tipo de matriz da economia psíquica dos algoritmos, a captológica[28].

---

22 [referência ao(s) autor(es) suprimida]

23 [referência ao(s) autor(es) suprimida]

24 BACHRACH, Y., et. al. **Personality and patterns of Facebook usage**. In Proceedings of the 4th annual ACM web science conference, pp. 24-32, 2012.

25 [referência ao(s) autor(es) suprimida]

26 GRAEPEL, T.; KOSINSKI, M.; STILLWELL, D. **Private traits and attributes are predictable from digital records of human behavior**. PNAS, Washington, DC, v. 110, n. 15, pp. 5802-5805, 2013.

27 [referência ao(s) autor(es) suprimida]

28 [referência ao(s) autor(es) suprimida]

Essa matriz tem como objetivo capturar, mobilizar e direcionar a atenção dos usuários das plataformas digitais, de modo que as tecnologias empregadas tenham efeito persuasivo diretamente sobre os consumidores[29].

Ademais, a captologia tem como fundamento a teoria de B.J. Fogg - fundador do Laboratório de Tecnologias Persuasivas em Stanford -, cuja ênfase se deu em pesquisas práticas e teóricas com fins de elucidar uma intersecção entre tecnologias computacionais e persuasão, visando efeitos planejados[30].

Desta feita, pode-se identificar uma aproximação da captologia com a Psicologia Behaviorista, afinal ambas analisam como manipular o comportamento humano de modo a obter padrões desejados, prevendo e controlando as ações. Shoshana Zuboff, inclusive, reconhece, em certa medida, que o capitalismo de vigilância cria uma arquitetura behaviorista[31] propícia à atuação veemente e em ampla escala das *big techs*.

Insta salientar ainda os estudos de Nir Eyal[32], no que concerne à ideia de captura e constância da atenção. A teoria de Eyal consiste basicamente em métodos e etapas de alto nível de resultado prático para empreendedores que almejam tornar seus produtos cada vez mais atraentes aos seus consumidores, a partir da criação do "modelo do gancho", que objetiva estimular a criação de hábitos de consumo[33].

O "modelo do gancho"[34] é dividido em quatro etapas: gatilhos - externos e internos -, ação, recompensas variáveis e investimento. Passemos à elucidação de cada uma delas.

A primeira etapa consiste nos chamados "gatilhos", que seriam estímulos que despertam algum comportamento desejado, comparativamente à teoria behaviorista, poderíamos compará-los com as condicionantes comportamentais. Os gatilhos se subdividem em externos e internos: os primeiros seriam quaisquer fenômenos que chamassem a atenção do usuário ou consumidor à ação - a exemplo de notificações chamativas, normalmente na cor vermelha, nos *smartphones* a fim de "fisgar" o indivíduo para os aplicativos -; e os últimos seriam emoções - em sua maioria ne-

29 [referência ao(s) autor(es) suprimida]

30 FOGG, B.J. **A Behavior Model for Persuasive Design**, Persuasive Technology Lab Stanford University, 2009.

31 ZUBOFF, S. Op. Cit., 2019.

32 EYAL, N.; HOOVER, R. **Hooked:** How to Build Habit-Forming Products, Ed. Portfólio, 2014.

33 [referência ao(s) autor(es) suprimida]

34 EYAL, N.; HOOVER, R. Op. Cit., pp.7-8.

gativas - que impulsionariam os usuários a retornar às redes, como o tédio, a tristeza e até mesmo a raiva[35].

A segunda etapa é denominada "ação", que consiste na análise do comportamento adotado pelos usuários diante dos gatilhos. A ação, para ser efetiva, deve ser fácil e acessível, a fim de que o agir venha como uma atitude automática, um hábito. Além disso, cabe ressaltar que esse hábito criado com fins econômicos favorece o monopólio das *big techs*, afinal essa otimização de tempo e tarefa - se tornando quase um costume, uma regra - dos usuários estimula-os a permanecer nas mesmas plataformas por mais tempo[36].

A terceira etapa do modelo do gancho para captura da atenção é chamada de "recompensas variáveis", que se assemelha muito aos experimentos behavioristas - especialmente aos realizados por B. F. Skinner, ao inserir variabilidade de recompensas por determinado comportamento[37]. Nessa etapa, portanto, parte-se do pressuposto de que a existência de grande variedade de recompensas aumentaria significativamente o comportamento desejado: a *timeline* das plataformas digitais tornaram-se, em certa medida, variáveis e imprevisíveis[38].

Por fim, Eyal sugere que a quarta e última etapa seria o "investimento" das empresas em mais mecanismos de captura da atenção, de maneira a perpetuar e aprimorar gradualmente a matriz captológica da economia da atenção[39].

Esse ciclo vicioso e eficiente - sob o prisma econômico - apresentado por Eyal representa um claro déficit na autodeterminação informativa dos indivíduos inseridos nesse sistema vigilante altamente manipulador[40] dominado por grandes plataformas digitais.

3 - A LEGISLAÇÃO EUROPEIA E BRASILEIRA: O CONSENTIMENTO DOS TITULARES DE DADOS PESSOAIS

A fim de elucidar como as práticas sub-reptícias de obtenção de dados mencionadas vão de encontro com as legislações brasileira e europeia, torna-se de suma

35 [referência ao(s) autor(es) suprimida]

36 [referência ao(s) autor(es) suprimida]

37 ZANATTA, R. A. F.; ABRAMOVAY, R. **Dados, vícios e concorrência:** repensando o jogo das economias digitais. Estudos Avançados, [S. l.], v. 33, n. 96, p. 421-446, 2019. DOI: 10.1590/s0103-4014.2019.3396.0021. Disponível em: https://www.revistas.usp.br/eav/article/view/161303. Acesso em: 22 jul. 2021.

38 [referência ao(s) autor(es) suprimida]

39 WU, T. Op. Cit., 2016.

40 [referência ao(s) autor(es) suprimida]

relevância entendermos como a questão do consentimento é tratada no Regulamento Geral de Proteção de Dados e na Lei Geral de Proteção de Dados. Isso porque, a partir do momento que forem identificadas as práticas consideradas lícitas relacionadas a essa base legal, será possível traçar um panorama dos abusos praticados pelas grandes plataformas e *big techs* aos seus usuários e consumidores.

No primeiro momento, será examinado o GDPR e suas nuances à respeito da base legal do consentimento, bem como serão mencionadas as *Guidelines* de nº 5 do *European Data Protection Board,* que originaram o entendimento a respeito do consentimento contido no regulamento, para, em seguida, realizarmos uma análise da legislação brasileira. Com isso, a partir de uma perspectiva comparada, será possível identificarmos as diferenças e semelhanças da posição adotada por cada legislação no que tange, especificamente, ao consentimento dos titulares de dados e, com isso, possibilitar um diagnóstico das ilicitudes das condutas das referidas empresas.

3.1 - O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU

Assim como a Diretiva 95/46 e o Regulamento 2016/679, as *Guidelines* de nº 5 do *European Data Protection Board,* de 4 de maio de 2020, estabelecem um ponto de partida para a análise da noção do consentimento no Regulamento Geral de Proteção de Dados da União Europeia, focando nas mudanças dessa concepção a partir do advento do Artigo 29 do *Working Party Opinion* 15/2011.

Segundo as *Guidelines*, passou a ser obrigação dos controladores de dados a descoberta de novas soluções de operação com observância de parâmetros legais a respeito da proteção de dados pessoais e do interesse dos seus fornecedores.

De acordo com o artigo 6 do GDPR, o consentimento é uma das seis bases legais para o tratamento de dados pessoais:

> Artigo 6. Licitude do tratamento
> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> **(a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas**;
> (b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> (c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> (d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

(e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
(f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.[41] - (grifo meu)

Ademais, o artigo 4 (11) do GDPR define o consentimento como "(...) uma **manifestação livre, específica, informada e explícita**, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[42] - grifos meus.

Desta feita, para que se entenda plenamente como o consentimento deve ser aplicado sob a ótica do GDPR, devemos analisar cada elemento que caracteriza sua validade: a necessidade de ele ser concedido livremente, de ser específico, de ser informado e de ser fornecido explicitamente por ato positivo claro e inequívoco.

---

41 "*Art. 6 GDPR - Lawfulness of processing*
Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) **the data subject has given consent to the processing of his or her personal data for one or more specific purposes;**
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." - Tradução livre: UNIÃO EUROPEIA, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Art. 6: Lawfulness of processing**, 2016a. Disponível em: <https://gdpr-info.eu/art-6-gdpr/>. Acesso em: 07 dez. 2020.

42 UNIÃO EUROPEIA, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Art. 4 (11): Definitions**, 2016b. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>, Acesso em: 07 dez. 2020.

3.1.1 – O CONSENTIMENTO LIVRE

O elemento da liberdade, no contexto da proteção de dados, implica a real possibilidade de escolha e de controle do titular sobre seus dados. Logo, se houver qualquer tipo de pressão ou coação para a concessão desse consentimento, sob pena de consequências negativas exageradas, o consentimento não será tido como lícito.

Além disso, é considerada uma relação de desequilíbrio entre o controlador e o titular de dados, principalmente quando esse controlador é uma autoridade pública, em um contexto laboral entre empregado e empregador ou em casos de fornecimentos de produtos e serviços por monopólios empresariais. Nesses casos, pode-se discutir a inadequação do consentimento como base legal a ser utilizada para fundamentar o tratamento de dados pessoais, tendo em conta essa assimetria de poder relacional.

Desse modo, para que o consentimento seja efetivamente livre, não pode estar vinculado a nenhum tipo de empacotamento (*bundling)* com aceitação de termos ou condições, nem a nenhuma amarração (*tying)* com previsões contratuais ou serviços que não sejam necessários para a plena eficácia contratual. Ou seja, as bases legais do consentimento e do contrato não podem, de maneira alguma, serem confundidas, pois isso limitaria a liberdade de escolha dos titulares de dados.

Logo, é necessária uma vinculação objetiva entre o processamento de dados e o propósito de execução do contrato. Um exemplo em que não há respeito a essa conexão de finalidade contratual seria a situação hipotética de um aplicativo de edição de foto requer, ao seu usuário ou à sua usuária, o acesso a sua geolocalização, sem dar a opção a esses usuários de não consentir com esse fornecimento de informação para usufruir de seu serviço. Considerando que a geolocalização não é um serviço necessário para a edição de fotos – finalidade a que o aplicativo se propõe –, torna-se ilícito o consentimento dado pelos usuários, a partir do momento em que se constata que o consentimento não foi fornecido livremente[43].

Outrossim, insta salientar que, quando um serviço envolve múltiplos processamentos de dados para mais de um fim, há a necessidade de que o titular e eventual fornecedor dos dados possa escolher quais dados ele permite serem processados, em vez de terem de consentir por todo um pacote de dados para diversos propósitos. O consentimento deve ser dado para cada um deles, devendo haver, portanto, granularidade.

---

43 UNIÃO EUROPEIA. **Guidelines 05/2020 on consent under Regulation 2016/679**, Adopted on 4 May 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt >, Acesso em: 7 dez. 2020.

Um caso que exemplifica claramente uma situação não granular de consentimento é a situação em que uma loja pede o consentimento dos seus clientes cadastrados para fornecer dados a fim de enviar-lhes, por e-mail, as ofertas do mês e , concomitantemente, para divulgar esses mesmos dados com outras lojas do mesmo grupo empresarial para finalidades de *marketing*. Considerando que, nessa situação, não houve separação de autorizações para cada finalidade, não houve granularidade no requerimento do consentimento.

Ademais, cabe destacar ainda que, para que o consentimento seja livre, há a necessidade de o controlador de dados demonstrar que o titular pode recusar ou retirar o consentimento sem detrimento algum, ou seja, sem nenhum custo ou desvantagem. Algumas situações que podem configurar detrimento são: intimidação, coerção ou qualquer outro tipo de consequência negativa para o titular e eventual fornecedor dos dados.

3.1.2 – O CONSENTIMENTO ESPECÍFICO

Além de livre, o consentimento válido deve ser específico e, para que isso ocorra, a noção de granularidade tem suma relevância novamente: o controlador deve separar informações a fim de determinar especificamente os propósitos para os quais pretende tratar aqueles dados.

Essa exigência de especificidade do uso dos dados coletados tem como objetivo evitar a ocorrência do fenômeno denominado de *function creep*, isto é, quando nossos dados são usados para um fim diferente daquele originalmente justificado. Isso faz com que os controladores que desejem obter consentimento de coleta de dados para vários diferentes propósitos devam proporcionar aos titulares opções *opt-in* separadas para cada um desses fins aos quais serão destinados esses dados.

Por fim, já que os controladores devem fornecer informações específicas sobre a finalidade do tratamento dos dados, isso já indica também para a necessidade de que o consentimento seja informado, como outro pressuposto de sua validade.

3.1.3 – O CONSENTIMENTO INFORMADO

Para que se configure o consentimento informado, o GDPR elenca, em seu artigo 20 o conjunto mínimo de informações necessárias a serem passadas ao fornecedor de dados, sendo elas[44]: i) a identidade do controlador; ii) o propósito de cada operação de processamento; iii) que tipo de dados serão coletados e usados;

44 UNIÃO EUROPEIA, Op. Cit., 2016a.

iv) a existência do direito de retirada do consentimento; v) informações relativas a decisões automatizadas; e vi) possíveis riscos concernentes à transferência de dados.

Portanto, pode-se constatar que o GDPR não prescreve a forma pela qual as informações mínimas devem ser veiculadas, de modo que a informação sobre o consentimento pode ser alcançada de diversas maneiras, como, por exemplo, por declarações escritas ou orais, por mensagens de vídeos ou por áudios.

Todavia, independentemente da forma veiculada, essa informação deve apresentar uma linguagem clara e compreensível para todas as pessoas. E, se por um acaso, esse controlador visa a obter consentimento de titulares que são responsáveis por crianças, pessoas analfabetas, ou portadoras de deficiências auditivas e/ou visuais, por exemplo, ele deve adequar a linguagem da informação veiculada para que seja compreensível para o respectivo público.

3.1.4 – O CONSENTIMENTO EXPLÍCITO POR ATO POSITIVO CLARO E INEQUÍVOCO

O consentimento ainda requer um ato positivo claro e inequívoco que não demonstre, de modo algum, ambiguidade. Isso significa que o fornecedor deve ter consentido por meio de uma ação afirmativa, que pode ter sido obtida por diversos meios - escritos, orais, inclusive eletrônicos.

Logo, o silêncio ou a mera falta de manifestação do titular de dados não podem ser considerados formas de obtenção do consentimento. Contudo, os controladores ainda têm a liberdade de obter o consentimento por meios alternativos, a exemplo de movimentos físicos dos titulares, desde que estes sejam qualificados como atos afirmativos.

Um possível exemplo de manifestação de consentimento por movimento físico é ilustrado na situação em que, em um aplicativo de *delivery*, como iFood e Uber Eats, para permitir o acesso à geolocalização, o usuário ou a usuária tenha que clicar o dedo sobre a tela do aparelho móvel para fornecer esse consentimento de maneira explícita.

Contudo, de maneira a obter o consentimento explícito propriamente dito, é necessária a configuração de situações em que há claro risco de falha na proteção de dados dos titulares. As *Guidelines* de nº 5 elencam duas hipóteses mais usuais: na transferência internacional de dados e na automatização de decisões, incluindo casos de *profiling*.

Logo, o termo "explícito" refere-se ao modo como o titular expressou seu consentimento: ele deve explicitá-lo normalmente por meio de uma declaração escrita para que seja evitada potencial dúvida futura quanto à validade daquele con-

sentimento. Porém, é fato que hoje temos outros meios de obtê-lo, a exemplo de preenchimento de formulário online, envio de e-mail, escaneamento de documento assinado ou assinando-o eletronicamente.

3.2 - A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

O consentimento na Lei Geral de Proteção de Dados Brasileira é interpretado de maneira semelhante ao do Regulamento Geral de Proteção de Dados Europeu, embora possua suas particularidades, a serem elucidadas nesta seção.

Em seu artigo 5º, inciso XII, a LGPD define o consentimento como uma "**manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[45]. Assim, o consentimento pode ser considerado, em certa medida, um processo de tomada de decisão do titular de dados.

Em adição, em seu artigo 7º, o consentimento é elencado como uma das dez bases legais para o tratamento de dados:

> CAPÍTULO II
> DO TRATAMENTO DE DADOS PESSOAIS
> Seção I
> Dos Requisitos para o Tratamento de Dados Pessoais
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular; (...)[46]

Ademais, a LGPD, em seu artigo 8º, estabelece que o consentimento deverá ser fornecido por escrito ou por qualquer outro meio que demonstre a manifestação de vontade do titular; e, caso seja fornecido por escrito, deverá constar de cláusula destacada das demais cláusulas contratuais.

A legislação brasileira, assim como a europeia, estabelece que cabe ao controlador de dados o ônus da prova de que o consentimento foi obtido dentro dos limites legais. Outra semelhança com o GDPR seria a de que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

---

45 BRASIL, **Lei nº 13.709, de 14 ago. 2018**, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 07 dez. 2020.

46 BRASIL, Op. Cit., 2018.

Outrossim, a LGPD declara vedado o tratamento de dados pessoais mediante **vício de consentimento**, além de considerar que o consentimento deve referir-se a finalidades determinadas, sendo tidas como nulas as autorizações genéricas para o tratamento de dados.

O artigo 9º da LGPD, ademais, enuncia o direito que o titular de dados tem ao **acesso facilitado** às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de **forma clara, adequada e ostensiva** para atendimento do princípio do livre acesso.

Dentre as informações sobre o tratamento dos dados, estão inclusas[47]: i) finalidade específica do tratamento; ii) forma e duração do tratamento, observados os segredos comercial e industrial; iii) identificação do controlador; iv) informações de contato do controlador; v) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; vi) responsabilidades dos agentes que realizarão o tratamento; e vii) direitos do titular, com menção explícita aos direitos contidos no art. 18 da LGPD.

Insta salientar ainda que, no §1º do art. 9º, é estabelecido que, caso as informações fornecidas ao titular, quando o consentimento for requerido, tenham conteúdo abusivo ou enganoso ou não tenham sido previamente apresentadas com transparência, de forma clara e inequívoca, o consentimento será considerado nulo.

No caso brasileiro, desta feita, cabe à Autoridade Nacional de Proteção de Dados (ANPD) garantir a autodeterminação informativa dos cidadãos, de modo a promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais. Além disso, a ANPD torna-se responsável por estimular a adoção de uma padronização de conduta por parte dos fornecedores de serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados e, consequentemente, faça haver a observância de um consentimento livre, informado, inequívoco e expresso - como bem preceitua a LGPD.

4 - CONSIDERAÇÕES FINAIS: PRÁTICAS ABUSIVAS PARA OBTENÇÃO DE CONSENTIMENTO INVÁLIDO DOS USUÁRIOS E CONSUMIDORES

A partir do momento que as grandes plataformas e as *big techs* se utilizam de técnicas manipulatórias que cerceiam a capacidade de decisão de seus usuários e consumidores, torna-se evidente a invalidade do consentimento para o tratamento de dados concedido por esses titulares às referidas empresas.

Isso porque, tendo em vista os pré-requisitos apresentados tanto pelo GDPR, quanto pela LGPD, relativos à validade do consentimento: manifestação livre, es-

47 BRASIL, Op. Cit., 2018.

pecífica, informada e explícita - nos termos da primeira legislação - e manifestação livre, informada e inequívoca - de acordo com a segunda -, pode-se constatar uma clara violação à autodeterminação informativa que capacitaria os titulares a consentir licitamente com relação ao tratamento de seus dados.

Cabe ressaltar que muitos usuários de aplicativos, sites e plataformas digitais nem ao menos leem os termos de política de privacidade e de uso dos respectivos controladores e, quando o fazem, acabam por não entender a linguagem técnica desses termos. "Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja não desfrutar de importantes produtos e serviços online. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais (...)"[48].

Além de os usuários e consumidores não poderem contar com a clareza dos contratos - um tanto quanto uma imposição unilateral como barganha para usufruto de produtos e serviços - não é garantida a devida transparência por parte dos controladores, na figura de grandes plataformas e *big techs*, de maneira a terem resguardados seus direitos e garantias como titulares de dados pessoais.

"Por isso, a disciplina do consentimento não deve ser tratada sob viés negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão."[49]. Logo, pode-se inferir que nada adianta uma base legal prevista em lei se não há de fato um livre fluxo informacional e uma real autonomia dos titulares de dados pessoais.

Portanto, há uma evidente vulnerabilidade dos titulares de dados pessoais face às grandes plataformas e *big techs,* visto seu poderio econômico, manipulativo - preditivo e captológico -, bem como sua capacidade de dominância de mercado e poder de algoritmização e extração de dados. Não há hoje uma proteção efetiva a vícios de consentimento, mas sim um estímulo a driblar a autodeterminação informativa dos consumidores, de modo que práticas sub-reptícias de coleta de dados tornam-se cada vez mais frequentes pelas grandes companhias de tecnologia.

Cabem às Autoridades Nacionais de Proteção de Dados e às agências reguladoras e comissões responsáveis pela defesa do consumidor - no Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) e a Secretaria Nacional do Consumidor (Senacon); e, na Europa, o *European Data Protection Board* e a *European Commission*

48 MENDES, L.S.; FONSECA; G.C.S. da. **Proteção de Dados Para Além do Consentimento**: Tendências de Materialização. In: BIONI, B.R.; et. al. (org.). Tratado de proteção de dados pessoais. São Paulo: Gen-Forense, 2020, p. 352.

49 TEPEDINO, G; FRAZÃO, A; OLIVA, M.D. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019, p. 48.

- zelarem pela observância e *enforcement* da coleta lícita do consentimento válido para o tratamento de dados dos titulares, no papel de usuários e consumidores de grandes plataformas e *big techs* dentro do contexto de um capitalismo de vigilância datificado.

REFERÊNCIAS BIBLIOGRÁFICAS

BACHRACH, Y., et. al. **Personality and patterns of Facebook usage.** In Proceedings of the 4th annual ACM web science conference, pp. 24-32, 2012.

BRASIL. **Lei nº 13.709, de 14 ago. 2018**, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 07 dez. 2020.

BRUNO, F.G.; BENTES, A.C.F.; FALTAY, P. **Economia psíquica dos algoritmos e laboratório de plataforma**: mercado, ciência e modulação do comportamento. Revista FAMECOS, v. 26, n. 3, p. e33095, 27 dez. 2019.

DONEDA, D. **O Direito Fundamental à Proteção de Dados Pessoais**. In: MARTINS, G.M.; LONGHI, J. V. R. (Orgs.). Direito Digital: Direito Privado e Internet. 2. Ed. São Paulo: Editora Foco, 2019, p. 35-54.

EYAL, N.; HOOVER, R. **Hooked:** How to Build Habit-Forming Products, Ed. Portfólio, 2014.

FRAZÃO, A. **Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência**. In: Empresa, Mercado e Tecnologia, 2019, p. 182.

_____, A. **Proteção de dados pessoais e democracia:** a ameaça da manipulação informacional e digital. In: A Lei Geral de Proteção de Dados LGPD. Revista dos Tribunais, 2021, pp. 739-762.

FOGG, B.J. **A Behavior Model for Persuasive Design**, Persuasive Technology Lab Stanford University, 2009.

GRAEPEL, T.; KOSINSKI, M.; STILLWELL, D. **Private traits and attributes are predictable from digital records of human behavior**. PNAS, Washington, DC, v. 110, n. 15, pp. 5802-5805, 2013.

HARARI, Y.N. **21 Lições para o Século 21**. São Paulo: Companhia das Letras, 2018.

MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor.** Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

_____, L.S.; FONSECA; G.C.S. da. **Proteção de Dados Para Além do Consentimento**: Tendências de Materialização. In: BIONI, B.R.; et. al. (org.). Tratado de proteção de dados pessoais. São Paulo: Gen-Forense, 2020.

[referência ao(s) autor(es) suprimida]

SIMON, H. **Designing organizations for an information-rich world**. In: GREENBERGER, M. Computers, communications and the public interest. Baltimore: The John Hopkins Press, 1917

TEPEDINO, G; FRAZÃO, A; OLIVA, M.D. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

THE ECONOMIST. **The new titans**. And how to tame them. 20 jan. 2018. Disponível em: <https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans>. Acesso em: 29 nov. 2020.

UNIÃO EUROPEIA. **Guidelines 05/2020 on consent under Regulation 2016/679**, Adopted on 4 May 2020. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt>, Acesso em: 7 dez. 2020.

UNIÃO EUROPEIA, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Art. 6: Lawfulness of processing**, 2016a. Disponível em: <https://gdpr-info.eu/art-6-gdpr/>. Acesso em: 07 dez. 2020.

UNIÃO EUROPEIA, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Art. 4 (11): Definitions**, 2016b. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>, Acesso em: 07 dez. 2020.

WU, T. **The attention merchants**: the epic scramble to get inside our heads, New York; Kopf, 2016.

ZANATTA, R. A. F.; ABRAMOVAY, R. **Dados, vícios e concorrência:** repensando o jogo das economias digitais. Estudos Avançados, [S. l.], v. 33, n. 96, p. 421-446, 2019. DOI: 10.1590/s0103-4014.2019.3396.0021. Disponível em: https://www.revistas.usp.br/eav/article/view/161303. Acesso em: 22 jul. 2021.

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

NOTA:

O presente trabalho foi realizado com o benefício financeiro do CNPq em projeto de iniciação científica (ProIC), sob orientação do Professor Doutor Othon de Azevedo Lopes; incentivo da mesma instituição em outro ProIC, sob orientação da Professora Doutora Ana Frazão; e apoio do Observatório da LGPD, grupo de pesquisa da Universidade de Brasília ministrado pela Professora Doutora Laura Schertel Mendes. Meus sinceros agradecimentos.