10

PORQUE NÃO HÁ MAIS ESCAPATÓRIA: A VIGÊNCIA DOS PRINCÍPIOS NORTEADORES DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E SUA APLICAÇÃO NAS RELAÇÕES DE CONSUMO, BEM COMO NO TRATAMENTO DESSES DADOS

Mario Filipe Cavalcanti de Souza Santos
Bacharel pela Faculdade de Direito do Recife (UFPE)
Advogado

RESUMO: O presente artigo visa demonstrar a vigência de todo arcabouço principiológico e normativo da privacidade e da proteção de dados pessoais dos consumidores no Brasil, e dos imperativos de tratamentos adequados desses dados, em razão do seu recepcionamento no ordenamento jurídico desde muito antes da promulgação da Lei Geral de Proteção de Dados Pessoais.

PALAVRAS-CHAVE: Proteção de dados. Consumidor. Violação de dados. Princípios do Direito. Privacidade. Tratamento de Dados.

INTRODUÇÃO: A QUESTÃO RELEVANTE

Quando exerci a capacidade postulatória para reclamar em juízo[1] a responsabilização de uma das maiores empresas da construção civil brasileira, pela violação dos dados pessoais e sensíveis de um consumidor, o sócio nominal de meu escritório, aquela era a primeira vez que alguém fazia isso no Brasil. Ainda perpassava o imaginário de muitos, dúvidas acerca da vigência da matéria abraçada pelo então novel diploma da Lei Geral de Proteção de Dados Pessoais (LGPD)[2], e muito se falava em quando se daria a sua vigência. Parecia haver uma contínua e ansiosa espera.

1 Ref.: 'Ação de Obrigação de Fazer c/c Indenização por danos morais c/c Tutela de Urgência Liminar em razão de Tratamento inadequado de dados – divulgação não autorizada', processo nº. 1080233-94.2019.8.26.0100, em trâmite na 13ª Vara Cível do Foro Central da Comarca de São Paulo, Tribunal de Justiça do Estado de São Paulo. Ação ajuizada em 16/08/2019, um ano após a promulgação da LGPD.

2 BRASIL, Lei Federal nº. 13.709/2018 'Lei Geral de Proteção de Dados Pessoais'. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

É que naquele momento, a LGPD apenas se avizinhava. Promulgada pelo presidente interino, Michel Temer, em 14 de agosto de 2018, e publicada no dia seguinte, a previsão original para a entrada em vigor era após 18 (dezoito) meses da data de sua publicação, portanto, fevereiro de 2020. O texto original, no entanto, previa a regulação e fiscalização das questões de privacidade no Brasil por uma "Autoridade Nacional de Proteção de Dados" (ANPD) que, no entanto, ainda não havia sido criada.

Com a aprovação da Medida Provisória nº. 869/2018[3], que tinha como objetivo estabelecer os regramentos para a criação da ANPD, a vigência da LGPD também restou alterada, dessa vez estipulada de forma bipartida: em 28 de dezembro de 2018 entrariam em vigor os ditames de criação da "Autoridade Nacional de Proteção de Dados", e após 24 (vinte e quatro) meses da data da sua publicação originária, os demais artigos.

Portanto, os Poderes Executivo e Legislativo federais pareciam intentar a prorrogação dos ditames legais da proteção dos dados e da privacidade, tendo em vista que com a nova determinação a lei em si entraria em vigor somente seis meses depois da primeira previsão: agosto de 2020 – portanto, dois anos após a sua originária promulgação.

Note-se que àquela época o *General Data Protection Regulation* (GDPR), regulamento geral de proteção de dados europeu, já estava em vigor e trazia ao mundo os exemplos dos ditames atualizados da privacidade e do respeito aos dados do consumidor como princípios norteadores das novas relações de consumo na era digital, no âmbito da União Europeia. E dizemos "ditames atualizados", porque já vigiam em países europeus atos regulatórios os mais variados sobre a proteção de dados pessoais dos cidadãos. O estado brasileiro, portanto, aderia ao movimento, mas tentava frear a sua efetiva vigência.

Todavia, enquanto os debates pareciam se avolumar sobre quando se daria a vigência efetiva da legislação de dados e o que as empresas deveriam fazer para se adequar àquele novo sistema, parecia haver uma omissão generalizada sobre a vigência efetiva das normas principiológicas que garantem ao consumidor no Brasil, a proteção de seus dados pessoais, o respeito à finalidade contratada no tratamento, e a autodeterminação informativa, assim como tantos outros princípios que a LGPD não trouxe originalmente, mas apenas balizou.

E no caso do sócio nominal de meu escritório, os danos, as perturbações da paz familiar e os assédios gerados diariamente a partir da violação de seus dados pela empresa a quem os confiou originalmente, como consumidor, nos dava um único imperativo e fazia erigir uma questão relevante, após inúmeras tentativas de resolução amigável da controvérsia: a judicialização da matéria.

3 Essa Medida Provisória foi promulgada como Lei Federal nº. 13.853/2019, pelo Congresso Nacional.

Como é sabido, *o direito não socorre aos que dormem*, e era preciso fazer algo imediatamente. E foi o que fizemos. Posteriormente, com o advento da Pandemia do SARS-Cov-2 (Covid-19), mais uma vez a vigência da LGPD restaria em pauta, por meio da Medida Provisória nº. 959/2020[4], que buscava postergar a *vacatio legis* até 03 de maio de 2021, com essa exposição de motivos[5]:

> Esta mesma Medida Provisória também propõe o adiamento da entrada em vigor dos dispositivos previstos na Lei Geral de Proteção de Dados em consequência de uma possível incapacidade de parcela da sociedade em razão dos impactos econômicos e sociais da crise provocada pela pandemia do Coronavírus.

Como pode ser visto, enquanto o Poder Executivo e parcela do Poder Legislativo, pareciam entender existir uma necessidade de adequação do empresariado brasileiro aos ditames da LGPD, adequação esta que teria de ser interrompida em razão dos impactos econômicos da pandemia, o próprio ordenamento jurídico brasileiro já possuía ditames que determinavam o respeito à privacidade, bem como à proteção de dados, sendo tais ditames imperiosos de aplicação pelo Poder Judiciário, tendo em vista a norma-princípio contida no art. 5º, inciso XXXV da Constituição da República, que determina o que se convencionou chamar "princípio da inafastabilidade da jurisdição"[6]:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito.

4 Até a última edição do presente artigo antes da publicação, essa Medida Provisória teve as seguintes tramitações relevantes: **1)** Em 07/08/2020 em seu Parecer, o relator na Câmara baixa pediu vigência imediata em 2020, sob o argumento da intensificação da imersão da sociedade no 'mundo digital' com a pandemia e a importância da garantia da proteção dos dados dos consumidores, **2)** em 25/08/2020, no entanto, o plenário da Câmara baixa decidiu pelo adiamento da vigência até 31/12/2020, **3)** remetida ao Senado, em 26/08/2020 os dispositivos de adiamento foram considerados prejudicados, tendo em vista a votação da matéria pelo Congresso ainda naquele exercício legislativo, quando se decidiu o PL nº. 1.179/2020 pela prorrogação unicamente das sanções administrativas da LGPD para agosto de 2021, tendo sido convertido na Lei nº. 14.010/2020, com isso, **4)** a MP foi devolvida ao Executivo para crivo de sanção ou veto sem o adiamento. Aguardava-se, portanto, o entendimento da Presidência da República para que fosse enfim definida a data da vigência da LGPD.

5 GUEDES, Paulo Roberto Nunes. Ministro de Estado da Economia. Medida Provisória nº. 959/2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf. Acesso em: 14/06/2020

6 Constituição da República Federativa do Brasil de 1988. Título II, Dos Direitos e das Garantias Fundamentais. Capítulo I, Dos Direitos e deveres individuais e coletivos. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14/06/2020

E nesse sentido, devemos dizer, o Poder Judiciário paulista entendeu perfeitamente a questão, e tanto o foi que determinou liminarmente a cessação da violação dos dados do consumidor autor da demanda, sob pena de multa. Tal decisão, de tão relevante, restou amplamente divulgada pela mídia jornalística especializada brasileira[7].

O presente artigo visa, portanto, explanar tais princípios normativos e normas legais constitucionais e infraconstitucionais a nível federal no Brasil, que já regulavam a necessidade de proteção aos dados pessoais dos consumidores, assim como o respeito à autodeterminação informativa e a uma série de princípios resumidos e balizados no bojo da LGPD. Portanto, visa demonstrar a nítida vigência de tais regramentos, de modo a não haver "escapatória", nem motivos para seus descumprimentos pelo empresariado que possui atividades no Brasil, que, em razão do tratamento desses dados, possui responsabilidade objetiva nos casos de sua violação.

1. DADOS: O NOVO INSUMO, MAS A QUEM PERTENCEM? CONSIDERAÇÕES SOBRE O *BIG DATA* E A EXPLORAÇÃO DOS NOVOS ARQUÉTIPOS DE CONSUMO

Aplicando o *Data Protection Act* de 1998, o *Information Commissioner's Office* (ICO), a autoridade independente do Reino Unido criada para a garantia dos direitos da informação e da privacidade, multou o Facebook Inc. em £500.000 (quinhentas mil libras esterlinas) em 2018, por não proteger as informações pessoais dos usuários.

Na investigação levada a cabo pelo ICO, constatou-se que de 2007 a 2014, o Facebook tratou os dados de seus usuários de modo inadequado, permitindo que os desenvolvedores de *Apps* acessassem tais informações, sem o consentimento expresso e informado dos usuários – estimou-se que os dados de cerca de 87 milhões de pessoas ao redor do mundo foram violados.

Sobre o assunto, assim se manifestou a Dra. Elizabeth Denham, Comissária da Informação do Reino Unido[8], que presidiu a investigação:

7 VALENTE, Fernanda. ***Juíza multa construtora por compartilhar dados pessoais de cliente***. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2019-ago-23/juiza-impoe-multa-cyrela-repassar-dados-pessoais-cliente; Portal Intelectual: ***Proteção de dados: Cyrela é processada por tratamento inadequado de dados de consumidores e sofre liminar***. Disponível em: https://www.portalintelectual.com.br/protecao-de-dados-cyrela-e-processada-por-tratamento-inadequado-de-dados-de-consumidor-e-sofre-liminar/;
ROSA, Arthur. ***Liminar evita uso de dados de consumidor***. ***Informações foram divulgadas a terceiros por empresa.*** Valor Econômico. Disponível em: https://valor.globo.com/legislacao/noticia/2019/09/29/liminar-evita-uso-de-dados-de consumidor.ghtml

8 DENHAM, Elizabeth. ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/

> *Facebook failed to sufficiently protect the privacy of its users before, during and after the unlawful processing of this data. A company of its size and expertise should have known better and it should have done better.*
>
> *We considered these contraventions to be so serious we imposed the maximum penalty under the previous legislation. The fine would inevitably have been significantly higher under the GDPR. One of our main motivations for taking enforcement action is to drive meaningful change in how organisations handle people's personal data.*

As palavras da Comissária da Informação do ICO são relevantíssimas para demonstrar os novos *checks and balances* extremamente necessários para a nova era digital em que vivemos.

Isso porque, malgrado as novas interfaces de interação das relações de consumo contemporâneas, os sistemas de garantias e de proteção ao consumidor prosseguem mais vivos do que nunca e existem porque, não esqueçamos, o consumidor prossegue sendo a parte mais fraca da relação. Tal fato, segundo o magistério de Kildare Gonçalves de Carvalho[9]:

> Leva à necessidade de coibir práticas ilícitas resultantes de um sistema econômico competitivo, que nem sempre respeita os valores éticos, causando variados danos ao consumidor, no que diz respeito à sua vida, privacidade e interesses econômicos ou a outros bens.

E esses danos são enormes e incontáveis, se levarmos em consideração o novo *modus operandi* de desenvolvimento de negócios no mundo atual, por intermédio da exploração do que se convencionou chamar *big data*.

Para Grassegger e Krogerus[10]:

> *Big data* significa, em essência, que tudo o que fazemos, tanto *online* como *offline*, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso celular está em nosso bolso, cada *link* é armazenado. Especialmente cada *like*. Durante muito tempo, não era inteiramente claro o uso que esses dados poderiam ter – exceto, talvez, que poderíamos encontrar anúncios de remédios para hipertensão logo após termos pesquisado no Google 're-

9 CARVALHO, Kildare Gonçalves. ***Direito Constitucional. Teoria do Estado e da Constituição. Direito Constitucional Positivo***. Belo Horizonte: Del Rey Editora, 2008, p. 728.

10 GRASSEGGER, Hannes; KROGERUS, Mikael. ***The data that turned the world upside down***. Motherboard, 2007, in MAGRANI, Eduardo. ***A internet das coisas***. Rio de Janeiro: FGV, 2018, p. 23.

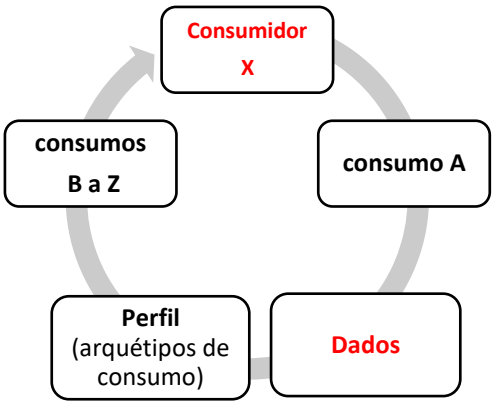
duzir a pressão arterial'.

Segundo o magistério de Shoshana Zuboff[11], professora da Harvard University, o *big data* não é uma "tecnologia" ou um "efeito tecnológico", como muitos querem nos fazer acreditar, mas é:

> Acima de tudo, o componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que chamo capitalismo de vigilância. Essa nova forma de capitalismo de informações procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado.

Como se pode perceber, o *big data* é a reunião de dados de indivíduos por diversas fontes, que possibilitam o desenvolvimento do *capitalismo de vigilância,* aqui nomeado pela professora de Harvard como os atos de comércio, de captação de dados e informações dos indivíduos para interpretá-los, geralmente por meio do uso de algoritmos, possibilitando a identificação de padrões e tendências comportamentais[12] que permitirão a acumulação de receitas por meio, justamente, do estímulo ao consumo.

Trata-se, portanto, de esquema que se retroalimenta, como no diagrama abaixo:



11 ZUBOFF, Shoshana. ***Big Other: surveillance capitalism and the prospects of an information civilization***. *Journal of Information Technology*, v. 30, 2015, p. 75-89 *in* BRUNO, Fernanda et al. (org.). ***Tecnopolíticas da Vigilância. Perspectivas da margem***. Tradução: Heloísa Cardoso Mourão. São Paulo: Boitempo Editorial, 2018.

12 CHRISTIAN, Brian; GRIFFITHS, Tom. ***Algoritmos para viver. A ciência exata das decisões humanas***. Tradução: Paulo Geiger. São Paulo: Companhia das Letras, 2017, p. 14.

> Veja-se que o diagrama ilustra, justamente, a capacidade de gerar novos consumos (Consumos B a Z) e, com isso, acumulação, através do tratamento dos dados de um consumidor X, dados esses conseguidos, não raras vezes e, verdade seja dita, na esmagadora maioria das vezes, a partir de uma compra avulsa (Consumo A), seja por intermédio de *cookies* (nas compras *online*), seja por intermédio do preenchimento de cadastros impostos como requisitos para a compra, portanto, sem qualquer intenção do consumidor no permissivo dessa cadeia de vigilância e controle.

Tais dados, tratados para essas finalidades, geram **perfis dos consumidores**, espécie de representações ideais de cada um, o que chamaríamos **arquétipos de consumo**, tendo em vista que, tal como na "alegoria da caverna", de Platão[13], a imagem que se faz do real é o que importa aos acorrentados, e não o real em si.

E essa imagem que se faz do real é, justamente, o perfil digital do consumidor, ou seja, o acúmulo de dados que informam terceiros acerca de aspectos pessoais e comportamentais privados de cada consumidor, como no dizer do regulamento europeu[14],

> nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Nesse caso, melhor não poderia ser o nome da mídia social desenvolvida por Mark Zuckerberg, afinal, trata-se, de fato, de um *facebook*, isto é, um repositório de perfis idealizados de cada pessoa, mas com alto grau de influência sobre elas, tanto no aspecto político – como nos mostrou o caso *Cambridge Analytica*[15] –, como do ponto de vista do consumo.

No aspecto político, resta cada vez mais claro que o escândalo da violação dos dados dos usuários do Facebook possibilitou a eleição de Donald Trump, um completo *outsider*, mal quisto pelos políticos tradicionais, ditos *insiders* e considerados "guardiães da democracia estadunidense"[16]. E tudo isso se deu, justamente, pelo tratamento inadequado dos dados dos usuários pelo Facebook, que permitiu

13 PLATÃO. ***A República***. 514-a/517-c. in MARCONDES, Danilo. ***Textos básicos de filosofia***. Dos Pré-Socráticos a Wittgenstein. 2ªed. Rio de Janeiro, Zahar, 2000.

14 PARLAMENTO EUROPEU. Jornal Oficial da União Europeia. 'Regulamento Geral de Proteção de Dados' da União Europeia. Tradução livre. Item 4, art. 4º Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=pt.

15 Para mais informações sobre esse caso recomendamos: The Guardian. ***The Cambridge Analytica Files***. Disponível em: https://www.theguardian.com/news/series/cambridge-analytica-files.

16 LEVITSKY, Steven; ZIBLATT, Daniel. ***Como as democracias morrem***. Tradução: Renato Aguiar. Rio de Janeiro: Zahar, 2020.

que terceiros, alheios ao conhecimento desses mesmos usuários e às finalidades da entrega desses dados, diante dos arquétipos criados a partir das informações coletadas desses usuários, direcionaram cada usuário às campanhas de ódio de Donald Trump, por meio da exploração do que se convencionou chamar *fake News*[17] e dos "pontos fracos" de cada usuário, como confessou o denunciante Christopher Wylie[18], analista de dados que trabalhou com a *Cambridge Analytica*, diretamente na manipulação dos usuários da rede social:

> *We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on.*

Frise-se o que diz Wylie: foram utilizados os dados de milhões de pessoas, a partir do Facebook, para explorar "o que se sabia dessas pessoas", direcionando os seus "demônios internos" para conseguir, por esse intermédio, o resultado esperado a partir disso. Portanto, para exercer controle sobre as pessoas.

Ressalte-se que o afã do controle da mentalidade da população não é algo novo, está incrustado no próprio nascimento das relações públicas[19]. Todavia, o que temos visto nos últimos tempos, é um avanço desse controle na era digital, por meio da utilização dos dados pessoais e sensíveis dos cidadãos, captados por *bots*, que, de posse de tais informações, promovem as marcas[20], estimulando o consumo, em detrimento da vontade autodeterminada dos consumidores.

Nesse condão, imperioso afirmar que no aspecto do consumo, portanto, a coisa não é tão diferente. No exemplo do Google, restou plenamente demonstrada a acumulação gerada pelo tratamento dos dados originados nos arquétipos de consumo, tendo em vista que o Google e outras plataformas, permitem o uso gratuito de seus serviços pelos usuários (consumidores), justamente como espécie de armadilhas, na qual esses últimos caem para se tornarem assediados constantemente pelas publicidades de terceiros (que pagam as contas do Google) que, de posse dos dados e informes de costumes e tendências de cada indivíduo, estabelecem as tendências do "capitalismo dadocêntrico"[21], criam "públicos" e geram a retroali-

17 MELLO, Patrícia Campos. ***A máquina do ódio. Notas de uma repórter sobre fake News e violência digital***. São Paulo: Companhia das Letras, 2020.

18 CADWALLADR, Carole; GRAHAM-HARRISON, Emma. ***Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach***. The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 16/06/2020.

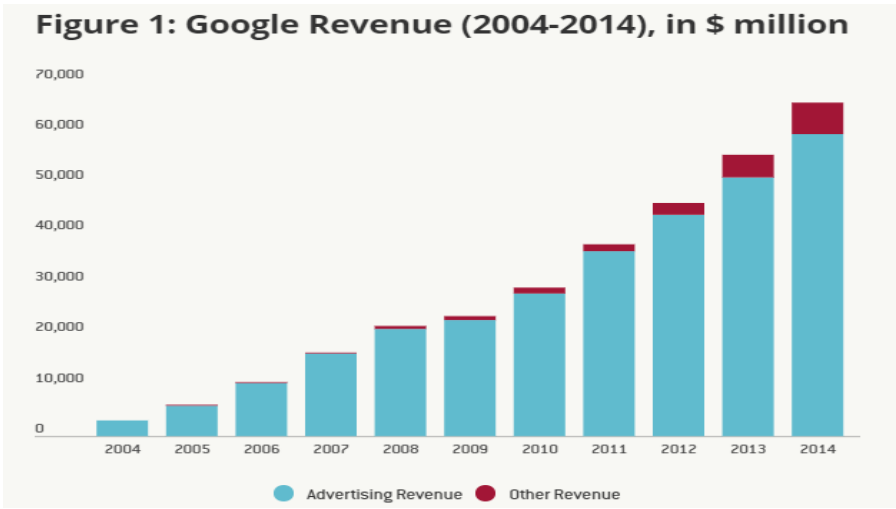
19 CHOMSKY, Noam. ***Mídia. Propaganda política e manipulação***. Tradução: Fernando Santos. São Paulo: Martins Fortes, 2017, pp. 22, 23.

20 PEREZ, Clotilde; TRINDADE, Eneus. ***Das Mediações Comunicacionais à mediação comunicacional numérica no consumo: uma tendência para a pesquisa***. São Paulo: Trabalho apresentado no IX Propesq PP – Encontro de Pesquisadores em Publicidade e Propaganda, 2018, p.09.

21 MOROZOV, Evgeny. ***Big Tech. A Ascensão dos dados e a morte da política***. Tradução: Claudio Marcondes. São Paulo: Ubu Editora, 2018, p. 33.

mentação do consumo – como no diagrama exposto algumas páginas acima.

Veja-se que de 2004 a 2014, portanto, no intervalo de apenas uma década, as publicidades direcionadas renderam ao Google mais de 90% de sua receita total em milhões de dólares americanos[22]:



O Facebook, de outro lado, somente em 2012 já valia US$75 bilhões de dólares americanos, 85% disso advindo diretamente de publicidade direcionada, portanto, do uso dos dados dos usuários para impulsionar vendas de terceiros[23]. Atualmente, US$ 82 bilhões de dólares é somente o patrimônio pessoal do CEO do Facebook, segundo a Forbes[24], chegando o valor total da rede, somente em 2019, a US$630 bilhões, independentemente do abalo na reputação da marca[25] com o escândalo no caso *Cambridge Analytica*.

Portanto, inegável que os dados dos consumidores valem muito e valem para outros, como no dizer de Morozov *"*a privacidade está se tornando uma mercadoria"[26].

22 Fonte 01: Bruegel. https://www.bruegel.org/2016/01/the-economic-value-of--personal-data-for-online-platforms-firms-and-consumers/#_ftnref6
Fonte 02: Google (2015), 'Financial tables' https://investor.google.com/financial/tables.html

23 DE LORI, Andrews. ***Facebook is using you***. Sunday Review. The New York Times. Disponível em: https://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html?_r=0. Acesso em 16/06/2020.

24 KLEBNIKOV, Sergei. ***Por que as ações do Facebook parecem indestrutíveis***. Forbes, 2020. Disponível em: https://forbes.com.br/negocios/2020/01/por-que-as-acoes-do-facebook-parecem-indestrutiveis/. Acesso em 16/06/2020.

25 The Harris Poll. 2019 Corporate Reputation Rankings. Disponível em: https://theharrispoll.com/axios-harrispoll-100/. Acesso em 17/06/2020.

26 MOROZOV, Evgeny. *Op. cit*, p. 36.

Vimos de forma resumida, portanto, que os dados se tornaram o novo insumo mercadológico que tem gerado acumulação e estímulo ao consumo, que, por sua vez, gera mais acumulações. Mas a quem pertencem, afinal de contas, os dados?

Primeiramente importante entender o que são.

O *Data Protection Act* de 1998, do Reino Unido, já fazia constar que dados pessoais são informações pessoais que identificam indivíduos vivos, que lhe dizem respeito e podem construir uma identificação deles, senão vejamos:

> *'personal data' means data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.*

Nessa mesma linha de raciocínio, o Regulamento Geral europeu, vigente desde 2018, assim definiu os 'dados pessoais' em seu art. 4º, item 1:

> Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Portanto, inequívoco que por "dados" devemos entender toda e qualquer informação capaz de individualizar uma pessoa humana, identificando-a ontologicamente, assim como em suas preferências relacionais e interacionais.

Nesse sentido, importante resgatar fala da Dra. Elizabeth Denham[27], acerca do pertencimento e, portanto, da titularidade dos dados, quando de seu comentário acerca do caso de violação de dados pessoais dos consumidores da British Airways, multada em £183.39 em setembro de 2018, já sob a égide do novo GDPR:

27 DENHAM, Elizabeth. ICO. ***Intention to fine British Airways £183.39M under GDPR for data breach***. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/

> *People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.*

Portanto, os dados são pessoais e pertencem aos usuários das plataformas, assim como aos consumidores dos bens e serviços liberados por meio de cadastros ou *links* de acesso – como ocorre na esmagadora maioria das compras via *e-commerce* com a utilização de *cookies* pelos *players* –, devendo esses mesmos consumidores ter ingerência sobre seus dados, decidindo conscientemente a sua destinação, inclusive do ponto de vista econômico.

O Dr. Jean Tirole[28], Prêmio Nobel de Economia, já alertava para esse problema:

> No futuro, o valor agregado residirá essencialmente no tratamento dos dados. Poderemos controlar o acesso aos nossos próprios dados, bem como sua confidencialidade, ou seremos prisioneiros de uma empresa, uma profissão ou um Estado guardando ciosamente o controle do acesso a esses dados?

E mais do que simplesmente apontar a problemática, Tirole nos traz ambos os lados que compõem a questão, porque se de um lado os dados por assim dizer pertencem aos consumidores, o tratamento desses dados e os sistemas de criação de perfis, algoritmos e *bots* para estabelecimento das tendências, seriam, certamente, propriedade intelectual das empresas.

Aliás, sobre a definição de "tratamento" de dados, assim dispõe o GDPR (texto que serviu de influência àquele descrito pela LGPD[29] brasileira):

> Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

28 TIROLE, Jean. ***Economia do bem comum***. Rio de Janeiro: Zahar, 2020, p. 422.

29 Texto do art. 5º, inciso X da LGPD brasileira: "*X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".*

Portanto, justamente como apontado pelo Dr. Tirole, tal operação e a definição dos regramentos de *inputs/outputs* dos algoritmos para o estabelecimento das tendências, é desenvolvimento tecnológico e, portanto, propriedade intelectual das empresas e, muitas vezes, interferem na qualidade dos dados captados. Como, pois, resolver o impasse?

O economista nos dá uma possibilidade de solubilidade, ao enfocar a forma de aquisição dos dados. Se a aquisição se deu através de altos investimentos das empresas, sem a participação direta dos consumidores, tais dados a elas pertenceriam. Se, todavia, os dados são colhidos diretamente dos consumidores, sem nenhum esforço, os dados seriam dos consumidores[30].

O caso das redes sociais, por exemplo, atende a esse último parâmetro, tendo em vista que o Facebook, seus braços (Instagram, WhatsApp, etc.), e outras redes sociais atuantes, não pesquisam os dados, mas apenas os recebem da própria pessoa deles titular. O usuário, no entanto, cede seus dados para poder participar de uma rede virtual de amizade, quando, em realidade, está possibilitando, sem saber, a criação de arquétipos de consumo de si mesmo, e, com isso, um tratamento para muito além da finalidade originalmente intentada.

Na mesma esteira se encontram os casos em que o consumidor procede a uma compra avulsa mediante preenchimento de seus dados pessoais ou a uma compra *online*, na qual seus dados ficam registrados como verdadeiras "pegadas digitais"[31] disponíveis ao provedor da *internet*, à eventual operadora de serviço (de *desktop* ou *smartphone*), aos *websites* e mesmo às plataformas de busca.

Na prática, vemos o mesmo diálogo dos conquistadores portugueses com os nativos do novo continente no século XV. Isso porque, em troca de miçangas e espelhos, os europeus ganharam informações que permitiram a dominação das terras e a subjugação dos povos ameríndios. No nosso paralelo contemporâneo, em troca de acesso a plataformas e de participação em mídias sociais, os consumidores concedem informações e dados que os tornarão reféns de controle e, frise-se, sem o saber.

Nesse sentido, útil dizer que, quando estabelecemos acima uma distinção clara entre o que se entende por "dados" e o que se entende por "tratamento de dados", o fizemos porque essa distinção, se se operasse com rigidez na realidade, poderia facilitar os processos de compreensão e freios éticos das condutas. Nessa esteira, leciona o Dr. Tirole[32]:

30 TIROLE, Jean. *Op. cit.*, pp. 422/423.

31 SUMPTER, David. ***Dominados pelos números. Do Facebook e Google às Fake News. Os algoritmos que controlam nossa vida***. Tradução: Ana Maria Sotero, Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 57

32 *Idem. ibidem*, p. 423.

> Se existisse uma separação nítida entre dados fornecidos pelo cliente e o tratamento desses dados, a política a seguir seria mais simples: os dados deveriam pertencer ao cliente e serem ao portador, isto é, intransferíveis a terceiros se o cliente assim desejasse.

Na realidade, as coisas já devem ser encaradas dessa forma. Porque o princípio da finalidade determina já há muito, que os dados sejam utilizados pelo controlador, dentro dos parâmetros contratados, portanto, para as finalidades contratadas. O conhecimento do tipo de tratamento e processamento dos dados, é, portanto, imprescindível ao consumidor.

Portanto, os regramentos que estabeleceram os princípios legais da proteção dos dados são de grande imperiosidade, porque ampliam o sistema de proteção ao consumidor, dando a este o direito de determinar os limites à fruição desses dados, limites esses que não podem ser engessados por contratos de adesão ou em meros "Termos de uso", onde o consumidor não possui verdadeira autonomia decisória.

Isso porque, já se passaram os tempos em que o *pacta sunt servanda* valia mais do que a função social que todo e qualquer contrato precisa desempenhar na nova era, como aliás, determina o art. 421 do Código Civil Brasileiro[33] e como lecionam Humberto Theodoro Jr.[34] e Arnaldo Rizzardo[35], respectivamente:

> A função social do contrato consiste em abordar a liberdade contratual em seus reflexos sobre a sociedade (terceiros) e não apenas no campo das relações entre as partes que o estipulam (contratantes). Quando o art. 421 do novo Código brasileiro fala em função social para o contrato está justamente cogitando dos seus efeitos externos, isto é, daqueles que podem repercutir na esfera de terceiros.

> A função social do contrato exprime a necessária harmonização dos interesses privativos dos contraentes com os interesses de toda a coletividade; entre outras palavras, a compatibilização do princípio da liberdade com a igualdade, vez que para o liberal o fim principal é a expansão da personalidade individual e, para o igualitário, o fim principal é o desenvolvimento da comunidade em seu conjunto, mesmo que ao custo de diminuir a esfera de liberdade dos singulares.

33 BRASIL. Lei Federal nº. 10.406/2002 'Código Civil Brasileiro'. "Art. 421. *A liberdade contratual será exercida nos limites da função social do contrato*". Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

34 THEODORO JR., Humberto. ***O contrato e sua função social***. 2ª ed. Rio de Janeiro: Forense, 2004, pp. 35 e 41.

35 RIZZARDO, Arnaldo. ***Contratos***. 5ª ed. Rio de Janeiro: Forense, 2005, p. 20.

Ao contrário do percebido por muitos, os direitos de proteção de dados e privacidade não entrarão em vigor no Brasil em 03 de maio de 2021 – ou na eventual nova data, caso haja mais um prolongamento da *vacatio legis* da lei geral de dados –, mas já vigoram por meio de outros dispositivos legais que, interconectados dada a aplicação sistêmica do ordenamento, já garantem aos consumidores proteção diante dos ditames da era digital, conforme abaixo se verá.

2. A MAGNA CONSTITUIÇÃO DA REPÚBLICA BRASILEIRA E O DIÁLOGO COM A CARTA DA ONU E COM A CONVENÇÃO AMERICANA DE DIREITOS HUMANOS – ESTABELECENDO OS PRECEDENTES

Há mais de setenta anos foram lançados as bases e os precedentes do novo espírito colaborativo que anunciava o desejo de construção de um mundo mais comunitário e pacífico, restando, à época, constituído um documento jurídico-político que encerraria com maestria esse espírito: a Declaração Universal dos Direitos Humanos (DUDH)[36].

É da DUDH que vem, pois, o gérmen do reconhecimento da relevância do direito à privacidade, como direito humano e fundamental, no âmbito da contemporaneidade e como um bem *erga omnes*[37], e é a partir daí que há uma verdadeira guinada no panorama dialético do entendimento da privacidade, que havia sido anteriormente esmagado pelos regimes totalitários do século XX. Eis as disposições:

> Art. III. Todo ser humano tem direito à vida, à liberdade e à segurança pessoal.
>
> Art. XII. ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio e na sua correspondência, nem ataques à sua honra e à sua reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.
>
> Art. XVII. 1. Todo ser humano tem direito à propriedade, só ou em sociedade com outros. 2. Ninguém será arbitrariamente privado de sua propriedade.

36 ONU. DUDH. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf

37 CAVALCANTI DE SOUZA SANTOS, Mario Filipe. A generalização do direito à privacidade na dialética do escorço histórico. **Revista da Associação Paulista da Propriedade Intelectual**. São Paulo, n. 07, p. 38-43, mai./ago. 2020.

Vê-se, portanto, que o direito à privacidade, à propriedade e à segurança pessoal, correlatos entre si e inegavelmente conectados à lógica da necessária proteção dos dados pessoais, são elevados ao patamar de direitos supranacionais e de garantias fundamentais exigíveis por qualquer ser humano, tendo em vista que interconectados com o que veio a se chamar de "princípio da dignidade da pessoa humana". Como lembraram Eduardo Bittar e Guilherme Almeida[38]:

> A Declaração de 1948 foi a forma jurídica encontrada pela comunidade internacional de eleger os direitos essenciais para a preservação da dignidade do ser humano. Trata-se de um libelo contra o totalitarismo. Seus 30 artigos têm como objetivo principal evitar que o homem e a mulher sejam tratados como objetos descartáveis.

Na mesma esteira da DUDH, é inegável precedente à proteção de dados no Brasil, o texto da Convenção Americana de Direitos Humanos (CADH), estabelecida em 1969 e amplamente conhecida como "Pacto de San José da Costa Rica", promulgada pelo Decreto nº. 678/1992[39], que dispõe em seu art. 11:

> Artigo 11 - Proteção da honra e da dignidade
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Vê-se que o espírito da norma interamericana é o mesmo daquele expresso desde 1948 na norma da ONU: **garantir o direito à privacidade** e à propriedade como intrínsecos à condição de ser humano.

E é nesse espeque clarividente que a Constituição da República Federativa do Brasil de 1988, se baseou ao eleger como princípio fundamental do próprio Estado Democrático de Direito, a dignidade da pessoa humana e como cláusula pétrea, portanto, imutável, dos direitos e garantias fundamentais individuais e coletivos, o **respeito à privacidade, ao sigilo dos dados e à autodeterminação do indivíduo**, senão vejamos:

38 BITTAR, Eduardo C. B.; ALMEIDA, Guilherme Assis de. ***Curso de Filosofia do Direito***. São Paulo: Atlas, 2001

39 BRASIL, Convenção Americana de Direitos Humanos. Decreto nº. 678/1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> III - a dignidade da pessoa humana.
>
> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal
>
> LXXII - conceder-se-á habeas data:
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Inviolável, pois, a dignidade da pessoa humana e todos os aspectos dela decorrentes, como o direito à vida privada, à intimidade e ao sigilo dos dados – além de, em última hipótese, as comunicações de dados, portanto, a vontade do indivíduo humano sobre a transmissão de suas informações pessoais.

Segundo o magistério de José Afonso da Silva[40], quando estabelece o direito à intimidade:

> A Constituição está reconhecendo que o homem tem direito fundamental a um lugar em que, só ou com sua família, gozará de uma esfera jurídica privada e íntima, que terá que ser respeitada como sagrada manifestação da pessoa humana.

40 SILVA, José Afonso da. ***Curso de direito constitucional positivo***. 40ª. ed. São Paulo: Malheiros, 2017, p. 209.

Vê-se, portanto, que embora a Carta Política brasileira reconheça no ambiente doméstico a guarita inconteste da intimidade, os novos tempos e o desenvolvimento do fenômeno da *internet* das coisas (*IOT*, na sigla em inglês) têm estendido a captação de dados e o mercado de vigilância, até mesmo a esse ambiente, como alertou Morozov[41]:

> O modelo do capitalismo 'dadocêntrico' adotado pelo Vale do Silício busca converter todos os aspectos da existência cotidiana em ativo rentável: tudo aquilo que costumava ser o nosso refúgio contra os caprichos do trabalho e as ansiedades do mercado.

Por isso que, segundo a visão do Ministro do Supremo Tribunal Federal Alexandre de Moraes[42], a determinação constitucional da inviolabilidade do sigilo de dados deve ser entendida como complementar à previsão ao direito da intimidade e da vida privada, tendo em vista que:

> A defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional.

De outro lado, inconteste também que o enaltecimento do *habeas data* como norma constitucional, demonstra a guarida na Lei Maior do Brasil, do **princípio da autodeterminação informativa**, portanto, o direito do indivíduo ter conhecimento sobre o que é feito com seus dados, de requerer a correção dessas informações e, o que posterior veio a se entender: a exclusão desses dados de eventuais bases que violam a sua finalidade, vez que, como lecionou Catarina Sarmento e Castro, professora da Faculdade de Direito de Coimbra[43]: "o direito à autodeterminação informativa nasce, assim, para garantir um direito à intimidade privada no que aos tratamentos de dados pessoais diz respeito".

41 Idem, ib idem, p. 33.
42 MORAES, Alexandre de. ***Direito constitucional***. 32. ed. São Paulo: Atlas, 2016, p. 74.
43 CASTRO, Catarina Teresa Rola Sarmento e. ***Direito da informática, privacidade e dados pessoais*****.** Coimbra: Almedina, 2005, p. 339.

Vê-se, portanto, que as normas internacionais consubstanciadas na Declaração Universal dos Direitos Humanos (DUDH) e na Convenção Americana de Direitos Humanos (CADH), inspiraram a Constituição da República brasileira, de 1988. E esta, por sua vez, elencou os direitos à privacidade, neles o da proteção/sigilo de dados, como garantias fundamentais dos indivíduos, o que, por óbvio, se estende às relações de consumo.

3. O CÓDIGO DE DEFESA DO CONSUMIDOR COMO MICROSSISTEMA DE PROTEÇÃO

No Brasil, após grande demanda da sociedade civil, instituiu-se na última década do século XX, a Lei Federal nº. 8.078/1990, que disporia sobre a proteção ao consumidor, o famoso Código de Defesa do Consumidor (CDC), dispositivo legal que estabelece um microssistema de proteção ao indivíduo humano em sua relação de consumo, dada a desigualdade existente entre as empresas, o mercado competitivo e os indivíduos, esses últimos, ocupando a ponta extrema e frágil da corda.

Visa, portanto, o CDC, tutelar a relação de consumo e, nesse desiderato, impõe ao fornecedor a necessidade de prestar serviços e fornecer produtos sem falhas ou vícios, sob pena de responsabilização civil.

Assim que, havendo defeitos relativos à prestação de serviço ou insuficiência nas informações prestadas ao consumidor, são responsáveis legalmente os fornecedores, e de forma objetiva, conforme disciplina estampada no art. 14, *caput* do CDC[44], que determina:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Indo ainda mais longe, numa redação legislativa exemplar, o CDC expõe no parágrafo primeiro do art. 14, que o "serviço defeituoso" é aquele que não fornece ao consumidor a segurança que dele poderia esperar, senão vejamos:

> Art. 14. (...)
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as cir-

44 BRASIL, Código de Defesa do Consumidor. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

> cunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido.

Ora, entendemos que tal disposição do Código de Defesa do Consumidor tutela eficientemente os casos de violação de dados.

Isso porque, inegável que quando os dados dos consumidores são coletados mediante a aquisição de um bem ou a prestação de um serviço, é evidente que tais dados devem ser utilizados tão somente para essa finalidade. Deveria, portanto, o empresário inferir que, embora os dados sejam o novo insumo de mercado, se a intenção é a sua utilização para quaisquer finalidades que lhe garanta retorno financeiro, para além dos limites contratados, todos os consumidores titulares desses dados deveriam ser reconhecidos como seus acionistas, a quem deveria esse mesmo empresário remeter a parte que lhes coubesse.

Há quebra de confiança, portanto, e defeito na prestação do serviço, ainda que se fale em obrigação acessória, quando ocorre a desvirtuação da finalidade contratada, portanto, quando esses dados são utilizados para outras finalidades, inclusive por terceiros – no caso do Facebook/*Cambridge Analytica*, para criar arquétipos de vigilância e controle das opiniões políticas (dados sensíveis) e no caso de meu cliente, a utilização de seus dados (pessoais e sensíveis), por terceiros, estranhos à sua relação de consumo, para oferecer-lhe bens e serviços não solicitados.

Nesse sentido, é pacífica a jurisprudência brasileira no sentido de que o fornecedor que presta serviços eivados de falhas e vícios tem o dever de indenizar o consumidor, além de reparar tais falhas, como nos precedentes abaixo, dos Tribunais de Justiça dos Estados de São Paulo[45] e do Rio Grande do Sul[46], vejamos:

> RECURSO – Apelação – 'Ação de indenização por danos materiais e morais' – Insurgência contra a r. sentença que julgou parcialmente procedente a demanda – Inadmissibilidade – Incontroversa existência de relação jurídica entre as partes – Evidenciada existência de fraude na realização de transações bancárias, em elevados valores, através do sistema de 'internet banking' – Banco apelante que responde não só pela segurança das ferramentas disponibilizadas em ambiente virtual, bem como pelo sigilo das informações pessoais de seus clientes – Apelante que não se desincumbiu de seu ônus proba-

45 TJ-SP - AC: 10009777320178260197 SP 1000977-73.2017.8.26.0197, Relator: Roque Antonio Mesquita de Oliveira, 18ª Câmara de Direito Privado, Data de Publicação: 14/03/2019.

46 TJ-RS - AC: 70054358205 RS, Relator: Paulo Roberto Lessa Franz, Décima Câmara Cível, Data de Publicação: Diário da Justiça do dia 18/07/2013.

> tório, previsto no artigo 373, inciso II, do CPC/2015 – Transações ilegítimas – Casa bancária que responde objetivamente por danos relativos a fraude, nos termos da Súmula 479 do STJ – Valores indevidamente debitados da conta corrente da apelada, que devem ser integralmente restituídos – Sentença mantida – Honorários advocatícios bem fixados e majorados – Recurso improvido.
>
> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE REPARAÇÃO POR DANOS MATERIAIS E MORAIS. FALHA NA PRESTAÇÃO DO SERVIÇO. WEB HOSTING. FALHA NA PRESTAÇÃO DE SERVIÇO. CONFIGURAÇÃO. Hipótese em que o conjunto probatório dos autos conforta a versão do autor, apontando para a ocorrência de falha na prestação de serviços prestados pela ré. Sentença mantida. (...) DANO MORAL. CONFIGURAÇÃO. Caso concreto em que a empresa autora teve sua imagem abalada, em razão da falha na prestação de serviço realizado pela ré, causando lesão à sua reputação e imagem. Caracterizado o dano moral puro, exsurgindo, daí, o dever de indenizar. Sentença mantida. QUANTUM INDENIZATÓRIO. MANUTENÇÃO. (...) Sentença mantida. APELAÇÃO DESPROVIDA.

Veja-se que o CDC garante a inversão do ônus da prova, de modo que prescinde que o consumidor identifique a gênese da violação de seus dados, bastando que apresente suficiente indício de que eles foram violados, isto é, que foram entregues para determinado tratamento específico e que estão sendo utilizados por terceiros, estranhos à relação original, com fortes indícios de receptação a partir daquela relação original[47].

Cabe, portanto, ao fornecedor do bem ou serviço comprovar que os dados não foram violados, tendo em vista que o fornecedor responde independente se teve dolo ou culpa na violação dos dados.

Tal disciplina (da inversão do ônus da prova) encontra-se expressamente encartada como "direito básico do consumidor" no art. 6º, VIII do CDC, senão vejamos:

47 É justamente nesse sentido que se dá o caso Fabrício Vilela Coelho *vs* Cyrela Brazil Realty, por mim patrocinado, referenciado na primeira nota do presente artigo: após a aquisição de um imóvel no empreendimento "Thera Ibirapuera", da empresa citada, o consumidor (e também advogado) Fabrício, passou a ser assediado por terceiros em todos os meios possíveis e imagináveis, de forma extremamente insistente, sem limites de horários ou de qualquer convenção social, e em todos esses contatos, os terceiros citavam o empreendimento da Cyrela e o fato do consumidor ter adquirido imóvel nele. Como eles sabiam disso? Como podiam ofertar ao consumidor móveis personalizados no exato formato do imóvel adquirido? Como podiam oferecer financiamentos que se adequavam perfeitamente às informações financeiras de meu cliente? Era, pois, o típico caso de *data breach.* A sensação do consumidor diante do fato de seus dados pessoais e sensíveis terem sido violados e repassados a terceiros é de frustração o dano moral excede a própria perturbação da paz em si, causada pelos contatos reiterados.

> Art. 6º São direitos básicos do consumidor:
> VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

Note-se que esse regramento é pacífico na jurisprudência brasileira[48]:

> PROCESSO CIVIL - CDC - INVERSÃO DO ÔNUS DA PROVA - REQUISITOS. Nos termos do art. 6º, inciso VIII, do CDC, é direito do consumidor hipossuficiente, no processo civil, a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor.

Frise-se, ainda, que, como determinado pelo próprio CDC, em seu art. 47, as cláusulas dos contratos avençados com os consumidores no caso de entrega de dados (inclusive eventuais "Termos de uso"), devem ser interpretadas do ponto de vista mais favorável ao consumidor.

Portanto, inegável que o Código de Defesa do Consumidor, dá prosseguimento à onda de proteção, cujos precedentes foram delineados pela própria Carta política.

4. A PRIMAVERA DOS REGULAMENTOS ESPECÍFICOS DA PROTEÇÃO DE DADOS NO BRASIL: A LEI DO CADASTRO POSITIVO

Em 09 de junho de 2011, restou promulgada pela presidente da República Dilma Vana Rousseff, a Lei Federal nº. 12.414/2011[49], intitulada Lei do Cadastro Positivo (LCP) que disciplina a formação e consulta aos bancos de dados com informações de adimplementos de obrigações financeiras pelas pessoas, naturais ou jurídicas, no Brasil.

A legislação, que atendia à demanda de setores do mercado que intentavam estimular o adimplemento por meio de um *score* originado de um histórico de crédito do consumidor, se mostrou bem mais do que isso, permitindo que, a partir das bases lançadas, se iniciasse o que chamaremos "primavera dos regulamentos específicos da proteção de dados no Brasil".

48 TJ-MG, 2.0000.00.420630-2/000(1), Relator: GUILHERME LUCIANO BAETA NUNES, Data de Publicação: 10/03/2004

49 BRASIL, Lei Federal nº. 12.411/2011 'Lei do Cadastro Positivo'. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

Isso porque, no intento de criar uma alternativa paralela ao já conhecido "cadastro negativo" ou "cadastro de restrição de crédito" gerado para desestimular o inadimplemento das obrigações, o "cadastro positivo", ou "*bureau* positivo", tem como objetivo compartilhar com instituições interessadas em empreender análise de crédito (para atender demanda do consumidor), dados que permitam a construção de um novo arquétipo de consumo, o perfil de "bom pagador", em outras palavras, seu histórico de adimplemento de obrigações, conforme argumenta o Sistema de Proteção ao Crédito no Brasil (SPC)[50]:

> O Cadastro Positivo reúne, de forma segura, as informações de pagamentos que você já fez ou está fazendo. Esses dados ficam guardados num histórico que leva em conta não apenas o momento atual, mas toda a sua vida financeira recente. Conforme você paga suas contas, seu comportamento de pagamento é registrado em seu histórico. Assim, as empresas poderão analisar seu perfil como um todo, e não apenas se seu nome está negativo ou não.
> Desta forma, você poderá ter acesso a menos juros e menos burocracia na hora de solicitar crédito.

Como pode ser visto, trata-se de cadastro de dados relativos aos pagamentos realizados pelo consumidor, de modo a permitir maior garantia aos empresários, quanto à tendência de adimplemento, e em troca, promete dar aos consumidores maior facilidade de acesso ao crédito – sistema que possui lógica que se retroalimenta, portanto.

Note-se, contudo, que tal sistema é absolutamente voluntário – não podendo ser imposto pelas empresas aos consumidores – e, jamais permite a divulgação ostensiva desses dados pessoais a terceiros, para finalidades não previstas, conforme ditames da própria Lei do Cadastro Positivo.

Tão firme é o entendimento da legislação no sentido da **exclusividade de tratamento dos dados no atendimento da finalidade do cadastro**, que tal dicção está estampada já do primeiro artigo, sendo revisitada pelos arts. 3º e 7º da lei, senão vejamos:

> Art. 1º Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei nº 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor.
> Art. 3º Os bancos de dados poderão conter informações de adimple-

50 Sistema de Proteção ao Crédito (SPC). Cadastro Positivo Consumidor. Disponível em: https://www.spcbrasil.org.br/cadastropositivo/consumidor/index.html#oquee. Acesso em 16/06/2020

> mento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> Art. 7º As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:
> I - realização de análise de risco de crédito do cadastrado
> II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Portanto, a finalidade do cadastramento dos dados do consumidor no referido "*bureau* positivo" é única e exclusivamente a de atestar a confiabilidade do consumidor no que tange ao adimplemento de suas obrigações, e o acesso é dado a instituições com intuito de consultar esse histórico de crédito, para subsidiar decisão de conceder ou não crédito/financiamento ao consumidor.

Vê-se, pois, a preocupação do texto legal com a especificação da finalidade do tratamento dos dados, bem como com o engessamento de seu tratamento, no esteio da atividade contratada. Temos aqui, então, uma nítida limitação às atividades do controlador dos dados e lançados os regramentos que podem ser estendidos para todo e qualquer caso de tratamento de dados de consumidor no Brasil: **a vigência e efetivação do princípio da finalidade**.

E tanto é assim que a legislação, em seu art. 5º, inciso V, determina que é direito do cadastrado, portanto, do consumidor, ser informado previamente sobre a finalidade do tratamento dos dados, assim como dos destinatários de tais dados em caso de compartilhamento, senão vejamos:

> Art. 5º São direitos do cadastrado:
> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento.

Na mesma toada, o inciso VII do mesmo artigo erige como direito do cadastrado, portanto, do consumidor, que seus dados pessoais somente sejam utilizados com a finalidade para a qual foram coletados, senão vejamos:

> Art. 5o São direitos do cadastrado:
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

Vê-se, portanto, a enorme relevância do diploma legal da LCP no Brasil,

para vias de implementar, já nos idos de 2011, os regramentos principiológicos do princípio da finalidade do tratamento dos dados e do respeito ao interesse expresso do consumidor.

E veja-se que o Superior Tribunal de Justiça[51], interpretando a LCP, deixou cristalino outro princípio que seria balizado futuramente pela LGPD brasileira, o **princípio da autodeterminação informativa**. Tendo em vista que aquela Corte de Justiça infraconstitucional entende que é nula de pleno Direito a cláusula que obriga o consumidor a anuir à transferência de seus dados, do fornecedor de serviço originalmente contratado para o cadastro positivo, portanto, para o compartilhamento com outras instituições financeiras, senão vejamos:

> RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. (...)
> 3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.
> 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança.
> 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada.
> 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição.
> 7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.
> 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez

51 STJ, REsp 1.348.532 – SP, Rel. Min. Luís Felipe Salomão, 4ªT, Dj: 10/10/2017

> que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44).
>
> 11. Recurso especial parcialmente provido.

O entendimento acima, esposado pelo STJ, demonstra, portanto, que a validade do tratamento dos dados do consumidor para a criação de um *score* em seu nome somente ocorre **quando o consumidor expressa sua vontade** de anuí-lo **de forma consciente**, não podendo ser obrigado por contratos de adesão ou por "Termos de uso", por exemplo.

Antes mesmo da afirmação do precedente acima, os Tribunais de Justiça dos Estados já julgavam matérias nesse sentido, como podemos ver na jurisprudência do Tribunal de Justiça do Estado do Paraná[52], abaixo colacionada:

> RECURSO INOMINADO. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS E MATERIAIS. REPASSE DE INFORMAÇÕES PESSOAIS E DADOS BANCÁRIOS A OUTRAS EMPRESAS PELA EMPRESA DE TELEFONIA. COBRANÇAS INDEVIDAS REALIZADAS NO CARTÃO DE CRÉDITO DA RECLAMENTE. RESTITUIÇÃO DO INDÉBITO, EM DOBRO, DEVIDA. CONDUTA ABUSIVA. DANO MORAL. QUANTUM INDENIZATÓRIO MANTIDO. RECURSO CONHECIDO E DESPROVIDO.
> 1. In casu ficou demonstrado que após o repasse de dados pessoais e informações bancárias dos consumidores pela empresa de telefonia à corré, sem prévia autorização, a reclamante sofreu cobranças em seu cartão de crédito por serviços não solicitados.
> 2.Nestas condições, diante da conduta abusiva das reclamadas, é devida a repetição do indébito, em dobro, eis que evidente a má-fé e o intuito de obterem lucro indevido em prejuízos dos consumidores, bem como a indenização por danos morais, na medida em que a situação extrapolou a mera cobrança de dívida.

Inegável, portanto, que a LCP inaugurou a primavera da proteção de dados no Brasil.

5. FINCANDO ESTACAS: O MARCO CIVIL DA INTERNET

Nesse mesmo esteio, apenas três anos após a promulgação e entrada em vigor da Lei do Cadastro Positivo (LCP), a presidente da República Dilma Vana Rousseff também promulgou outra lei extremamente importante para a matéria da

52 TJPR, 0002916-31.2014.8.16.0184/0, Mag. Rela. Renata Ribeiro Bau, 3ª TR, Dj: 15/10/2015

proteção de dados no Brasil: a Lei Federal nº. 12.965/2014[53], conhecida amplamente como o Marco Civil da Internet (MCI).

Entendemos que essa legislação, tamanha sua importância, finca estacas quanto aos ditames da proteção de dados no Brasil. Isso porque, foi promulgada com o intento de estabelecer "*princípios, garantias, direitos e deveres para o uso da internet*" e é fático que, sob esse desiderato, construiu-se em verdadeira disciplina legislativa da proteção de dados e da privacidade dos cidadãos, sobretudo em sua relação de consumo digital, no país.

Isso porque, ao estabelecer os princípios da disciplina do uso de redes digitais, aquele diploma legislativo garantiu o seguinte, senão vejamos:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei.

Ora, **a proteção dos dados pessoais tornou-se princípio básico expresso do diploma legal do MCI**, passando a regrar as atividades de transmissão e transferências de informações em rede, assim como determinando a responsabilização dos controladores pelo desvio de tais princípios.

Indo mais longe, estabeleceu como direitos e garantias dos particulares a inviolabilidade de sua intimidade, sob pena de indenização pelos danos morais ou patrimoniais decorrentes de sua violação, veja-se:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação.

Ainda nesse sentido, e certamente instituindo normativo completamente adequado, o MCI determinou em seus incisos VII e VIII, do art. 7º, como assegurados os direitos dos particulares sobre a utilização dos dados na finalidade expressa pela contratação, salvo consentimento livre, expresso e informado, em

53 BRASIL, Lei Federal nº. 12.965/2014 'Marco Civil da Internet'. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

correlação perfeita aos ditames do art. 5º, incisos V e VII da LCP, citada no tópico acima:

> Art. 7º. (...) são assegurados os seguintes direitos:
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> justifiquem sua coleta;
> não sejam vedadas pela legislação; e
> estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

Vê-se, portanto, que tal é a harmonia legislativa do ordenamento jurídico quanto à matéria ventilada, bem como a harmonia entre normas, que tanto na legislação de 2011 (LCP), quanto na legislação de 2014 (MCI), ambas em vigor, exige-se o tratamento adequado dos dados do consumidor, devendo esses serem utilizados em finalidade que justifique sua coleta e que esteja especificada em contrato e com a qual o consumidor concorde, sem coação.

Ainda nesse espeque, importante aclarar que a disposição do art. 7º, inciso IX do MCI aperfeiçoou a disposição legal do art. 4º da LCP, para assim dispor, senão vejamos:

> Art. 7º. (...) são assegurados os seguintes direitos:
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais.

Ora, como visto, não basta que haja "cláusula perdida" em contratos extensos, ou letras diminutas no rodapé de uma página, para que o empresário possa se valer dos dados pessoais de seus clientes, mas deve haver destaque no contrato que chame a atenção do consumidor acerca de qualquer autorização referente ao tratamento desses dados e a finalidade envolvida e, mesmo, deve haver lógica entre o tratamento contratado e o escopo do próprio serviço garantido pelo contrato, sendo, portanto, impensável que um consumidor adquira um imóvel e ganhe "de quebra", a exposição de seus dados a terceiros para impulsionamento de vendas.

Na Seção II do MCI, intitulada "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", aquele diploma legal assim estabeleceu:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Portanto, vemos que inegável a força da legislação brasileira, tanto nos ditames da Constituição da República (CRFB), quanto naqueles da Lei do Cadastro Positivo (LCP), como no Marco Civil da Internet (MCI) quanto à proteção dos dados pessoais, o seu tratamento dentro dos limites definidos, a estipulação da finalidade de tratamento de forma clara, devendo o consumidor decidir por anuir ou não de forma consciente, livre e informada, bem como a responsabilização dos controladores dos dados pelo desvirtuamento de todos esses princípios e normativos legais.

Até nesse ponto, a legislação federal advinda do MCI é clara e protege o consumidor, sendo, indubitavelmente a primavera dos regulamentos da proteção de dados no Brasil.

6. À GUISA DE RETOQUE: A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Nesse sentido, vemos claramente que **a Lei Geral de Proteção de Dados Pessoais (LGPD), nada mais é do que um regulamento geral** de todas essas normas já presentes há muitos anos em nosso ordenamento jurídico, servindo como espécie de balizamento dos princípios e normativos diretivos das questões atreladas aos dados.

Tal diploma normativo segue tendência mundial de centralização dos normativos anteriormente esparsos, de proteção dos dados dos consumidores, seja na utilização de redes digitais, ou mesmo nos meios tradicionais de compra – portan-

to, seja ou não no campo do digital.

Neste aspecto, tal legislação se encontra na vanguarda mundial, conforme exemplos do *General Data Protection Regulation* (GDPR) na União Europeia, que passou a ser obrigatório em 25 de maio de 2018 e aplicável a todos os países do bloco, e o *California Consumer Privacy Act of 2018* (CCPA), nos Estados Unidos da América, implementado através de uma iniciativa em âmbito estadual, na Califórnia, onde foi aprovado no dia 28 de junho de 2018.

Portanto, independente da data em que a LGPD entre em vigor, seus princípios e axiomas já são aplicáveis tendo em vista todo o aparato normativo já mencionado, inclusive, a recepção já há 09 (nove) anos dos direitos de proteção de dados no Brasil no âmbito infraconstitucional e há 32 (trinta e dois) anos no âmbito constitucional.

Há que se notar, inclusive, que as disposições da LGPD não inovam quanto aos direitos ora analisados, apenas expandindo-os e lhes dando roupagem mais complexa.

Isso porque, tal como nas legislações federais supracitadas, a LGPD assim determina quanto aos direitos dos consumidores e, portanto, dos particulares na garantia da proteção de seus dados, na inviolabilidade da intimidade, e da vida privada etc.:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
>
> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

No campo dos regramentos ao tratamento dos dados, salta aos olhos as limitações impostas, vejamos:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> (...)
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> (...)
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

Portanto, resta cristalino que a nova lei repisa determinações já há muito cogentes quanto à necessidade de consentimento prévio e consciente pelo titular dos dados, bem como da utilização dos dados em respeito da finalidade contratada.

Quanto ao regramento e ao esclarecimento dos liames do consentimento do titular dos dados, a LGPD vai ainda mais longe que o MCI, mas trilhando a mesma esteira, deixando claramente firmadas a **necessidade de consentimento expresso, direto, objetivo, consciente e para uma finalidade específica**, senão vejamos:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> Art. 9º 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:
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.
> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

Cristalino, pois, que a LGPD brasileira já está em vigor vias de fato, dados os princípios e normas legais por ela balizados, mas que já presentes na norma maior da República e nas leis federais que garantem ao consumidor o respeito e a necessária proteção de seus dados.

Nesse sentido, para além da criação de uma Agência Nacional de Proteção de Dados[54] como instância administrativa regulatória/fiscalizatória, pode todo e qualquer consumidor se valer do Poder Judiciário para fazer cessar qualquer lesão ou ameaça de lesão aos direitos que já possuem sobre seus dados, independentemente do acesso à instância administrativa, como é cediço.

7. NA TRILHA DO EXPOSTO: UM PRECEDENTE NO SUPREMO TRIBUNAL FEDERAL

Na trilha de todo o exposto, e para demonstração do absoluto acerto da tese contida no presente artigo e da decisão que tomamos de ajuizamento da ação de meu cliente ainda em 2019, o plenário do Supremo Tribunal Federal julgou por 10 votos a 1, em 06 de maio de 2020, a confirmação das liminares deferidas em cinco Ações Diretas de Inconstitucionalidade ajuizadas contra a Medida Provisória nº. 954/2020.

Tal MP, promulgada pelo atual presidente da República, tinha como objetivo obrigar empresas de telecomunicações a repassar ao governo federal, por meio da fundação Instituto Brasileiro de Geografia e Estatística (IBGE), relação dos nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas, sob o argumento de que tais dados seriam tratados para vias de estatísticas oficiais da pandemia do SARS-Cov-2 (Covid-19) no Brasil.

Note-se, por absolutamente curioso, que a recomendação da MP em questão não foi proposta pelo Ministério da Saúde, mas pelo da Economia[55].

Contra tal Medida Provisória, cinco ADIs foram impetradas por quatro partidos políticos brasileiros[56] e pelo Conselho Federal da Ordem dos Advogados

54 Na mesma data em que o Senado votou prejudicado o adiamento da LGPD, o Executivo promulgou o Decreto nº. 10.474/2020, instituindo a ANPD.

55 GUEDES, Paulo Roberto Nunes. Ministro de Estado da Economia. MP nº 954/2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1591963010459&-disposition=inline. Acesso em 17/06/2020

56 Partido Social Democracia Brasileira (PSDB) – ADI nº. 6388; Partido Socialista Brasileiro (PSB) – ADI nº. 6389; Partido Socialismo e Liberdade (PSOL) – ADI nº. 6390 e Partido Comunista do

do Brasil (CFOAB)[57], sob o argumento comum de que tal MP, ao obrigar[58]:

> as empresas de telefonia fixa e móvel a disponibilizar à Fundação IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, viola os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e o sigilo dos dados.

O Voto proferido pela Ministra Relatora Rosa Weber, seguido pela esmagadora maioria do plenário do Supremo, é, justamente, de derrubada da MP do Executivo federal, tendo em vista a sua falta de clareza quanto à finalidade específica, bem como da amplitude do tratamento desses dados:

> Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a norma não oferece condições para a avaliação da sua adequação e necessidade. Desatende, assim, a garantia do devido processo legal.

Veja-se que a falta de apoio da própria sociedade civil a essa Medida Provisória é esmagadora, conforme se pode ver da consulta pública[59] disponibilizada no "E-Cidadania", portal do Senado da República na internet para consulta à população:

Brasil (PCdoB) – ADI nº. 6393.

57 ADI nº. 6387.

58 SECOM-STF. ***Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE***. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1. Acesso em 17/06/2020.

59 Resultado apurado pelo Senado até às 15h39 de 17/06/2020. Fonte: Senado. https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=141619

Importante frisarmos que em seu Voto, a Exma. Ministra relatora, além de contextualizar a relevância das questões atinentes ao tratamento de dados pessoais, tornou cristalina a proteção que tais dados possuem como matéria constitucional, valorada como preceito fundamental da Carta Política, sendo extremamente relevante o seu cumprimento tanto pelos agentes públicos, quanto pelos privados, vejamos:

> Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.
>
> A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (right to privacy) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.
> A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do 'sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal.

Vê-se, portanto, que o Supremo Tribunal Federal decidiu em maio do corrente ano que a matéria da proteção de dados encontra-se devidamente recepcionada pela própria Constituição da República, desde 1988, por meio da disposição do art. 5º, nos incisos já citados no presente artigo.

Tal decisão, portanto, reconhece a matéria da proteção de dados como direito fundamental da personalidade humana e, por isso, dialoga perfeitamente bem com as disposições do CDC, da LCP, do MCI e da própria LGPD, cuja vigência tem sido postergada desnecessariamente, assim como dos regramentos análogos do Direito Comparado, como o GDPR europeu.

CONCLUSÃO: NÃO HÁ MAIS ESCAPATÓRIA

A conclusão a que chegamos é nítida: não há mais escapatória.

O mundo *hiperconectado*, a era digital, as novas interfaces tecnológicas,

as mediações algorítmicas e, portanto, numéricas, da realidade social, todas essas perspectivas, como afirmara o Dr. Eneus Trindade[60], professor-pesquisador da Universidade de São Paulo, geram uma nova compreensão de sociedade e cultura:

> When thinking about the production of data in algorithms, we realize that the promotion of standards for data inclusion happens through the actors. Such actors are not necessarily human since AI has data capture machines. This finding favors the dialogue with the actor-network perspective of Latour, which studies the actors in connection in the digital networks and their flows of meanings. That is the narrative/discursive course of the networks, as a new domain of understanding of society and culture.

E para além da própria compreensão do cultural e do social, vivemos uma remodelação do mundo, sob as mediações do digital e dos algoritmos e isso se dá tanto na esfera do público – e, assim, das políticas públicas para vigilância e controle[61] das populações –, como na esfera do privado – e, assim, da utilização do *big data* para o tratamento dos arquétipos de consumo para além do conhecimento das pessoas, para gerar acumulação através de um consumismo que se retroalimenta, portanto, de uma outra vigilância e de um outro controle.

Nesse contexto, não podemos apontar as mediações algorítmicas em si mesmas, como nocivas ao social e aos direitos de privacidade, mas podemos facilmente entender que os atores que controlam o novo *modus operandi* do poder global possuem suas próprias agendas e elas não incluem a vontade conscientemente informada das pessoas.

Assim que, os ditames dos direitos à privacidade e os seus consectários correlatos, como os da proteção à intimidade, à vida privada, ao sigilo dos dados, ao tratamento adequado e que respeite a finalidade contratada, todos esses preceitos se fundam nos movimentos globais por uma ética do digital e da transferência de dados e, sobretudo, no Brasil, na Constituição da República promulgada desde 1988, nos tratados e convenções internacionais nos quais o Brasil é signatário há décadas, nas Leis do Cadastro Positivo e do Marco Civil da Internet.

Nesse sentido, embora a Lei Geral de Proteção de Dados Pessoais brasileira, ainda tenha a sua vigência protelada por uma espécie de acordo entre os Poderes Executivo e Legislativo, somente podemos entender como proteladas as normas procedimentais da persecução administrativa da proteção dos dados e da

60 TRINDADE, Eneus. ***Algorithms and Advertising in Consumption Mediations: A Semio-pragmatic Perspective***. In: Meiselwitz G. (eds) Social Computing and Social Media. Communication and Social Communities. HCII 2019. Lecture Notes in Computer Science, vol 11579. Springer, Cham. p. 518.

61 GRAHAM, Stephen. ***Cidades sitiadas. O novo urbanismo militar***. Tradução: Alyne Azuma. São Paulo: Boitempo Editorial, 2016. p. 52.

responsabilização dos infratores, não a salvaguarda dos direitos nela previstos, pelo Poder Judiciário.

Isso porque, as normas principiológicas e, mesmo, aquelas cuja positivação já se encontram há muito recepcionadas pelo ordenamento jurídico brasileiro, impõem a sua inescusável vigência e, assim, os movimentos necessários dos atores comerciais à proteção dos dados pessoais dos consumidores e o seu tratamento adequado e dentro das finalidades contratadas.

O vilipêndio de qualquer desses direitos, no Brasil, deve ser corrigido pelo Poder Judiciário, que, afinal de contas, é o guardião das leis e da Constituição.

De fato, não há mais escapatória.

REFERÊNCIAS BIBLIOGRÁFICAS

BITTAR, Eduardo C. B.; ALMEIDA, Guilherme Assis de. **Curso de Filosofia do Direito**. São Paulo: Atlas, 2001.

BRASIL, Código de Defesa do Consumidor. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm;

_____Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm;

_____ Convenção Americana de Direitos Humanos. Decreto nº. 678/1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf;

_____ Lei Federal nº. 10.406/2002 'Código Civil Brasileiro'. "Art. 421. *A liberdade contratual será exercida nos limites da função social do contrato*". Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

_____ Lei Federal nº. 13.709/2018 'Lei Geral de Proteção de Dados Pessoais'. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm;

_____ Lei Federal nº. 13.853/2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm;

_____ Lei Federal nº. 12.411/2011 'Lei do Cadastro Positivo'. Dispo-

nível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm;

_____ Lei Federal nº. 12.965/2014 'Marco Civil da Internet'. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian.** Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

CARVALHO, Kildare Gonçalves. **Direito Constitucional**. **Teoria do Estado e da Constituição. Direito Constitucional Positivo**. Belo Horizonte: Del Rey Editora, 2008.

CASTRO, Catarina Teresa Rola Sarmento e. **Direito da informática, privacidade e dados pessoais.** Coimbra: Almedina, 2005.

CHOMSKY, Noam. **Mídia. Propaganda política e manipulação**. São Paulo: Martins Fortes, 2017.

CHRISTIAN, Brian; GRIFFITHS, Tom. **Algoritmos para viver. A ciência exata das decisões humanas**. Tradução: Paulo Geiger. São Paulo: Companhia das Letras, 2017.

DE LORI, Andrews. Facebook is using you. Sunday Review. **The New York Times.** Disponível em: https://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html?_r=0.

DENHAM, Elizabeth. ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information. Disponível em: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued--with-maximum-500-000-fine/;

_____ Intention to fine British Airways £183.39M under GDPR for data breach. Disponível em: https://ico.org.uk/about-the-ico/news-and--events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.

GRAHAM, Stephen. **Cidades sitiadas. O novo urbanismo militar**. São Pau-

lo: Boitempo Editorial, 2016.

GRASSEGGER, Hannes; KROGERUS, Mikael. **The data that turned the world upside down**. Motherboard, 2007, in MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018.

GUEDES, Paulo Roberto Nunes. Ministro de Estado da Economia. Medida Provisória nº. 959/2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf;

_____ Ministro de Estado da Economia. MP nº 954/2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1591963010459&disposition=inline.

KLEBNIKOV, Sergei. Por que as ações do Facebook parecem indestrutíveis. **Forbes**, 2020. Disponível em: https://forbes.com.br/negocios/2020/01/por-que-as-acoes-do-facebook-parecem-indestrutiveis/.

KNAST, Priscilla. **7 tipos de cookies do navegador.** Disponível em: www.oficinadanet.com.br/internet/24798-7-tipos-de-cookies-do-navegador.

LEVITSKY, Steven; ZIBLATT, Daniel. **Como as democracias morrem**. Rio de Janeiro: Zahar, 2020.

MORAES, Alexandre de. **Direito constitucional**. 32. ed. São Paulo: Atlas, 2016.

ONU. DUDH. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf.

MOROZOV, Evgeny. **Big Tech. A Ascensão dos dados e a morte da política**. São Paulo: Ubu Editora, 2019.

PARLAMENTO EUROPEU. Jornal Oficial da União Europeia. 'Regulamento Geral de Proteção de Dados' da União Europeia. Item 4, art. 4º Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=pt

PLATÃO. **A República**. 514-a/517-c. in MARCONDES, Danilo. **Textos básicos de filosofia**. Dos Pré-Socráticos a Wittgenstein. 2ªed. Rio de Janeiro, Zahar, 2000.

PEREZ, Clotilde; TRINDADE, Eneus. **Das Mediações Comunicacionais à mediação comunicacional numérica no consumo:** uma tendência para a pesquisa. São Paulo: Trabalho apresentado no IX Propesq PP – Encontro de Pesquisadores em Publicidade e Propaganda, 2018.

Portal Intelectual: **Proteção de dados:** Cyrela é processada por tratamento inadequado de dados de consumidores e sofre liminar. Disponível em: https://www.portalintelectual.com.br/protecao-de-dados-cyrela-e-processada-por-tratamento-inadequado-de-dados-de-consumidor-e-sofre-liminar/.

RIZZARDO, Arnaldo. **Contratos**. 5ª ed. Rio de Janeiro: Forense, 2005.

ROSA, Arthur. Liminar evita uso de dados de consumidor. Informações foram divulgadas a terceiros por empresa. **Valor Econômico.** Disponível em: https://valor.globo.com/legislacao/noticia/2019/09/29/liminar-evita-uso-de-dados-de-consumidor.ghtml.

SECOM-STF. **Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 40ª. ed. São Paulo: Malheiros, 2017.

Sistema de Proteção ao Crédito (SPC). Cadastro Positivo Consumidor. Disponível em: https://www.spcbrasil.org.br/cadastropositivo/consumidor/index.html#oquee.

SUMPTER, David. **Dominados pelos números. Do Facebook e Google às Fake News. Os algoritmos que controlam a nossa vida**. Rio de Janeiro: Bertrand Brasil, 2019.

THEODORO JR., Humberto. **O contrato e sua função social**. 2ª ed. Rio de Janeiro: Forense, 2004.

The Harris Poll. 2019 Corporate Reputation Rankings. Disponível em: https://theharrispoll.com/axios-harrispoll-100/

TIROLE, Jean. **Economia do bem comum.** Rio de Janeiro: Zahar, 2020.

TRINDADE, Eneus. **Algorithms and Advertising in Consumption Media-**

tions: A Semio-pragmatic Perspective. In: Meiselwitz G. (eds) Social Computing and Social Media. Communication and Social Communities. HCII 2019. Lecture Notes in Computer Science, vol 11579. Springer, Cham.

VALENTE, Fernanda. Juíza multa construtora por compartilhar dados pessoais de cliente. **Consultor Jurídico.** Disponível em: https://www.conjur.com.br/2019-ago-23/juiza-impoe-multa-cyrela-repassar-dados-pessoais-cliente.

ZUBOFF, Shoshana. Big Other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, 2015, p. 75-89 *in* BRUNO, Fernanda et al. (org.). Tecnopolíticas da Vigilância. Perspectivas da margem. São Paulo: Boitempo Editorial, 2018.