Como citar: ZANATTA, Rafael; SECAF, Helena; MENDONÇA, Julia. A aplicabilidade da Lei Geral de Proteção de Dados Pessoais aos corretores de dados, in: VILLAS BOAS CUEVA, Ricardo; FRAZÃO, Ana. **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters, 2021, p. 957-988.

A aplicabilidade da Lei Geral de Proteção de Dados aos corretores de dados[1]

Rafael A. F. Zanatta[2]
Helena Secaf[3]
Júlia Mendonça[4]

1. Introdução

"Você pode não saber quem são os corretores de dados, mas eles conhecem você"[5]. Essa é a frase que introduz a reportagem da Avast publicada em 2021 sobre corretores de dados, também conhecidos como *data brokers* ou *information brokers*. São empresas que agregam, coletam, armazenam, licenciam e vendem dados pessoais - incluindo seus derivados e inferências - com finalidade lucrativa. São organizações privadas que historicamente atuam de forma discreta e que hoje operam um negócio

[1] Este artigo é uma versão expandida de uma apresentação realizada por Rafael Zanatta no II Seminário Internacional sobre a Lei Geral de Proteção de Dados (LGPD) – Arquitetura da privacidade no Brasil: Eixos centrais da política nacional de proteção de dados, realizado pelo Centro de Estudos Judiciários do Conselho da Justiça Federal (CEJ/CJF), em parceria com a Escola Nacional de Formação e Aperfeiçoamento de Magistrados (Enfam) e o Instituto Brasiliense de Direito Público (IDP), em 30 de abril de 2021. Na ocasião, a apresentação contou com comentários do ministro Paulo de Tarso Sanseverino, Danilo Doneda e Marcela Mattiuzzo. Os autores agradecem também as discussões com Bruno Bioni, Mariana Rielli e equipe de pesquisadores da Associação Data Privacy Brasil de Pesquisa.

[2] Diretor da Associação Data Privacy Brasil de Pesquisa. É mestre pela Faculdade de Direito da USP e doutorando pelo Instituto de Energia e Ambiente da USP. Mestre em direito e economia pela Universidade de Turim. Alumni do Privacy Law and Policy Course da Universidade de Amsterdam. Research Fellow da The New School (EUA). Membro da Rede Latino-Americana de Vigilância, Tecnologia e Sociedade (Lavits). Membro do Instituto Brasileiro de Responsabilidade Civil (Iberc).

[3] Pesquisadora na Associação Data Privacy Brasil de Pesquisa. Bacharel em direito pela Fundação Getúlio Vargas de São Paulo.

[4] Pesquisadora na Associação Data Privacy de Pesquisa. Graduanda em Direito pela Universidade Federal da Bahia (UFBA).

[5] LATTO, Nica. Data Brokers: Everything You Need to Know. AVAST. 2021. Disponível em: https://www.avast.com/c-data-brokers. Acesso em: 20 abr. 2021.

bilionário de "enriquecimento de dados", "insights analíticos" e perfilização de consumidores para inúmeros fins comerciais.[6]

Em 1997, Stephane Bressan e Thomas Lee, em estudo publicado no Massachusetts Institute of Technology, argumentaram que os corretores de dados são agentes que operam negócios de compra e venda de informação como *commodity*. São agentes especializados na "coleta e redistribuição de informação"[7], em especial, dados pessoais. Mais de 20 anos depois, em artigo escrito para a *Encyclopedia of Big Data* da editora Springer, Abdullah Alowairdhi e Xiaogang Ma conceitualizam os corretores de dados como aqueles que "adquirem e armazenam dados individuais como produtos em uma infraestrutura de dados confidencial, que armazena, compartilha e consome dados por meio de tecnologias em rede"[8]. Muitos deles não são apenas *intermediários*, mas se estruturam como poderosas empresas de armazenamento de informação, logística e acesso a seus serviços por sofisticados arranjos de computação em nuvem. É assim que operam empresas como Acxiom, Experian[9], Epsilon, CoreLogic, Datalogix, Intelius, PeekYou, Exactis, Recorded Future, entre outras.

O desconhecimento sobre os corretores de dados é generalizado. Em 2012, em matéria escrita para o The New York Times, a jornalista Natasha Singer observou que "poucos consumidores já ouviram falar da Acxiom"[10], apesar da empresa realizar 50 trilhões de transações de dados por ano, possuir informação de 500 milhões de "consumidores ativos" e mais de 1.500 *data points* por pessoa nos Estados Unidos da América. Se, por um lado, essas empresas são desconhecidas pela população, elas são amplamente conhecidas por bancos, grandes empresas de varejo, lojas de

---

[6] Para uma análise sociológica sobre os corretores de dados no Brasil, ver SILVEIRA, Sergio Amadeu da; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. *Liinc em Revista*, v. 12, n. 2, p. 217-230, 2016. SILVEIRA, Sergio Amadeu da. *Tudo sobre tod@ s: Redes digitais, privacidade e venda de dados pessoais*. São Paulo: Edições Sesc, 2017. SAMPAIO, Alice Castaldi. *Data Brokers: um novo modelo de negócios baseado em vigilância de dados*. Dissertação de Mestrado. Universidade Estadual de Campinas, 2017.

[7] BRESSAN, Stephane. LEE, Thomas. Information Brokering on the World Wide Web. *WebNet 97 World Conference*, 1997. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/2663/SWP-3963-37617980-CISL-9708.pdf?sequence=1. Acesso em: 19 maio. 2021.

[8] ALOWAIRDHI, Abdullah; MA, Xiaogang. Data Brokers and Data Services, in: SCHINTLER, L; MCNEELY, C (ed.). *Encyclopedia of Big Data*. New York: Springer, 2019.

[9] No Brasil, a Experian é conhecida como Serasa Experian.

[10] SINGER, Natasha. Mapping and Sharing the Consumer Genome, The New York Times, 16 de Jun., 2012. Disponível em: https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html. Acesso em: 19 maio. 2021.

departamento e montadoras. Há um amplo interesse não apenas em acessar os dados "minerados e refinados", mas adquirir os modelos preditivos sobre comportamento dos consumidores. Como afirmado pelos executivos da Acxiom, o objetivo da empresa é "reconhecer os consumidores, lembrar suas ações, classificar seus comportamentos e influenciá-los"[11].

Como os corretores de dados são afetados pelas leis de proteção de dados pessoais? A existência de legislações como a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018 - "LGPD") impossibilitam sua operação, tornando-as imediatamente ilícitas? Deveriam os corretores de dados interromperem suas atividades no Brasil, em razão da chegada da LGPD?

É evidente que essas empresas não fecharão suas portas por conta do advento da LGPD, mas é inegável que suas operações serão profundamente afetadas pela aplicação da lei, pela atuação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e pelo sistema de tutela coletiva de proteção de dados no Brasil, incluindo o Ministério Público, Defensorias Públicas e ONGs. Em termos de aplicabilidade do direito fundamental à proteção de dados pessoais, esse impacto é notável em ao menos três aspectos: (i) a capacidade de demonstração de base legal de tratamento de dados pessoais, (ii) a licitude das operações de perfilização e de construção de modelos preditivos, diante dos direitos dos titulares dos dados pessoais, e (iii) os deveres de transparência e boa-fé aplicáveis aos corretores, em especial a aplicabilidade do precedente do caso sobre *credit scoring* no Superior Tribunal de Justiça.

O objetivo deste artigo é demonstrar como a LGPD afeta os mercados de corretores de dados, tendo em mente o problema das bases legais para tratamento de dados, os deveres aplicáveis aos corretores de dados e o princípio da boa fé e a indenização por tratamento de dados excessivos. Para apoiar essa discussão jurídica, o artigo inicia com uma explicação mais profunda sobre o que são (e quem são) os corretores de dados e como as autoridades públicas, em especial as dos EUA, têm enxergado a natureza de suas operações de uma perspectiva de transparência e respeito aos direitos básicos dos consumidores.

[11] SINGER, Natasha. *op. cit.*

O artigo conclui com uma reflexão sobre a natureza dos danos em casos de usos de informações excessivas e perfilizações que podem ser consideradas ilícitas. Discute-se o impasse da adoção do dano moral *in re ipsa* ou a construção de um tipo distinto de dano, conectando-se com os precedentes do Superior Tribunal de Justiça.

2. Compreendendo o papel dos corretores de dados e os riscos de suas operações

2.1. O que são corretores de dados?

De forma geral, pode-se dizer que corretores de dados (*data brokers*) são empresas com finalidade lucrativa que agregam, coletam, armazenam, categorizam, licenciam e vendem dados pessoais, seus derivados e inferências. Essas empresas não necessariamente possuem uma relação direta com os titulares dos dados, os quais geralmente não têm conhecimento claro deste processo.

A literatura que se dedica a destrinchar as particularidades sobre este mercado mostra que as definições tendem a ser bastante convergentes. Verbicaro e Vieira (2021), em artigo recente para a Revista de Direito do Consumidor, conceituam os corretores de dados como intermediários "que coletam informações pessoais dos consumidores de variadas fontes para vendê-las ou cedê-las a outras empresas"[12]. Ressaltam que "normalmente não participam da relação de consumo tradicional; muitas vezes, o consumidor desconhece a sua existência e a sua prática"[13]. Jordan Abbott, diretor do setor de ética de dados da Acxiom, uma das maiores corretoras de dados do mundo, segue pelo mesmo caminho, conceituando corretores de dados como

[12] "Data brokers são intermediários que coletam informações pessoais dos consumidores de variadas fontes para vendê-las ou cedê-las a outras empresas. São empresas que normalmente não participam da relação de consumo tradicional; muitas vezes, o consumidor desconhece a sua existência e a sua prática. Para a Federal Trade Commission, os data brokers compilam informações dos consumidores com o principal objetivo de traçar perfis a fim de direcionar a publicidade. Tal tratamento de informação normalmente não é informado ao consumidor, que tem seus dados coletados, manipulados e compartilhados sem seu conhecimento e, consequentemente, sem seu consentimento. Trata-se de um ciclo informacional obscuro na relação, que influi, porém, diretamente no êxito do negócio." VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. *Revista de Direito do Consumidor*. vol. 134. ano 30. p. 195-226. São Paulo: Ed. RT, mar./abr. 2021. Acesso em: 19 maio. 2021.

[13] VERBICARO, Dennis. VIEIRA, Janaína. op. cit.

"entidades que coletam, agregam e vendem dados pessoais, seus derivados e inferências por meio de fontes públicas e privadas díspares"[14].

O relatório publicado pelo Cracked Labs em 2017 sobre *Vigilância Corporativa na Vida Cotidiana* afirma que, para além da agregação, combinação e comercialização de grandes quantidades de informações coletadas de diversas fontes online e offline (publicamente disponíveis ou compradas e licenciandas de outras empresas), os corretores de dados "analisam dados, fazem inferências, classificam as pessoas em categorias e fornecem milhares de atributos sobre indivíduos a seus clientes"[15]. Aqui mora um dos maiores riscos da atividade, conforme será delineado mais adiante neste artigo.

Conforme relatório concluído pela Federal Trade Comission (FTC),[16] baseado em estudo aprofundado sobre nove *brokers*, os corretores de dados inferem os interesses do consumidor a partir dos dados que coletam. Eles usam esses interesses, junto com outras informações, para colocar consumidores em categorias. O relatório ressalta, também, que os corretores de dados fornecem os dados não apenas aos usuários finais, mas também a outros corretores de dados.[17].

Segundo o artigo publicado pela Avast em 2021,[18] os corretores de dados podem ser divididos em quatro categorias principais: (i) Marketing e Publicidade, (ii) Informações Financeiras, (iii) Pesquisa de Pessoas e (iv) Informações de Saúde. A categoria de Marketing e Publicidade engloba as atividades de publicidade direcionada, marketing "personalizado", anúncios que aparecem como relevantes de maneira suspeita ou outros anúncios de produtos em que se tenha clicado antes. Informações Financeiras, por sua vez, é a categoria delimitada por corretores de detecção de fraude ou mitigação de risco, que negociam informações financeiras

[14] ABBOTT, Jordan. Time to Build a National Data Broker Registry - The New York Times, Opinion. 2019. Disponível em: https://www.nytimes.com/2019/09/13/opinion/data-broker-registry-privacy.html. Acesso em: 20 abr. 2021.
[15] CHRISTL, Wolfie. Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. 2017. Cracked Labs. Disponível em: http://crackedlabs.org/en/corporate-surveillance. Acesso em: 20 abr. 2021.
[16] FEDERAL TRADE COMMISSION (FTC). Data Brokers: A Call for Transparency and Accountability. 2014. Disponível. em: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Acesso em: 19 maio. 2021.
[17] FEDERAL TRADE COMMISSION (FTC), 2014. op cit.
[18] LATTO, Nica. op. cit.

pessoais, como pontuação de crédito e "risco" financeiro percebido. Eles podem, também, ajudar a prevenir fraudes, verificando identidades reais. Pesquisa de Pessoas enquadra os corretores de dados que pesquisam pessoas, oferecendo relatórios de dados especializados sobre pessoas individuais. Por fim, a categoria de Informações de Saúde abarca os corretores que compilam problemas de saúde percebidos com base em pesquisas on-line (como sintomas, terapias, etc.) e off-line, como a compra de medicamentos na qual se utilizou cartões de fidelidades de farmácias, construindo um perfil sobre a saúde das pessoas

A autora faz a ressalva de que esses dados compilados pelos corretores de Informações de Saúde podem, inclusive, ser usados por seguradoras, as quais podem adquirir esses conjuntos de dados e utilizá-los para aumentar taxas ou até mesmo se recusar a fazer um seguro. Comenta, ainda, que quando se considera que os dados podem nem mesmo ser válidos (pode-se estar procurando pelos sintomas de seu marido ou comprando remédios para sua avó), a corretagem de informações de saúde pode ser uma das práticas de corretagem mais injustas.[19] Aqui já se começa a ter uma noção mais concreta dos riscos desse mercado - de grandes proporções, muito lucrativo e, como já mencionado, muito pouco transparente.

2.2. Quais os principais agentes econômicos desse mercado?

Jogar luz sobre o mercado de corretagem de dados perpassa pelo conhecimento de quem são os *data brokers*. Alguns dos corretores de dados são mais conhecidos que outros. A Experian e a Equifax são dois exemplos mais conhecidos no campo de birôs de crédito. A Experian possui dados de crédito sobre 918 milhões de pessoas, bem como dados de marketing de 700 milhões. A Equifax, por sua vez, possui uma base de dados de 820 milhões de pessoas[20].

A Acxiom é outro exemplo relevante. É uma empresa que tem coletado dados sobre centenas de milhões de pessoas desde 1969, sendo a maior parte desses dados oriundos de registros públicos, pesquisas com consumidores, listas de assinantes de

[19] LATTO, Nica. op. cit.
[20] CHRISTL, Wolfie. op. cit.

revistas, relatórios resumidos sobre compras no varejo e rastreamento online.[21] Dessa forma, são "[...] 23.000 servidores constantemente coletando, agrupando e analisando mais de 50 trilhões de transações de dados exclusivos todos os anos"[22]. A empresa fornece até 3.000 elementos de dados sobre 700 milhões de pessoas de milhares de fontes em muitos países, incluindo os EUA, Reino Unido e Alemanha. Inicialmente uma empresa de marketing direto, a Acxiom desenvolveu seu banco de dados centralizado do consumidor no final dos anos 1990.[23]

A Datalogix também pode ser citada. É propriedade da Oracle, a qual lida principalmente com o rastreamento de padrões de comportamento para aumentar as vendas, coletando dados de compras online e offline dos consumidores. A Datalogix "desfrutou de um relacionamento confortável de seis anos com o Facebook, durante os quais ajudou a rastrear quais usuários compravam produtos com base em anúncios do Facebook"[24]. A Oracle, por sua vez, anuncia em seu site a possibilidade de ter IDs únicos de 5 bilhões de pessoas.[25]

É importante notar que há um interesse relevante de várias organizações em adquirir empresas especializadas nesse tipo de perfil de corretagem de dados. A Abacus Canada é um bom exemplo, foi lançada em 2005 pela gigante de marketing online com sede nos Estados Unidos, a DoubleClick Inc.[26]A Abacus Canada é uma extensão da Abacus Alliance, também com sede nos Estados Unidos, que contava com mais de 2.400 membros em oito países em maio de 2005.[27] A DoubleClick, por sua

[21] CHRISTL, Wolfie. op. cit.
[22] LATTO, Nica. op. cit.
[23] CHRISTL, Wolfie. op. cit.
[24] LATTO, Nica. op. cit.
[25] A maioria desses dados foi retirada do já mencionado relatório de 2017, Vigilância Corporativa na Vida Cotidiana, o qual apresenta em detalhes o funcionamento dessas empresas mencionadas (e outras mais), pormenorizando sua atividade em termos de quantidade de dados, setor predominante de atuação, tipos de dados coletados e espécies de predições. CHRISTL, Wolfie. Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. 2017. Cracked Labs. Disponível em: http://crackedlabs.org/en/corporate-surveillance. Acesso em: 20 abr. 2021.
[26] THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC). On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship. 2006. Disponível em: https://cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Acesso em: 19.maio. 2021.
[27] THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC. op. cit.

vez, foi comprada pela Google em 2008, por US $3,1 bilhões.[28] Ou seja, há um interesse bastante robusto nesse mercado: o ramo é grande e lucrativo.

Conforme já mencionado, este é um mercado que opera sorrateiro, escondido tanto dos cidadãos comuns (muitas vezes titulares dos próprios dados em transação), quanto de regras regulatórias. Os corretores de dados possuem uma capacidade profunda de, a partir da coleta e agregação de dados, categorizar os titulares e extrair dessa categorização informações sobre interesses e comportamentos. Dada a natureza e tamanho da atividade (e lucratividade) isso não é trivial: traz à tona a discussão de quais seriam as inferências razoáveis que o sistema jurídico permite. E acima de tudo, qual seria a licitude de construção desses perfis para que isso possa ser licenciado, vendido ou negociado para enriquecimento de outras bases de dados. Esses pontos serão tratados mais adiante. O próximo tópico, no entanto, foca na opacidade deste mercado e, concomitantemente, nos tipos de riscos que essas atividades apresentam aos titulares e à sociedade como um todo.

2.3. O diagnóstico sobre opacidade e riscos nos mercados de corretores de dados

Ao definir corretores de dados, Justin Sherman, em seu artigo "Data Brokers Are a Threat to Democracy", incorpora no próprio conceito uma crítica: “corretores de dados são intermediárias do capitalismo de vigilância - compram, agregam e reembalam dados de uma variedade de outras empresas, tudo com o objetivo de vendê-los ou distribuí-los posteriormente”[29]. Essa acusação de que os corretores de dados são uma ameaça à democracia não surge sem razão: a atividade de “'encaixar uma pessoa', a partir de seus dados pessoais, em um perfil social e inferir algo sobre ela”[30] traz consequências no campo individual e, fundamentalmente, no campo coletivo.

[28] LAWSKY, David. Google closes DoubleClick merger after EU approval. Reuters. 2008. Disponível em: https://www.reuters.com/article/us-google-doubleclick-eu-idUSBFA00058020080311. Acesso em: 13 mai 2021.

[29] SHERMAN, Justin. Data Brokers Are a Threat to Democracy. Wired. 2021. Disponível em: https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/. Acesso em: 13 maio. 2021.

[30] ZANATTA, Rafael. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. In: MIRAGEM, Bruno; MARQUES, Claudia Lima;

As preocupações com esse mercado, em especial a capacidade de perfilização e discriminação abusiva, remontam há mais de uma década. Em 2006, a Clínica Canadense de Política e Interesse Público da Internet (CIPPIC), da Universidade de Ottawa, produziu relatório sobre a indústria canadenese de corretagem de dados. Com o objetivo de trazer à tona a discussão sobre como informações detalhadas sobre as pessoas chegam às mãos de organizações com as quais não se tem nenhuma relação direta, o relatório já alertava para os problemas da atividade:

> "Embora a coleta e o uso de dados pessoais para fins de marketing direcionado possam parecer relativamente inofensivos, isso levanta questões de privacidade significativas. Em particular, o crescente acúmulo de dados pessoais e a consolidação de bancos de dados deixa os indivíduos vulneráveis a abusos por parte daqueles que têm acesso aos dados." (tradução livre)[31]

Seis anos depois, a Federal Trade Commission analisou a indústria de *data brokers* em um primeiro relatório sobre o assunto e identificou a falta de controle dos consumidores sobre a coleta e o uso de suas informações pelos corretores de dados. A Comissão chegou a apoiar uma legislação específica que forneceria aos consumidores acesso às suas informações mantidas por um corretor de dados. Para aumentar ainda mais a transparência, a Comissão apelou aos corretores de dados que compilam dados para fins de marketing para "explorar a criação de um site centralizado onde os corretores de dados poderiam (1) se identificar para os consumidores e descrever como eles coletam e usam os dados e (2) detalhar os direitos de acesso e outras opções que fornecem em relação aos dados do consumidor que mantêm".[32]

Em 2013, em tom ácido, o *Committee on Commerce, Science and Transportation* do Senado dos EUA, avaliou o problema das violações de direitos dos consumidores nos mercados de corretagem de dados e chegou à seguinte conclusão, por meio de seu relator:

MAGALHÃES, Lucia Ancona, Direito do Consumidor: 30 anos do CDC. Da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2021, p. 519.

[31] THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC), op. cit.

[32]FEDERAL TRADE COMMISSION (FTC). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. 2012. Disponível em: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers. Acesso em: 19 maio 2021.

> "os consumidores têm meios mínimos de aprender - ou fornecer informações - sobre como os corretores de dados coletam, analisam e vendem suas informações. A grande variedade de políticas de acesso e controle do consumidor fornecidas pelas empresas representativas mostram que os direitos do consumidor nesta área são oferecidos praticamente inteiramente a critério das empresas. As limitações contratuais impostas pelas empresas com relação à divulgação de suas fontes de dados aos clientes colocam barreiras adicionais à transparência do consumidor. E a recusa de várias das principais corretoras de dados em fornecer ao Comitê respostas completas sobre as fontes de dados e os clientes apenas reforça a aura de sigilo que cerca o setor"[33] (tradução livre)

Em 2014, no já mencionado relatório que se tornou amplamente conhecido,[34] produzido sob liderança de Julie Brill na Federal Trade Commission, a FTC argumentou que, embora possam existir benefícios, como a prevenção de fraudes, melhoria de ofertas de produtos e entrega de anúncios personalizados para consumidores, muitas das finalidades para as quais os corretores de dados coletam e usam os dados representam *riscos para os consumidores*. Esses riscos, em sua grande maioria, advém do problema da perfilização (*profiling*).[35]

Um dos pontos cruciais da perfilização é que ela está mais relacionada a grupos sociais do que ao indivíduo em si, o que provoca uma tensão ainda não resolvida na matriz individualista da proteção de dados pessoais".[36]Ou seja, a perfilização está mais preocupada em prever certeiramente o comportamento do indivíduo do que de fato acertar sua categorização social. A categorização é muito menos uma tentativa de

[33] COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Staff Report For Chairman Rockefeller, 2013. p. 36 Disponível em: https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. Acesso em: 19 maio. 2021.

[34] FEDERAL TRADE COMMISSION (FTC), 2014. op cit.

[35] Perfilização pode ser conceituada como: "O processo de 'descobrir' correlações entre dados em bancos de dados que podem ser usados para identificar e representar um sujeito humano ou não humano (indivíduo ou grupo) e / ou a aplicação de perfis (conjuntos de dados correlacionados) para individualizar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria".HILDEBRANDT, M. Defining Profiling. A New Type of Knowledge? In.: Hildebrandt, M.; Gutwirth, S. (Org.) Profiling the European Citizen: Cross-Disciplinary Perspectives. Cham/SWI: Springer Science, pp. 17-44. É isso que fazem os corretores de dados, como destacado pelo relatório da Cracked Labs, "os corretores de dados também calculam pontuações que prevêem o possível comportamento futuro de um indivíduo, em relação, por exemplo, à estabilidade econômica de alguém ou aos planos de ter um filho ou de mudar de emprego". CHRISTL, Wolfie. *op. cit.*

[36] ZANATTA, 2021, p. 518.

representação fiel do titular, mas de "[...] prever seu comportamento para um objetivo específico, feito a partir de uma massiva agregação de dados".[37]

Esse tipo de categorização automatizada pode levar a consequências materiais na vida não-virtual dos titulares. Por exemplo, se for negada a um consumidor a capacidade de concluir uma transação com base em erro em um produto de mitigação de risco, o consumidor pode ser prejudicado sem saber por quê. Nesses casos, o consumidor não só fica privado do benefício imediato, como também não pode tomar medidas para evitar que o problema se repita.[38] Isso se agrava dado que os processos de pontuação usados em alguns produtos de marketing não são transparentes para os consumidores: não se consegue realizar ações que possam mitigar os efeitos negativos de pontuações mais baixas, como limitar-se a anúncios de crédito subprime, ou receber diferentes níveis de serviço das empresas.[39]

Para além do risco do erro (informações imprecisas e incompletas), há o perigo da discriminação: "a natureza classificatória das tecnologias de perfilação [...] possui enorme potencial de aprofundar os padrões discriminatórios já existentes".[40]Nesse sentido, alerta o relatório da FTC, que "os profissionais de marketing podem até mesmo usar inferências aparentemente inócuas sobre os consumidores de maneiras que suscitam preocupações".[41] O exemplo dado é o de um consumidor que eventualmente tenha seu comportamento traçado à "entusiastas de motociclistas". Isso poderia ser útil a uma concessionária de motocicletas, mas também a uma seguradora que, "[...] usando esse mesmo segmento pode inferir que o consumidor se envolve em comportamento de risco".[42]Um outro exemplo também bastante problemático é a inferência, a partir dos dados agregados, de que determinado titular é alcoólatra e, a partir disso, empresas de marketing de bebidas alcoólicas passam a mirar propagandas nesse sujeito, aproveitando-se de sua vulnerabilidade. O relatório completa: "[...]

[37] HOSNI, David Salim Santos. MARTINS, Pedro Bastos Lobo. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. Internetlab. In.: Revista Internet & Sociedade, vol. 1, n.2. 2020. Disponível em: https://revista.internetlab.org.br/736-2/. Acesso em: 19 maio. 2021.
[38]FEDERAL TRADE COMMISSION (FTC), 2014. op cit.
[39]FEDERAL TRADE COMMISSION (FTC), 2014. op cit.
[40] HOSNI, David Salim Santos. MARTINS, Pedro Bastos Lobo. op. cit.
[41]FEDERAL TRADE COMMISSION (FTC), 2014. op cit.
[42]FEDERAL TRADE COMMISSION(FTC), 2014. op cit.

produtos de pesquisa sobre pessoas podem ser usados para facilitar o assédio, ou mesmo perseguição, e podem expor vítimas de violência doméstica, policiais, promotores, funcionários públicos ou outros indivíduos a retaliação ou outro dano"[43].

Como notado por Alice Sampaio, os corretores de dados "são atores importantes na consolidação e evolução de técnicas, como data mining e profiling, e na construção de um 'conhecimento' que classifica pessoas".[44] O risco reside não só nos problemas de transparência e insuficiência de acesso à informação pelo consumidor - problemas típicos da própria origem dos direitos dos consumidores da década de 1960 nos EUA -, mas principalmente na potencial abusividade no uso de dados e na ilicitude das formas de perfilização e construção de modelos de análise preditiva de comportamentos.[45] O problema central, como diagnosticado por governos e por acadêmicos, está na construção de *profilings*, na exploração de correlações entre milhares de *data points* para inferências sobre potencial comportamento humano e sobre os potenciais discriminatórios quando essas inferências deixam de ser razoáveis, tornando-se impróprias dentro de uma perspectiva ético-jurídica, com graves impactos sociais.[46]

Na próxima seção, explora-se como essa dimensão supraindividual, relacionada à natureza coletiva do problema da perfilização abusiva, encontra amparo jurídico na Lei Geral de Proteção de Dados Pessoais.

---

[43] FEDERAL TRADE COMMISSION(FTC), 2014. op cit.

[44] SAMPAIO, Alice Castaldi. 2017. op cit., p. 104.

[45] Com base no processamento de dados, e levando em consideração a finalidade deste processamento, o group profiling agrupa os indivíduos em "[...] categorias anteriormente desconhecidas, social e visualmente imperceptíveis com base na análise de dados, sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias".ROUVROY, A. Of data and Men. Fundamental Rights of Freedoms in a World of Big Data.Council of Europe, Directorate General of Human Rights and Rule of Law, 2016 vol.T-PD-BUR. p. 1-37. Ou seja, são categorias com as quais o próprio indivíduo não conseguiria se identificar, porque só fazem sentido na constância do processamento dos dados e não têm sentido social.

[46] "A perfilização se beneficia daquilo que Eubanks chama de "feedback looping de injustiça": grupos marginalizados estão mais suscetíveis à coleta de dados pessoais pois são beneficiários de políticas sociais e estão mais vulneráveis ao monitoramento estatal. Esses dados servem para reforçar a marginalidade, quando tais grupos são alvo de algoritmos preditivos, análises de risco e sistemas automáticos de elegibilidade." ZANATTA, 2021, p. 519.

3. A conformidade dos corretores de dados com a Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) possui impacto direto aos corretores de dados que exploram informações de cidadãos brasileiros ou que operam atividades de tratamento de dados pessoais no Brasil. Não é sem razão que diversas empresas que atuam como corretoras de dados no país já assumiram um discurso "pró LGPD" e de pretensa conformidade com a legislação.

Discute-se, adiante, três aspectos centrais da aplicabilidade da LGPD aos corretores de dados: (i) o problema das bases legais para tratamento de dados, (ii) os deveres aplicáveis aos corretores de dados, considerando o intercruzamento da LGPD com o Código de Defesa do Consumidor e a Lei do Cadastro Positivo e (iii) a problemática do tratamento de dados excessivos pelo corretor de dados, especialmente quando há impossibilidade do titular conhecer ou contestar um dado inferencial, construído a partir do cruzamento de seus dados pessoais em uma situação prévia de tratamento.

3.1. O problema das bases legais para tratamento de dados

O problema das bases legais (*legal grounds for data processing*) não é inédito no debate sobre aplicabilidade do direito ao mercado dos corretores de dados.

No já citado relatório publicado em 2006 pela Clínica Canadense de Política e Interesse Público da Internet (CIPPIC)[47], foi identificado que, geralmente, os corretores de dados dão algumas respostas semelhantes quando investigados sobre sua licitude. Uma das principais respostas "padrão" consiste na alegação de que os dados seriam "tratados com consentimento". No entanto, é necessário analisar que tipo de consentimento é esse, visto que, pela própria opacidade atualmente característica (e indesejável) do mercado, dificilmente seriam atendidas as especificidades relacionadas a essa base legal, dispostas no art. 5º, XII, da LGPD, quais sejam: um consentimento

[47] THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC). op. cit.

cedido de forma livre, informada e inequívoca, destinado a uma finalidade determinada.[48]

Em verdade, caso as informações fornecidas aos titulares tenham conteúdo enganoso ou abusivo,[49]em discordância com os parâmetros mencionados, pode arrastá-lo à uma cadeia interminável de compartilhamento e utilização, sem a sua real concordância, o que ensejaria a nulidade do consentimento.[50]

Outro relatório mais recente,[51] publicado em 2020, e originado de uma investigação realizada pelo Information Commissioner Office (ICO) contra as empresas Experian, Equifax e TransUnion, traz uma lição importante de que deve ser exigida uma base legal clara, bem como que os dados pessoais oferecidos devem estar em conformidade com a legislação de proteção de dados, antes de ser executado um serviço de corretagem. Segundo Elizabeth Denham, Diretora da ICO, a investigação teria revelado "falhas generalizadas e sistêmicas de proteção de dados em todo o setor", além de "falhas significativas de proteção de dados em cada empresa". Embora não seja de natureza vinculativa, o relatório também estabeleceu padrões relativos ao uso de informações das pessoas, destacando os princípios gerais de transparência adequada, justiça e legalidade.

Ressalte-se, entretanto, que se tratando muitas vezes de uma relação de consumo, em que a liberdade é relativizada, não se pode falar em protagonismo da vontade como principal fonte obrigacional.[52]

Nesse sentido, atualmente muitas corretoras de dados se valem de outra base legal para execução de seus serviços, o legítimo interesse, previsto no art. 7º, XI, da LGPD. Essa base legal é a mais contenciosa[53] em sua aplicação, devendo ser lida em

---

[48] COSTA, Inês da Silva. A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. *Revista Electrónica de Direito*. RED, v. 24, n. 1, p. 33-82, 2021.

[49] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: Estudos sobre as bases legais dos artigos 7º e 11.In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, 2021. Cap.06. p. 124.

[50] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario, 2020. op cit., p.124

[51] INFORMATION COMMISSIONER 'S OFFICE (ICO). Investigation into data protection compliance in the direct marketing data broking sector. 2020. Disponível em: https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf . Acesso em: 19 maio. 2021.

[52] VERBICARO, Dennis. VIEIRA, Janaína. op. cit.

[53]BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, 2021. Cap.08. p. 164.

conjunto com o art. 10 do mesmo diploma legal, tendo como fio condutor[54] o balanceamento entre o *interesse legítimo* de quem faz uso das informações e as *legítimas expectativas* dos titulares de dados. A Serasa Experian, que desde de 2007 faz parte do Grupo Experian, uma das maiores agências de crédito do mundo, deixa clara a hipótese de utilização dessa base legal em sua página de perguntas frequentes, ao responder o questionamento "Por que a Serasa Experian pode tratar os meus dados se eu não forneci o consentimento?".[55]

No entanto, para possibilitar o uso adequado de tal base legal, é necessário que seja realizado Teste de Legítimo Interesse (ou Legitimate Interests Assessment – LIA). Inspirado pela Opinion 06/24 do Grupo de Trabalho do Artigo 29,[56] o teste é composto por quatro fases que, diante do desenho normativo da LGPD e do princípio de *accountability*, devem ser documentadas.[57] As fases podem ser sistematizadas da seguinte forma:[58] a) Verificação da legitimidade do interesse: situação concreta e finalidade legítima (art. 10, *caput* e I da LGPD); b) Princípio da necessidade: minimização (art.10, §1º, da LGPD); c) Balanceamento: impactos sobre o titular dos dados e legítimas expectativas (art.10, II, da LGPD); d) Salvaguardas: transparência e minimização dos riscos ao titular do dado (art. 10, §§2º e 3º da LGPD).

Dessa forma, a simples alegação de que a atividade de uma corretora de dados estaria abarcada por tal base legal não seria suficiente, sendo necessária a comprovação da *legitimidade* da operação, por meio de apresentação da documentação dos processos realizados. Inclusive, na ocorrência de um tratamento a partir do legítimo interesse, a Autoridade Nacional de Proteção de Dados (ANPD) pode solicitar relatório de

[54]BIONI, Bruno Ricardo, 2020. op cit.

[55]A Serasa aponta que "O consentimento, ou seja, a autorização expressa do titular, é uma das hipóteses que legitimam o tratamento de dados pessoais, mas não é a única. Existem outras nove hipóteses que podem ser utilizadas como base legal para justificar o tratamento conforme a finalidade e a utilização dos dados, como a proteção do crédito ou o legítimo interesse, por exemplo. Nesses casos, desde que o tratamento seja feito conforme determina a LGPD, principalmente quanto ao cumprimento dos princípios e dos direitos do titular, não há necessidade de autorização expressa do titular". Ver: https://www.serasaexperian.com.br/lgpd/#:~:text=Por%20se%20tratar%20de%20uma,o%20tratamento%20dos%20dados%20positivos. Acesso em: 14 de maio. 2021.

[56]ARTICLE 29 DATA PROTECTION WORKING PARTY .Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014. Disponível em: https://www.dataprotection.ro/servlet/ViewDocument?id=1086. Acesso em: 19 maio. 2021.

[57]BIONI, Bruno Ricardo, 2020. op cit., p.172.

[58]BIONI, Bruno Ricardo, 2020. op cit., p.236

impacto à proteção de dados pessoais, sendo possível que a operação seja revista (art. 10, §3º, da LGPD).

Diante da dinâmica de mercantilização de dados, que coloca os titulares em situações de assimetria informacional quanto ao fluxo de seus dados,[59] o cuidado com a sua participação ativa deve ser também observado. Para possibilitar essa participação, é importante que o direito de oposição seja assegurado de forma clara e transparente. No caso de consentimento, o direito de oposição é potestativo,[60] podendo ser exercido a qualquer momento, por procedimento gratuito e facilitado (art. 8, §5º, da LGPD). Por sua vez, no caso do legítimo interesse, por meio de uma interpretação sistemática dos arts. 10, II e §2º, e 18, §2º, rechaçando uma assimetria normativa entre bases legais,[61] o titular também pode se opor ao tratamento realizado pelas corretoras, de modo que permita a manutenção das suas legítimas expectativas.

Por fim, ratifica-se que apesar de não ser um mercado ilícito *per si*, como será demonstrado no tópico abaixo, o tipo de vantagem social que os data brokers podem obter nesse mercado *deve* ser contrabalanceado com a proteção de direitos fundamentais combinado à parâmetros de transparências e razoabilidade, tornando fundamental a aplicação da LGPD.

3.2. Os deveres aplicáveis aos corretores de dados e o princípio da boa-fé

Em 2014, ocorreu o julgamento do Recurso Especial 1.419.697/RS, objeto da primeira audiência pública da história do STJ, para a consolidação do entendimento sobre a natureza dos sistemas de *scoring* e a possibilidade de violação a princípios e regras do Código de Defesa do Consumidor, capaz de gerar indenização por dano moral. Nesse contexto, o ministro Paulo de Tarso decidiu no sentido de que os sistemas de pontuação de crédito constituem uma *prática comercial lícita*, autorizada pelo art. 5o, IV, do Código de Defesa do Consumidor (CDC), e pelo art. 7o, I, da Lei do Cadastro Positivo. No entanto, apesar de lícita, essa prática deve ser tratada com o

[59]TEFFÉ, Chiara Spadaccini de; VIOLA, Mario, 2020. op cit.
[60]BIONI, Bruno Ricardo, 2020. op cit., p.173
[61]BIONI, Bruno Ricardo, 2020. op cit., p.175

máximo de transparência e boa-fé na relação com os consumidores, aplicando-se os princípios estabelecidos nos mesmos diplomas legais mencionados.

A decisão destacou que a utilização do sistema de pontuação de crédito por uma pessoa jurídica implica, necessariamente, em assumir obrigações e deveres básicos, como, por exemplo, a obrigação de informar quais dados foram utilizados para composição do *score*, se houver requerimento do consumidor.[62] Ainda, segundo o acórdão, a violação aos limites legais na utilização do sistema de *credit scoring*, pode ocasionar em abuso de direito (art. 187 do CC), ensejando a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais, nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3o, § 3o, I e II, da Lei n. 12.414/2011).

O precedente do STJ - que extrapola os limites específicos do *credit scoring* e se apresenta como um *leading case* para futuros casos sobre usos de dados, algoritmos e decisões automatizadas - estipulou alguns princípios balizadores que devem servir de parâmetro no desenvolvimento da atividade de corretagem de dados, tais como, veracidade, clareza, transparência, uso de informações não excessivas, além da já mencionada vedação ao uso de informações sensíveis.[63]

O direito aplicado aos corretores e reguladores de dados deve ser inspirado por essa discussão feita pelo Ministro Paulo de Tarso, haja vista que se reconheceu a ideia de que eles devem operar dentro de parâmetros políticos e éticos, combinando o CDC e Lei do Cadastro Positivo na época, sendo primordial agora a harmonização também com a LGPD. Como lembrado por Laura Schertel Mendes e Gabriel Soares da Fonseca na discussão sobre os limites materiais e contextuais da proteção de dados pessoais, a LGPD condiciona a legitimidade e a legalidade do tratamento de dados à observância da boa-fé (art. 6.º, caput) vedando que ele ocorra "mediante vício de consentimento" (art. 8.º, § 3.º), ou que tenha "fins discriminatórios, ilícitos ou abusivos" (art. 6.º, IX).[64]

---

[62] ZANATTA, 2021, p. 528-529.

[63] ZANATTA, Rafael. *Pontuação de Crédito e Direitos dos Consumidores: o desafio brasileiro*. São Paulo: Instituto Brasileiro de Defesa do Consumidor, 2017, p. 15.

[64] MENDES, Laura Schertel; FONSECA, Gabriel. Proteção de dados para além do consentimento: tendências de materialização. In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*.. Rio de Janeiro: Forense, 2021, p. 173.

Há um papel central garantido à boa-fé que orienta toda a dimensão de aplicação dos princípios da LGPD.

Como bem observado por Fabiano Menke e Guilherme Goulart em uma reflexão sobre boa-fé e o direito brasileiro, com especial ênfase à segurança das informações:

> "O princípio da boa-fé objetiva está previsto no art. 4.º, III, do CDC e também no caput do art. 6.º da LGPD, quando esta enumera os princípios de proteção de dados. É preciso lembrar também da importância do Código Civil para a delimitação e limites das funções da boa-fé objetiva, quando a utiliza como apoio de verificação de licitude, de acordo com o art. 187, cânone de interpretação, conforme o art. 113 e cláusula geral dos contratos, no art. 422. Além disso, a boa-fé também é geradora de deveres, sobretudo com a consideração dos chamados deveres anexos e de proteção. É de se notar a importância do direito obrigacional em tais relações, pois, no mais das vezes, o tratamento de dados pessoais é acompanhado da prestação de um serviço ou fornecimento de produto, ou seja, não é o objeto principal da prestação. Assim, os deveres anexos e de proteção são plenamente aplicáveis às relações obrigacionais que envolvem tratamento de dados. Isso significa que há a possibilidade de a prestação principal ser perfeitamente adimplida, mas os deveres de proteção não. Essa relação, diante também do princípio da boa-fé objetiva, constitui um fundamento ético para a atividade, conforme um de seus aspectos. Trata-se de garantir a confiança na relação, no sentido de o sujeito confiar que seus dados serão adequadamente protegidos pelo responsável"[65].

Acima de tudo, é necessário um esforço para que haja direito à transparência e que seja possível identificar a coleta de dados de tratamento. Isso porque, os corretores de dados têm um dever de *accountability* e de explicitação de que, além de operarem com dados que foram coletados licitamente, também não promovem um desvio de contexto de finalidade ou uso. Isso porque, sem estar em consonância com tais parâmetros estabelecidos, um mercado que já é opaco, pode trazer ainda mais riscos, ocasionando em violações aos direitos fundamentais dos titulares dos dados, bem como pode ensejar o perfilamento abusivo e discriminatório, conforme será posteriormente analisado, com a retomada da análise desse precedente.

A aplicabilidade da boa-fé implica que os corretores de dados não podem *abusar do seu direito* ao realizarem o tratamento de dados pessoais e a construção de

[65] MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*.. Rio de Janeiro: Forense, 2021, p. 342.

perfis preditivos para que possam ser negociados.[66] Isso abre um amplo debate sobre aquilo que Sandra Watcher e Brett Mittelstadt chamam de "inferências razoáveis".[67] Um corretor de dados, na posse de um conjunto de informações *online* e *offline*, como, por exemplo, a informação de que uma pessoa faz uso de medicação continuada para ansiedade e que frequenta com assiduidade uma casa de recuperação para adictos, não pode utilizar-se dessa informação para "encaixar a pessoa", por meio de técnicas de *profiling* ou até mesmo de *group profiling*,[68] em uma categoria de "consumidores com alto potencial de vício", negociando o acesso a essa informação, como uma forma de otimizar vendas para uma loja de calçados, ou uma grande revendedora de bebidas alcoólicas.

Mesmo nas informações "tornadas públicas" pelos titulares, que são copiadas e monetizadas aos montes pelos corretores de dados, esse tipo de conduta não poderia ocorrer. A LGPD é explícita ao dizer que, em seu Art. 7°, § 3º, que "o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização".

3.3. Perfilização e tratamento de dados excessivos: ilícito e natureza do dano

Por fim, uma terceira possibilidade de aplicabilidade da Lei Geral de Proteção

---

[66] Para uma discussão teórica sobre boa-fé no direito privado, ver: MARTINS-COSTA, Judith. *A boa-fé no direito privado: critérios para a sua aplicação*. 2. ed. São Paulo: Saraiva, 2018.

[67] No texto "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", escrito por Wachter e Mittelstadt, os autores apontam para a importância de implementação do direito inferências razoáveis, sendo necessário que os controladores de dados justifiquem proativamente suas escolhas de design para análises inferenciais de alto risco. Nesse sentido, também analisando as possibilidades de inferências abusivas, os autores destacam que a coleta de informações sobre jogos de azar, ou mesmo dependência de álcool para gerar publicidade direcionada, por exemplo, pode prejudicar ativamente o titular dos dados. MITTELSTADT, Brent; WACHTER,Sandra. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, Issue 2 . Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em: 19 maio. 2021.

[68]Group profiling é uma categoria de profiling cujo processo é levemente diferente do perfilamento tradicional: a categorização se dá conforme categorias não reconhecidas socialmente. Com base no processamento de dados, e levando em consideração a finalidade deste processamento, o group profiling agrupa os indivíduos em "[...] categorias anteriormente desconhecidas, social e visualmente imperceptíveis com base na análise de dados, sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias." ROUVROY, op cit. Ou seja, são categorias com as quais o próprio indivíduo não conseguiria se identificar, porque só fazem sentido na constância do processamento dos dados e não têm sentido social.

de Dados Pessoais e dos precedentes do Superior Tribunal de Justiça aos corretores de dados é o reconhecimento da pretensão de indenização no caso de tratamento de dados excessivos na perfilização e na modelagem de modelos preditivos.

As raízes desta tese encontram-se não somente na leitura abrangente da decisão do STJ no caso paradigmático do *credit scoring*, mas também encontram amparo em uma primeira decisão da Corte sobre direitos dos consumidores e proteção de dados pessoais.[69] Trata-se de um caso de 1995, relatado pelo ministro Ruy Rosado Aguiar, onde se reconheceu a capacidade de "opressão econômica" no tratamento de dados pessoais sem condições de controle e autodeterminação informativa por parte do consumidor. Disse o ministro Ruy Rosado naquele voto - em um caso onde o Clube de Diretores Lojistas de Passo Fundo tentava minar o art. 43 do Código de Defesa do Consumidor:

> "A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado e ao particular, para alcançar fins contrários à moral ou ao direito, como instrumento de perseguição política ou opressão econômica".[70]

Essa decisão conecta-se com debates contemporâneos da Corte sobre o direito do consumidor de "tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização",[71] porque desse direito "decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o

[69] STJ, Recurso Especial n. 22.337-8/RS, Relator Ministro Ruy Rosado Aguiar, Recorrente Clube de Diretores Lojistas de Passo Fundo, Recorrido José Orivaldo Branco, Quarta Turma do Superior Tribunal de Justiça, 13 de fevereiro de 1995.
[70] STJ, Recurso Especial n. 22.337-8/RS, Relator Ministro Ruy Rosado Aguiar, Recorrente Clube de Diretores Lojistas de Passo Fundo, Recorrido José Orivaldo Branco, Quarta Turma do Superior Tribunal de Justiça, 13 de fevereiro de 1995.
[71] STJ, Recurso Especial Nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 19/11/2019.

direito de acesso aos dados armazenados e o direito à retificação das informações incorretas".[72] Como reconhecido pelo STJ, a "inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade".[73]

Ao analisar o modelo de negócios da empresa Procob, que se apresentava como verdadeiro corretor de dados, a ministra Nancy Andrighi argumentou que "a recorrente se beneficia do compartilhamento de informações e, nessa medida, deve observância ao disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais".[74]

Essa remissão à Lei do Cadastro Positivo (Lei 12.414/2011) é fundamental, considerando que os cadastrados, nessa legislação, possuem alguns direitos claríssimos, como um direito de *imunidade*, no sentido de se *opor ao tratamento de dados excessivos e sensíveis*.[75] E é essa discussão sobre tratamento de dados pessoais com base em informações excessivas (as que não estiverem vinculadas à análise de risco de crédito ao consumidor) que motivou grande parte da discussão do já mencionado Recurso Especial 1419697/RS, julgado pela sistemática dos recursos representativos de controvérsia nos termos do art. 543-C do Código de Processo Civil.[76]

---

[72] STJ, Recurso Especial Nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 19/11/2019.
[73] STJ, Recurso Especial Nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 19/11/2019.
[74] STJ, Recurso Especial Nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 19/11/2019.
[75] Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. (...) § 3º Ficam proibidas as anotações de: I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.
[76] Art. 543-C. Quando houver multiplicidade de recursos com fundamento em idêntica questão de direito, o recurso especial será processado nos termos deste artigo. § 1o Caberá ao presidente do tribunal de origem admitir um ou mais recursos representativos da controvérsia, os quais serão encaminhados ao Superior Tribunal de Justiça, ficando suspensos os demais recursos especiais até o pronunciamento definitivo do Superior Tribunal de Justiça. § 2o Não adotada a providência descrita no § 1o deste artigo, o relator no Superior Tribunal de Justiça, ao identificar que sobre a controvérsia já existe jurisprudência dominante ou que a matéria já está afeta ao colegiado, poderá determinar a suspensão, nos tribunais de segunda instância, dos recursos nos quais a controvérsia esteja estabelecida.

Retomando a análise do precedente, decisão foi clara em definir que a prática comercial de avaliação de risco de crédito (*credit scoring*) é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei do Cadastro Positivo. De acordo com o STJ, na avaliação do risco de crédito, "devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011"[77]. E que, apesar de desnecessário o consentimento do consumidor consultado (não se trata de base de dados de consumo, e sim fórmula matemática), "devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas"[78]. A tese mais importante, no entanto, é a quinta, que diz:

> "O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados"[79]

Avaliando a *ratio decidendi* do precedente, entende-se que o elemento central é a identificação da pretensão de indenização em razão do cometimento do ilícito: o abuso de direito e o uso de informações excessivas na utilização do sistema de *credit scoring*. Se aplicado em casos futuros, especificamente aqueles envolvendo corretores de dados, é possível concluir que constitui ato ilícito o tratamento de dados excessivos pelo *broker*, que infere questões discriminatórias - por exemplo sobre raça - na construção de uma modelagem de perfil e negociação com outras empresas visando influenciar comportamento futuro do titular, para negociação com outras empresas.

O ilícito, nesse sentido, não está na conduta lesiva da perspectiva dos danos materiais ou morais causados e que supostamente deveriam ser explicitados pela parte

[77] STJ, Recurso Especial n. 1419697 RS 2013/0386285-0, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, Segunda Seção, Data de Publicação: DJe 17/11/2014.
[78] STJ, Recurso Especial n. 1419697 RS 2013/0386285-0, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, Segunda Seção, Data de Publicação: DJe 17/11/2014.
[79] STJ, Recurso Especial n. 1419697 RS 2013/0386285-0, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 12/11/2014, Segunda Seção, Data de Publicação: DJe 17/11/2014.

lesada.[80] O ato ilícito está no desrespeito aos limites legais, incluindo a boa-fé,[81] na utilização de técnicas de *profiling* para fins de corretagem de dados. Está na própria utilização de informações excessivas ou sensíveis para essas modelagens estatísticas e técnicas de *group profiling*.

Resgatando o raciocínio do ministro Paulo de Tarso Severino e outros ministros do STJ, pode-se afirmar que a hipótese de ilícito enseja a responsabilidade objetiva com dano presumido. Não é necessário demonstrar aflição, prejuízos materiais ou qualquer outro elemento constitutivo do dano demonstrado.[82] Neste caso, "o dano é considerado *in re ipsa*, isto é, não se faz necessária a prova do prejuízo, que é presumido e decorre do próprio fato e da experiência comum".[83] Essa é uma forma de endereçar o problema, considerando que a proteção de dados pessoais possui uma conexão íntima com os direitos da personalidade,[84] reconhecido na própria LGPD e pelo Supremo Tribunal Federal.

---

[80] "O dano moral tem como causa a violação a um direito subjetivo extrapatrimonial, protegido pelo ordenamento jurídico — no caso do brasileiro pela cláusula geral de tutela da personalidade (arts. 11 a 21 do Código Civil c/c art. 1º, III, da Constituição da República Federativa do Brasil). Logo, para que se fale em dano moral é necessário comprovar qual direito da personalidade foi lesado". SILVESTRE, Gilberto Fachetti; MARCHIORI, Bruna Figueira. As recentes caracterizações do dano moral no Superior Tribunal de Justiça. *Revista de Estudos Empíricos em Direito*, v. 7, n. 3, 2020, p. 227.

[81] Não se trata de amesquinhar a boa-fé, mas sim levá-la a sério. Sobre essa preocupação, ver: "Há que se ter cuidado, na concreção da boa-fé, para que não se cometa o exagero de se valer dessa cláusula geral como um coringa que desempenhe a função de 'salvar', em qualquer situação, a parte que descumpra seus deveres, que eventualmente tenha feito um mal negócio ou que pretenda dela se valer sem maiores fundamentos concretos e robustos que demonstrem a sua violação. É necessário evitar também o vezo da concreção da boa-fé objetiva no âmbito do Código Civil, como se o aplicador estivesse diante de caso em que incide o Código de Defesa do Consumidor. E, mesmo no âmbito do Código de Defesa do Consumidor, há que se ter cuidado para que a decisão judicial não incorra em arbitrariedades. A extravasação desmedida das regras e dos princípios consumeristas, para além das relações de consumo, acaba por prejudicar a própria proteção do consumidor". MENKE, Fabiano. Comentário aos artigos 104 a 185 do Código Civil. In: NANNI, Giovanni Ettore (org.). *Comentários ao Código Civil: direito privado contemporâneo*. São Paulo: Saraiva, 2019. v. 1, p. 198.

[82] Sobre a teoria do dano (o que se entende por dano), pode-se dizer, em linhas gerais, que o Superior Tribunal de Justiça aderiu à tese pacificada no enunciado 456 da V Jornada de Direito Civil: "A expressão "dano" no art. 944 abrange não só os danos individuais, materiais ou imateriais, mas também os danos sociais, difusos, coletivos e individuais homogêneos a serem reclamados pelos legitimados para propor ações coletivas".

[83] STJ, REsp: 640196 PR 2004/0043164-5, Relator: Ministro Castro Filho, Data de Julgamento: 21/06/2005, T3 - TERCEIRA TURMA, Data de Publicação: DJ 01.08.2005 p. 448.

[84] O fato de ser violação de direitos da personalidade reforça o paradigma do dano moral *in re ipsa*. "Toda lesão a um direito da personalidade, independentemente de sensações psíquicas que possa provocar na vítima, é considerada dano moral e, portanto, deve ser compensada". SILVESTRE, Gilberto Fachetti; MARCHIORI, Bruna Figueira. op cit., p. 228.

O conceito prevê a dispensa de prova do efetivo prejuízo a depender da comprovação do direito violado.[85] Como observado por Venceslau Costa Filho e Silvano Flumignan, "a partir da aplicação dessa teoria, definiu-se que o efeito da presunção ocorreria normalmente com a violação de direitos da personalidade. Essa ocorrência gerou a afirmação, cada vez mais frequente, de que seria possível a responsabilidade sem dano",[86] apesar da jurisprudência dominante do Superior Tribunal de Justiça exigir o dano como elemento central no sistema de responsabilidade civil.[87]

Essa será uma grande questão de interpretação da Lei Geral de Proteção de Dados Pessoais, especialmente no seu capítulo de responsabilidade civil. Para além de simplificar a demonstração do dano por meio da modalidade do "dano moral *in re ipsa*",[88] seria possível reconstruir uma teoria do dano à proteção de dados em casos onde há uma espécie de "perda de controle" sobre como determinadas informações passam a ser utilizadas para construção de *perfis* sem qualquer tipo de autorização, conhecimento ou oportunidade de oposição pelo titular do dado?

Esse é precisamente o debate travado no caso "Lloyd *vs* Google" na Suprema Corte do Reino Unido, que discute uma teoria do dano relacionada à *loss of control*. Um desafio maior será a construção de uma teoria do dano, para identificação do ilícito, ao invés do atalho ao dano presumido, que não exige sua explicitação.

---

[85] Segundo civilistas como Cavalieri Filho, a culpa presumida foi o mecanismo encontrado para favorecer a posição da vítima. CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 10. Ed. São Paulo: Atlas, 2012.

[86] FILHO, Venceslau Costa; FLUMIGNAN, Silvano. STJ exige comprovação do dano como pressuposto do dever de indenizar, *Conjur*, 26 de março de 2018. Disponível em: https://www.conjur.com.br/2018-mar-26/direito-civil-atual-stj-exige-comprovacao-dano-indenizacao#_ftn3. Acesso em: 19 maio. 2021.

[87] "A cláusula geral de responsabilidade civil extracontratual subjetiva, de responsabilidade contratual, de responsabilidade objetiva por atividade de risco e de fixação da indenização elegem o dano como figura central. A doutrina concentra a discussão no artigo 944 do Código Civil, que prevê o dano como a medida da indenização. Em relação aos prejuízos suscetíveis de avaliação econômica, não há grandes discussões a respeito do cálculo em virtude da função de equivalência da reparação". FILHO, Venceslau Costa; FLUMIGNAN, Silvano. *op. cit.*

[88] Como diz Cavalieri Filho, "não haveria que se falar em indenização, nem em ressarcimento, se não houvesse o dano. Pode haver responsabilidade sem culpa, mas não pode haver responsabilidade sem dano. Na responsabilidade objetiva, qualquer que seja a modalidade do risco que lhe sirva de fundamento – risco profissional, risco proveito, risco criado etc. – o dano constitui o seu elemento preponderante. Tanto é assim que, sem dano, não haverá o que reparar, ainda que a conduta tenha sido culposa ou até dolosa". CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil.* 10. Ed. São Paulo: Atlas, 2012, p. 70-71.

Um caminho potente - e alternativo - pode ser seguir as trilhas da ministra Nancy Andrighi em sua reflexão sobre a inobservância dos deveres associados ao tratamento que faz nascer para este a pretensão de indenização pelos danos causados. Aqui coloca-se uma relação dinâmica entre direitos e deveres: é responsabilidade do controlador explicitar a licitude do seu tratamento de dados pessoais, identificando a base legal para tratamento de dados e possibilitando o exercício dos direitos dos titulares dos dados pessoais. Falhar nessa tarefa significa fazer nascer a pretensão para indenização de um tipo de dano específico.

Outro caminho interessante a ser explorado é a superação do paradigma ressarcitório (dano e reparação) e um retorno aos modelos de tutela concentrados na remoção do ilícito e na tutela específica direcionada à fazer cessar o ilícito à privacidade e proteção de dados pessoais.[89] O art. 22 e 42 da LGPD, em leitura conjunta com o Código de Processo Civil, abre amplas possibilidades de tutela inibitória para remoção do ilícito, com possibilidades de obrigações de fazer e intervenção judicial nas operações de tratamento de dados pessoais. Optar pela tutela inibitória "significa abrir mão da discussão sobre os danos e sobre a responsabilidade subjetiva nos processos em que o objeto seja a tutela específica do ilícito".[90] Nestes casos, "bastará discutir e provar: (i) a ilicitude da conduta e (ii) a ocorrência, a probabilidade de ocorrência (ou continuidade) de uma (nova) conduta ilícita".[91] É uma forma de sair das armadilhas da demonstração de dano e das modalidades de reparação, olhando "para o futuro" e para a remoção do ilícito (tratamento abusivo de dados pessoais em violação à LGPD).

---

[89] Diz Luiz Guilherme Marinoni: "A ação inibitória se volta contra a possibilidade do ilícito, ainda que se trate de repetição ou continuação. Assim, é voltada para o futuro, e não para o passado. De modo que nada tem a ver com o ressarcimento do dano e, por conseqüência, com os elementos para a imputação ressarcitória – os chamados elementos subjetivos, culpa ou dolo. Além disso, essa ação não requer nem mesmo a probabilidade do dano, contentando-se com a simples probabilidade de ilícito (ato contrário ao direito). Isso por uma razão simples: imaginar que a ação inibitória se destina a inibir o dano implica na suposição de que nada existe antes dele que possa ser qualificado de ilícito civil. Acontece que o dano é uma conseqüência eventual do ato contrário ao direito, os quais, assim, podem e devem ser destacados para que os direitos sejam mais adequadamente protegidos". MARINONI, Luiz Guilherme. Tutela inibitória e tutela de remoção do ilícito. Jus Navigandi, Teresina, ano, v. 8, 2010. Ver também: MARINONI, Luiz Guilherme. Do processo civil clássico à noção de direito a tutela adequada ao direito material e à realidade social. *Revista de Direito Processual Civil*, Curitiba, v. 8, n. 30, p. 763-789, 2003.

[90] ZANETI JR, Hermes; ALVES, Gustavo Silva; LIMA, Rafael De Oliveira. A tutela específica contra o ilícito (art. 497, parágrafo único, CPC/2015) nas ações coletivas em defesa do consumidor. *Revista de Direito do Consumidor*, v. 110, 2017, p. 418.

[91] ZANETI JR, Hermes; ALVES, Gustavo Silva; LIMA, Rafael De Oliveira. *op. cit.*, p. 418.

4. Conclusão

Os corretores de dados são agentes econômicos de grande destaque pelo seu porte e por suas funções de reutilização e revenda de informações pessoais e capacidade de perfilização e análise preditiva de comportamentos na economia "datificada" deste século. Apesar de sua relativa opacidade e desconhecimento pelo público, são empresas que estão, há alguns anos, na mira dos reguladores e da comunidade internacional de proteção de dados pessoais.

A aplicabilidade da LGPD para os corretores de dados poderá gerar efeitos semelhantes àqueles que surgiram com o advento da legislação canadense de proteção de dados, em que algumas poucas empresas "fecharam as portas" diante da impossibilidade de demonstração de conformidade ou *compliance* com as leis. A grande maioria, no entanto, manteve e mantém um discurso de "ética dos dados" e de "respeito às leis de proteção de dados", apesar das muitas dúvidas sobre a licitude de diversas práticas de categorização, perfilização e modelagem estatística com fins de modulação do comportamento futuro das pessoas.

Além da problemática mais evidente da identificação das bases legais para tratamento de dados - um requisito legal tido como primário na LGPD -, as práticas de usos abusivos de dados pessoais e as inferências "não razoáveis" em técnicas de perfilização podem constituir abuso de direito e violação dos deveres de boa-fé, lançando uma discussão sobre ilícito. A identificação do ilícito nesses mercados, por sua vez, abre a discussão sobre responsabilidade e danos morais *in re ipsa*, na esteira da decisão paradigmática de 2014 no STJ sobre *credit scoring*, ou a tutela inibitória.

A verdadeira aplicabilidade da Lei Geral de Proteção de Dados Pessoais vai muito além de uma simples leitura de como a LGPD impacta a atividade das empresas desse segmento intensivo em dados, partindo de uma leitura isolada da legislação em si. A força normativa do direito aplicado aos corretores de dados advém do diálogo das fontes, da leitura integrada da LGPD com o Código Civil e Código de Defesa do Consumidor, e da correta interpretação dos bons precedentes já construídos pelo Superior Tribunal de Justiça no Brasil.

5. Referências Bibliográficas

ABBOTT, Jordan. Time to Build a National Data Broker Registry - The New York Times, Opinion. 2019. Disponível em: https://www.nytimes.com/2019/09/13/opinion/data-broker-registry-privacy.html. Acesso em: 20 abr. 2021.

ALOWAIRDHI, Abdullah; MA, Xiaogang. Data Brokers and Data Services, in: SCHINTLER, L; MCNEELY, C (ed.). *Encyclopedia of Big Data*. New York: Springer, 2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY .Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014. Disponível em: https://www.dataprotection.ro/servlet/ViewDocument?id=1086. Acesso em 19 maio. 2021.

BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional.In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, 2021. Cap.08. p. 163-176.

BRESSAN, Stephane. LEE, Thomas. Information Brokering on the World Wide Web. *WebNet 97 World Conference*, 1997. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/2663/SWP-3963-37617980-CISL-9708.pdf?sequence=1. Acesso em: 19 maio. 2021.

CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil.* 10. Ed. São Paulo: Atlas, 2012.

CHRISTL, Wolfie. Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. 2017. Cracked Labs. Disponível em: http://crackedlabs.org/en/corporate-surveillance. Acesso em: 20 abr. 2021.

COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. 2013. Staff Report For Chairman Rockefeller. p. 36 Disponível em: https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. Acesso em: 19 maio. 2021.

COSTA, Inês da Silva. A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. *Revista Electrónica de Direito*. RED, v. 24, n. 1, p. 33-82, 2021.

FEDERAL TRADE COMMISSION (FTC). Data Brokers: A Call for Transparency and Accountability. 2014. Disponível. em: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Acesso em: 19 maio. 2021.

FEDERAL TRADE COMMISSION (FTC). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Business and Policymakers. 2012. Disponível em: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers . Acesso em: 19 maio 2021.

FILHO, Venceslau Costa; FLUMIGNAN, Silvano. STJ exige comprovação do dano como pressuposto do dever de indenizar, *Conjur*, 26 de março de 2018. Disponível em: https://www.conjur.com.br/2018-mar-26/direito-civil-atual-stj-exige-comprovacao-dano-indenizacao#_ftn3. Acesso em: 19 maio. 2021.

HILDEBRANDT, M. Defining Profiling. A New Type of Knowledge? In.: Hildebrandt, M.; Gutwirth, S. (Org.) Profiling the European Citizen: Cross-Disciplinary Perspectives. Cham/SWI: Springer Science, p. 17-44.

HOSNI, David Salim Santos. MARTINS, Pedro Bastos Lobo. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. Internetlab. In.: Revista Internet & Sociedade, vol. 1, n.2. 2020. Disponível em: https://revista.internetlab.org.br/736-2/. Acesso em: 19 maio. 2021.

INFORMATION COMMISSIONER 'S OFFICE (ICO). Investigation into data protection compliance in the direct marketing data broking sector. 2020. Disponível em: https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf. Acesso em 19 maio. 2021.

LATTO, Nica. Data Brokers: Everything You Need to Know. AVAST. 2021. Disponível em: https://www.avast.com/c-data-brokers. Acesso em: 20 abr. 2021.

LAWSKY, David. Google closes DoubleClick merger after EU approval. Reuters. 2008. Disponível em: https://www.reuters.com/article/us-google-doubleclick-eu-idUSBFA00058020080311. Acesso em: 13 maio. 2021.

MARINONI, Luiz Guilherme. Do processo civil clássico à noção de direito a tutela adequada ao direito material e à realidade social. *Revista de Direito Processual Civil*, Curitiba, v. 8, n. 30, p. 763-789, 2003.

MARTINS-COSTA, Judith. *A boa-fé no direito privado: critérios para a sua aplicação*. 2. ed. São Paulo: Saraiva, 2018.

MENDES, Laura Schertel; FONSECA, Gabriel. Proteção de dados para além do consentimento: tendências de materialização. In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 73-95.

MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021, p. 339-359.

MENKE, Fabiano. Comentário aos artigos 104 a 185 do Código Civil. In: NANNI, Giovanni Ettore (org.). *Comentários ao Código Civil: direito privado contemporâneo*. São Paulo: Saraiva, 2019.

MITTELSTADT, Brent; WACHTER,Sandra. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, Issue 2 . Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em: 19 maio. 2021.

ROUVROY, A. Of data and Men. Fundamental Rights of Freedoms in a World of Big Data. Council of Europe, Directorate General of Human Rights and Rule of Law, 2016, vol.T-PD-BUR. p. 1-37.

SAMPAIO, Alice Castaldi. *Data Brokers: um novo modelo de negócios baseado em vigilância de dados*. Dissertação de Mestrado*f*. Universidade Estadual de Campinas, 2017.

SHERMAN, Justin. Data Brokers Are a Threat to Democracy. Wired. 2021. Disponível em: https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/. Acesso em: 13 maio. 2021.

SILVEIRA, Sergio Amadeu da; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. *Liinc em Revista*, v. 12, n. 2, p. 217-230, 2016.

SILVEIRA, Sergio Amadeu da. *Tudo sobre tod@ s: Redes digitais, privacidade e venda de dados pessoais*. São Paulo: Edições Sesc, 2017.

SILVESTRE, Gilberto Fachetti; MARCHIORI, Bruna Figueira. As recentes caracterizações do dano moral no Superior Tribunal de Justiça. *Revista de Estudos Empíricos em Direito*, v. 7, n. 3, 2020, p. 221-237.

SINGER, Natasha. Mapping and Sharing the Consumer Genome, The New York Times, 16 de Jun., 2012. Disponível em: https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html. Acesso em: 19 maio. 2021.

STJ, Recurso Especial n. 22.337-8/RS, Relator Ministro Ruy Rosado Aguiar, Recorrente Clube de Diretores Lojistas de Passo Fundo, Recorrido José Orivaldo Branco, Quarta Turma do Superior Tribunal de Justiça, 13 de fevereiro de 1995.

STJ, Recurso Especial Nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 19/11/2019.
STJ, REsp: 640196 PR 2004/0043164-5, Relator: Ministro Castro Filho, Data de Julgamento: 21/06/2005, T3 - TERCEIRA TURMA, Data de Publicação: DJ 01.08.2005, p. 448.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: Estudos sobre as bases legais dos artigos 7º e 11.In: BIONI, Bruno et al (org.). *Tratado de proteção de dados pessoais*. São Paulo: Forense, 2021. Cap.06. p.117-148.

THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC). On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship. 2006. Disponível em: https://cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf. Acesso em: 19 maio. 2021.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. *Revista de Direito do Consumidor*. vol. 134. ano 30. p. 195-226. São Paulo: Ed. RT, mar./abr. 2021. Acesso em: 19 maio. 2021.

ZANATTA, Rafael. Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, in: MIRAGEM, Bruno; LIMA MARQUES, Claudia; MAGALHÃES, Lucia Ancona, *Direito do Consumidor: 30 anos do CDC. Da consolidação como direito fundamental aos atuais desafios da sociedade*. Rio de Janeiro: Forense, 2021.

ZANATTA, Rafael. *Pontuação de Crédito e Direitos dos Consumidores: o desafio brasileiro*. São Paulo: Instituto Brasileiro de Defesa do Consumidor, 2017.

ZANETI JR, Hermes; ALVES, Gustavo Silva; LIMA, Rafael De Oliveira. A tutela específica contra o ilícito (art. 497, parágrafo único, CPC/2015) nas ações coletivas em defesa do consumidor. *Revista de Direito do Consumidor*, v. 110, 2017, p. 389-422.