



UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

LUÍSA CAMPOS FARIA

IMPACTOS DO BIG DATA E DAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS
NAS ANÁLISES ANTITRUSTE

Brasília, 2019

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

LUÍSA CAMPOS FARIA

IMPACTOS DO BIG DATA E DA LEI GERAL DE PRODUÇÃO DE DADOS NAS
ANÁLISES ANTITRUSTE

Monografia apresentada como
requisito parcial à obtenção do grau
de Bacharela em Direito pela
Faculdade de Direito da
Universidade de Brasília – UnB.
Orientadora: Profa. Dra. Amanda
Athayde Linhares Martins Rivera

Brasília, 2019

TERMO DE APROVAÇÃO

LUÍSA CAMPOS FARIA

IMPACTOS DO BIG DATA E DA LEI GERAL DE PRODUÇÃO DE DADOS NAS
ANÁLISES ANTITRUSTE

Monografia apresentada como requisito parcial à obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.
Orientadora: Profa. Dra. Amanda Athayde Linhares Martins Rivera

Brasília, 28 de junho de 2019.

Profa. Dra. Amanda Athayde Linhares Martins Rivera

Professora Orientadora

Profa. Izabella de Menezes Passos Barbosa

Membro da banca examinadora

Prof. Angelo Gamba Prata de Carvalho

Membro da banca examinadora

RESUMO:

A sociedade, especialmente nos últimos 20 anos, tem experimentado uma revolução tecnológica, que permitiu uma mudança radical na velocidade com que a informação é produzida, bem como um substancial aumento no volume de dados disponíveis, diariamente produzidos por milhões de pessoas ao redor do mundo. Tais dados, desse modo, passaram a ser utilizados e analisados para assunção de fins econômicos. Nesse sentido, houve uma concomitante mudança na dinâmica de competição dos mercados, que exigiu uma modificação na abordagem tradicionalmente realizada pelas autoridades antitruste. Este trabalho visa, nesse ínterim, elencar as principais transformações e conceitos da era do Big Data, além de explorar a legislação atinente à proteção dos dados pessoais, de maneira a demonstrar como estão resguardados os usuários. Por meio de um *overview* de relevantes artigos sobre o tema, bem como de análise referente à atuação das autoridades em duas operações atinentes aos *data-driven markets* - a mais antiga e recente finalizadas até o momento -, busca-se discutir possíveis abordagens e *standards* a serem considerados nas análises de mercados com características informacionais, especificamente com relação às análises levadas a cabo quando da efetivação do controle de estruturas. Ademais, quanto ao controle de condutas, busca-se abordar os principais ilícitos envolvendo dados já identificados. Ainda que tais ilícitos não tenham sido objetos de manifestação por parte das autoridades, a academia se debruça acerca dos principais pontos relacionados a esses mercados, pontos sobre os quais será feita pequena digressão.

Palavras-Chave: Antitruste; Big Data; Dados pessoais; Controle de Estruturas, Controle de condutas.

ABSTRACT:

Society, especially in the last 30 years, has experienced a technological revolution that has allowed for a radical change in the speed with information is produced, as well as a substantial increase in the volume of available data, that are daily produced by millions of people around the world. These data were then used and analyzed for the assumption of economic purposes. In this sense, there has also been a concomitant change in the competitive dynamics of the markets, which requires a change in the approach traditionally carried out by the antitrust authorities. This work aims, in the interim, to list the main changes and concepts of the Big Data era, as well as to explore the legislation regarding the protection of personal data produced, in order to demonstrate how users are safeguarded. Through an overview of relevant articles on the subject, as well as an analysis of the performance of the authorities in two operations related to data-driven markets - the oldest and most recently completed so far -, it is sought to discuss possible approaches and standards to be considered in the analysis of markets with informational characteristics, specifically with regard to the analyzes carried out when the control of structures was carried out. In addition, regarding the control of conducts, it is tried to approach the main illicit ones involving data already identified. Although such acts have not been the object of demonstration by the authorities, the academy is concerned with the main points related, and on which will be made a small digression.

Keywords: Antitrust; Big data; Personal data.

SUMÁRIO

INTRODUÇÃO.....	8
CAPÍTULO 1 - PROTEÇÃO DE DADOS E DIREITO ANTITRUSTE.....	9
1.1 - Big Data e a sociedade em rede.....	9
1.2 – O contexto internacional de proteção aos dados	12
1.2.1 – General Data Protection Regulation (GDPR) na Europa.....	13
1.2.2 – A Lei Geral de Proteção de Dados (LGPD) no Brasil.....	14
1.3 – O antitruste e as legislações acerca da proteção de dados: repercussões em estruturas e condutas	20
CAPÍTULO 2 - PROTEÇÃO DE DADOS E CONTROLE DE ESTRUTURAS	26
2.1 – O conceito de <i>data-opolies</i>	26
2.2 – Dados como ativos das empresas.....	29
2.3 - Proteção de dados como diferencial competitivo das empresas.....	30
2.4 – Critérios de notificação de Atos de Concentração e Big Data.....	33
2.5 - Risco de perda de inovações e demais problemas ligados às <i>data-driven companies</i>.....	37
2.7 - Aquisições estratégicas de empresas como instrumento de obtenção de bases de dados e a evolução da análise pela autoridade europeia: Do caso Google/Doubleclick ao caso Apple/Shazam.....	38
2.7.1 – Operação Google/Doubleclick	39
2.7.2 – Operação Apple Music/Shazam (2018).....	46
CAPÍTULO 3 - PROTEÇÃO DE DADOS E CONTROLE DE CONDUTAS	55
3.1 – A discricionarietà e a avaliação do conjunto probatório em condutas concorrenciais	55
3.2 – Condutas tradicionais na era do Big Data e as mudanças que devem ser objeto de atenção pelo antitruste.....	57
3.2.1 – Formação de cartel com computador como mensageiro	58
3.2.2 – Formação de cartel Hub and Spoke.....	59
3.2.3 – Formação de cartel baseado num agente previsível pela dinâmica do mercado	61
3.2.4 – Formação de cartel baseado na autonomia da máquina.	62
3.3 – Possíveis novas condutas na era do Big Data e o papel do antitruste.....	63

3.3.1 – <i>Data Breaches</i>	63
CONCLUSÃO.....	67
BIBLIOGRAFIA.....	69

INTRODUÇÃO

A sociedade informacional, cujas dinâmicas sociais acabaram sendo modificadas em razão da ampliação da quantidade e velocidade na produção e disseminação de informações acabou por impactar todas as relações, das sociais às econômicas. Nesse sentido, como forma de agregar valor e possibilitar a maximização dos lucros, nos últimos 20 anos diversas foram as empresas que surgiram e se especializaram em tal seara, de modo com que verdadeiros gigantes surgiram a partir da exploração da atividade informacional, como é o caso do Google e do Facebook.

A atividade econômica, nesse sentido, passou a monetizar a produção de dados massivos de um modo nunca antes imaginado, bem como a competir pela atenção das pessoas. Além disso, a massiva distribuição de informações também possibilitou que fossem contornadas algumas falhas de mercado, surgindo diversas plataformas capazes de diminuir os custos de transação em vários mercados, promovendo uma nova dinâmica em diversos setores.

Com a mudança na atividade empresarial e o surgimento de novos fatores a serem considerados nas interações concorrenciais, o Direito Antitruste viu-se obrigado a refletir sua atuação, vez que uma nova resposta passou a ser necessária a fim de mitigar problemas concorrenciais e possíveis danos aos consumidores e demais agentes em alguns mercados. Nesse contexto, a partir de uma revisão dos conceitos ligados ao Big Data e às *data-driven organizations* (ou, em bom português, as empresas que compõe a Economia Moviada a Dados), bem como a partir da revisão da obra de autores que tratam sobre o tema, busca-se, neste trabalho, mencionar e tratar de alguns conceitos que podem ensejar *standards* mínimos a serem considerados pelas autoridades antitruste quando da análise de operações envolvendo as *data-driven organizations*.

Ademais, busca-se ainda traçar um panorama geral das possíveis condutas já exaradas por algumas companhias ou já previstas como possíveis no meio acadêmico, de maneira analisar as agora mais amplas possibilidades apresentadas às empresas para consecução de ilícitos.

CAPÍTULO 1 - PROTEÇÃO DE DADOS E DIREITO ANTITRUSTE

1.1 - Big Data e a sociedade em rede.

A transição do século XX para o século XXI, para além de uma mera mudança entre séculos, entre os números que marcam os anos terrestres, trouxe uma profunda mudança da ordem social: do internet boom¹ do final dos anos 90 até os dias atuais, a sociedade experimenta uma revolução na maneira e na velocidade com que a informação é repassada, de modo com que esta tem se tornado cada vez mais central em nossa sociedade – e, por isso, tem adquirido cada vez mais valor econômico.

Em artigo, Manuel Castells discorda da denominação de sociedade de informação², em razão de que, segundo seu entendimento, a sociedade sempre foi pautada pela informação. A mudança havida e introduzida junto com as novas tecnologias, em seu entendimento, dizem respeito à organização da sociedade em rede. Nesse sentido, tais sociedades, embasadas em novas tecnologias, conseguem a um só tempo serem mais flexíveis e adaptáveis a novas realidades, além de mais complexas e eficientes.

A Organização para Cooperação e Desenvolvimento Econômico (OCDE) em 2014 já reconhecia a mencionada importância dos dados, e produziu um relatório sobre

¹ VARIAN, Hal R.; FARRELL, Joseph; SHAPIRO, Carl. “The economics of information technology: an introduction”, Chapter 1. Cambridge University Press, 2004. Disponível em: <
<https://books.google.com.br/books?id=LpgoKtzhVEC&pg=PA5&dq=The+economics+of+information+technology:+an+introduction+internet+boom&hl=pt-BR&sa=X&ved=0ahUKewju76mZkLLhAhWsj7kGHSbfD1sQ6AEIKTAA#v=onepage&q=The%20economics%20of%20information%20technology%3A%20an%20introduction%20internet%20boom&f=false>>.

² “A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. A rede é a estrutura formal (vide Monge e Contractor, 2004). É um sistema de nós interligados. E os nós são, em linguagem formal, os pontos onde a curva se intersecta a si própria. As redes são estruturas abertas que evoluem acrescentando ou removendo nós de acordo com as mudanças necessárias dos programas que conseguem atingir os objectivos de performance para a rede. Estes programas são decididos socialmente fora da rede mas a partir do momento em que são inscritos na lógica da rede, a rede vai seguir eficientemente essas instruções, acrescentando, apagando e reconfigurando, até que um novo programa substitua ou modifique os códigos que comandam esse sistema operativo”. CASTELLS, Manuel. “A sociedade em Rede: do Conhecimento à política”. Imprensa Nacional, 2005.

o tema³, ocasião em que, de início, trataram da natureza desse recurso e dos principais modos com que este poderia vir a ser economicamente explorado:

“The economic properties of data suggest that data is an infrastructural resource which in theory can be used by an unlimited number of users and for an unlimited number of purposes as an input to produce goods and services. The increasing returns to scale and scope, that the use of data generates, are at the origin of data-driven productivity growth realised by firms when data is used for e.g. the development of multi-sided markets, in which the collection of data on one side of the market enables the production of new goods and services on the other side(s) of the market (e.g. the use of data generated by social network services for advertisement purposes).

The value-creation mechanisms of data analytics, which include using data analytics to:

- Gain insights (knowledge creation): Data analytics are the technical means to extract insights and the empowering tools to better understand, influence or control the data objects of these insights (e.g. natural phenomena, social systems, individuals). For example, organisations increasingly rely on simulations and experiments not only to better understand the behaviour of individuals, but in order to better understand, assess, and optimize the possible impact of their actions on these individuals.

- Automate decision-making (decision automation): Data analytics (through machine learning algorithms) empower autonomous machines and systems that are able to learn from data of previous situations and to autonomously make decisions based on the analysis of these data. These autonomous machines and systems are getting more and more powerful as they can perform an increasing number of tasks that required human intervention in the past. Google’s driverless car is an illustrative example which is based on machine learning algorithms enriched by data that is collected from the sensors connected to the car and from services such as Google Maps and Google Street View.”

Hoje, todos os dias são produzidas imensas quantidades de informações - de dados -, e são diversas as empresas que adquirem vultosos lucros a partir da exploração

³ Fonte: DATA-driven Innovation for Growth and Well-being interim synthesis Report. October, 2014. Disponível em: <http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf>. Acesso em 12 de fevereiro de 2019.

e da monetização de dados produzidos por terceiros⁴: por exemplo, para além dos usos relatados no trecho supratranscrito, algumas empresas de tecnologia oferecem serviços gratuitos e úteis aos usuários, extraíndo lucro a partir de um direcionamento comercial de propaganda a estes, direcionamento este que é feito a partir dos dados produzidos pelos próprios usuários quando utilizam seus serviços⁵ - é o caso do Google e do Facebook. Às empresas que utilizam esse modelo de negócio, baseado na captação e monetização de dados pessoais fornecidos por seus usuários, chamamos de *data-driven organizations*⁶.

Faz-se necessário mencionar que um conceito bastante ligado às *data-driven organizations* é o de *Attention Markets*⁷. Nesse sentido, importante ressaltar o quanto a

⁴ Fonte: <<https://link.estadao.com.br/blogs/codigo-aberto/o-produto-e-voce/>> Acesso em 4 de março de 2019

⁵ “We live in a world where a large portion of online content is free. We do not pay to search on Google or Bing, post our photos on Facebook or MySpace, or read the latest news on CNN.com or FoxNews.com. Apps like Angry Birds are available for free in Apple’s and Google’s app stores. Why does everyone give away things online? The answer, in some ways, is that they do not. These businesses (“publishers”) monetize the content they provide for free by selling access to our attention. By collecting more data about their users, publishers can improve their products and target ads more precisely to the consumers who are most likely to respond. Do more searches on Google, and Google learns more about you. Combine your search data with what Google knows from your Gmail and other interactions with Google properties, as well as reports from tracking cookies placed by its display advertising network, and Google has a pretty good idea of what you like.3 Google can use this information to provide you with better search and map results, as well as more relevant ads, both of which will help Google’s bottom line. First, better content makes for a more attractive product, encouraging greater use of Google’s services, increasing both ad revenue and Google’s database of consumer information. 4 Second, the expansion of Google’s database also allows Google to earn more revenue by facilitating targeted ads that are more likely to elicit consumer responses.” PRIVACY AND ANTITRUST: UNDERPANTS GNOMES, THE FIRST AMENDMENT, AND SUBJECTIVITY James C. Cooper, George Mason University School of Law, Law and Economics Center George Mason Law Review, Forthcoming George Mason University Law and Economics Research Paper Series 13-39.

⁶ “[...] a data driven organisation is an organization where business decisions makers are given the power to explore and access data independently, not just about seeing a few canned reports at the beginning of every day or every week, they need to be able to ask questions and answers received based on the data before decisions are made. Firms that relentlessly measure and monitor the pulse of their business in continuous automated manner are also seen as data-driven.” Becoming a Data Driven Organization: The Handbook - Mirko Peters, 2018. BoD Norderstedt – Germany.

⁷ “We have brains with a limited capacity to process information, and we exist in an environment limited by time – 168 hours per week. Our brains are presented with too much information (by the sense organs) for the brain to process (ten million bits per second, by one estimate).”. WU, Tim. Blind Spot: The Attention Economy and the Law. Antitrust Law Journal, 2017. p. 11 “In this paper, I refer to the business model of attention resale as “attention brokerage.” In its purest form, these businesses rely solely on the resale of attention to make money. Examples of pure attention brokers includes businesses such as broadcast television networks, free newspapers, and many of the companies on the World Wide Web, like Facebook or Google. In economic terms, the Attention Broker can be described as a specialized version of a platform intermediary in a two-sided market.⁸⁶ In the literature pioneered by economists Jean-Charles Rochet and Jean Tirole, a platform intermediary is a firm that brings together buyers and sellers from two separate markets and facilitates their transactions.⁸⁷ Classic examples include credit card companies, shopping malls, or online firms like eBay. Each facilitates transactions by bringing together groups of buyers and sellers in one place or one format. To facilitate transactions, moreover, the platforms often charge fees to only one side of the market (typically the seller) so as to attract more buyer” Idem, p. 18.

escassa atenção das pessoas tem sido disputada por diversas empresas no mundo, garantindo que a capacidade de que os seres humanos dispendam tempo numa ou outra plataforma ou atividade seja algo economicamente reconhecido, e que tenha valor. As empresas, desta feita, para manterem seu modelo de negócios – em especial as digitais – investem recursos para que cada vez mais a atenção das pessoas seja atraída para seu produto, de maneira com que estas consigam cada vez mais abstrair dados referente às atividades das pessoas, traçando seu perfil e assim sendo capazes de tanto melhor fornecer mais conteúdo quanto eliminar os custos de transação entre fornecedores e consumidores, possibilitando direcionamento de produtos aos mais tendentes e interessados em seu consumo.

Tendo em vista, assim, a importância social e econômica que os dados pessoais adquiriram nos últimos anos, bem como o aumento na produção e na monetização destes dados, mormente realizados pelas grandes empresas de tecnologia, diversos foram os países se sentiram incumbidos a regular a maneira com que os dados pessoais devem ser manipulados.

1.2 – O contexto internacional de proteção aos dados

O tema relativo à proteção de dados foi inicialmente abordado de forma mais profunda em países mais desenvolvidos, mais especificamente nos EUA e nos países que compõem a União Europeia, de maneira com que foi dentro do contexto de tais países que as primeiras discussões, estabelecimento de *standards* e legislações se deram.

A primeira legislação relevante sobre o tema - que inclusive serviu de principal referência para a legislação pátria sobre o tratamento de dados pessoais - foi o General Data Protection Regulation (GDPR), encabeçado pela União Européia. Após 4 anos de debates intensos, iniciados a partir de uma proposta por parte da Comissão Europeia de reforma na anterior lei vigente sobre o tratamento de dados pessoais, o parlamento europeu em 2016 acabou por aprovar a mencionada Lei. O GDPR desse modo passou a vigor a partir de 25 de maio de 2016.

Além de ser uma legislação precursora no tratamento de dados pessoais, o GDPR foi um grande catalisador mundial para que os demais países do mundo se manifestassem a respeito dos dados pessoais, ou seja, para que produzissem suas próprias legislações a respeito do tema. Tal fato se deu em razão de algumas normas

estabelecidas pelo próprio GDPR quando da transferência internacional de dados pessoais pertencentes a cidadãos europeus, ou seja, da regulação acerca da exportação de dados de cidadãos europeus.

Nesse sentido, procurar-se-á, abaixo, traçar o contexto geral e os ditames tanto do GDPR, considerado principal marco referente à regulação da privacidade de dados pessoais, quanto da legislação brasileira, a fim de que possa ser percebida a similaridade entre ambas, e, portanto, o quanto a experiência europeia pode contribuir para a experiência brasileira, e o quanto os julgados a serem analisados trazem boas possibilidades no que tange aos rumos que as autoridades brasileiras podem tomar.

1.2.1 – General Data Protection Regulation (GDPR) na Europa

Em primeiro lugar, a legislação europeia estatui que os direitos e garantias dados aos cidadãos europeus dentro da união europeia devem ser mantidos quando os dados forem transferidos a outros países, ou a empresas pertencentes a outras jurisdições. Dessa forma, a Comissão Europeia prevê que os demais países devam oferecer um marco legal para a proteção de dados que seja adequado e equivalente aos padrões europeus de proteção. Na ausência de legislação sobre o tema, ou na ausência de legislação que seja considerada adequada a garantir a mesma proteção a dados pessoais conferida pela UE, as transferências de dados só podem ocorrer se obedecerem a determinadas circunstâncias, dentre as quais: a partir do consentimento expresso do indivíduo detentor dos dados para local em que a transferência seja imprescindível para a conclusão ou a realização de um contrato, por exemplo.

Além disso, o GDPR estabelece que os usuários tenham direito de saber quais serão armazenados e para qual finalidade, além do tratamento que haverá de ser dado a estes, devendo o este usuário (portanto, o proprietário dos dados pessoais fornecidos) consentir e autorizar o uso. A empresa deve fornecer tais explicações de forma clara e concisa, em linguagem acessível a todos. Além disso, deve ser garantida ao usuário a possibilidade de, a qualquer tempo, revogar a permissão para uso e tratamento de seus dados pessoais, bem como de solicitar a exclusão destes. Ademais, deve ser oferecida ao usuário a possibilidade de migração destes dados para outra empresa, assim como de acesso e de obtenção de cópia dos dados detidos.

O GDPR ainda institui diversas obrigações às empresas que deverão deter os dados pessoais dos cidadãos europeus. Em primeiro lugar, a proteção dos dados deve ser prioritária desde o início do projeto de um sistema, devendo ser conferidos aos dados um tratamento de anonimização (ou seja, devendo estes serem anônimos) ou de pseudonimização (que garante a impossibilidade de identificação do usuário a quem aqueles dados pertencem, de maneira com que para que esta seja possível deva ser também necessário o acesso a outros dados, que só quando somados aos primeiros tornem tal identificação possível - ou seja é necessário um cruzamento de dados para que estes permitam a identificação do usuário).

Outro ponto trazido no âmbito do GDPR diz respeito à obrigação das empresas em possuírem um *Data Protection Officer* (DPO) ou seja, um encarregado por supervisionar o tratamento conferido aos dados pessoais, bem como por produzir uma espécie de relatório anual acerca da proteção dos dados sob tratamento da empresa e de seu impacto. Ademais, também cabe a este executivo, no caso de um incidente envolvendo o vazamento de dados pessoais, a notificação das autoridades competentes em até 72 horas após o ocorrido.

Vale citar ainda que o GDPR é acompanhado pela vigência de um normativo, de título *ePrivacy Regulation*. Como função precípua, tal normativo revoga uma diretiva de 2002 (a denominada *ePrivacy Directive*), e particulariza e complementa alguns dos pontos tratados no GDPR, dentre os quais aqueles ligados à confidencialidade, ao uso de *cookies*, e outros.⁸

1.2.2 – A Lei Geral de Proteção de Dados (LGPD) no Brasil

Alguns meses após a entrada em vigência da legislação europeia, o Brasil acabou por também editar Lei a fim de regular o tratamento dos dados pessoais - trata-se da Lei 13.709 de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados (LGPD). Entende-se necessário fazer um apanhado geral pouco maior sobre tal legislação, a fim de que seja possível uma maior compreensão a respeito daquilo que esta tutela, e principalmente, de como a regulação dos dados é norteadada no Brasil, e quais são os parâmetros entendidos como importantes na proteção dos usuários e cidadãos.

⁸ Fonte: < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>>. Acesso em 3 de junho de 2019.

Tal legislação de pronto apresenta aquilo que pretende tutelar, que não se restringe à privacidade, mas também à liberdade e autonomia de escolha das pessoas naturais. Além disso, a norma já de início estabelece algumas definições com relação aos termos a serem utilizados ao longo de sua redação, a fim de que se faça completamente compreendida. Estabelece, por exemplo, que dados pessoais são todos aqueles que fornecem informação relacionada à pessoa natural identificada ou identificável. Define ainda como dado pessoal sensível aquele acerca da origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dado genético ou biométrico.

Outro ponto bastante relevante diz respeito à definição responsável por sedimentar a diferença existente entre o titular (pessoa natural a quem se referem os dados pessoais que são objetos de tratamento), o controlador (pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e o operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador) dos dados pessoais, bem como do encarregado (pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;), explicitando que os agentes de tratamento são constituídos pelo operador e controlador. Tais definições são importantes para o amplo e correto entendimento das obrigações estabelecidas ao longo do normativo.

A nossa lei, que muito se inspirou na legislação europeia, estabelece como diretrizes principais da proteção conferida aos dados pessoais (i) o respeito à privacidade; (ii) a autodeterminação informativa; (iii) a liberdade de expressão, de informação, de comunicação e de opinião; (iv) a inviolabilidade da intimidade, da honra e da imagem; (v) o desenvolvimento econômico e tecnológico e a inovação; (vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Outro ponto de relevância acerca da LGPD, diz respeito à exclusão do âmbito de sua tutela do tratamento conferido a dados pessoais que seja realizado (i) por pessoa natural para fins exclusivamente particulares e não econômicos; (ii) para fins exclusivamente jornalístico e artísticos; (iii) para fins acadêmicos ou que (iv) sejam para fins exclusivos ligados à segurança pública; à defesa nacional; à segurança do Estado;

ou às atividades de investigação e repressão de infrações penais. Também são excetuados os dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais considerado adequado.

A Lei brasileira, desta feita, submete a sua disciplina os dados pessoais que estejam de posse de qualquer pessoa física ou jurídica que os utilizem para fins comerciais e econômicos. Muito embora os assuntos referentes aos dados pessoais sempre tragam à mente as grandes empresas de tecnologia, é importante ressaltar que qualquer empresa que detenha dados pessoais de seus clientes está sujeita à tutela da Lei Geral de Proteção de Dados – inclusive aquele pequeno negócio que cadastra o endereço e o telefone de seus usuários, ou que exige o cadastro de sua digital para passar numa catraca. Desta feita, a Lei definiu como princípios norteadores a boa-fé, o princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade e transparência dos dados, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.

Tais princípios têm por função precípua assegurar que o usuário, como titular de seus dados pessoais terá livre acesso a seus dados, que deverão ser tratados de maneira adequada e limitada, no sentido de que só deverão ser tratados os dados considerados imprescindíveis para a realização das finalidades a que se propõe o controlador, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

De forma bastante similar ao pugnado no GDPR tais princípios garantem ainda que as informações a respeito do tratamento conferido aos dados pessoais sejam claras, precisas e acessíveis, garantindo aos titulares exatidão, clareza, relevância e atualização dos dados de acordo com as finalidades para as quais são utilizados. Por fim, a última inspiração colhida no GDPR se consubstancia nos princípios que buscam garantir a segurança da informação tratada, com adoção de medidas preventivas a um eventual vazamento de dados, que conte com uma posterior prestação de contas com relação ao tratamento oferecido e responsabilização ante infração ao LGPD.

Vale ressaltar que a lei confere um tratamento com algumas diferenças em se tratando dos dados pessoais de crianças e adolescentes, bem como dos dados pessoais considerados sensíveis.

Com relação ao tratamento conferido a crianças e adolescentes, a exigência legal é de que o tratamento seja feito no melhor interesse destes, bem como da coleta não consentida quando tais dados forem utilizados para contatar os pais ou responsáveis, além de tomar as medidas necessárias para que o consentimento no compartilhamento dos dados pessoais de menores seja dado pelos pais. Com relação ao tratamento de dados pessoais sensíveis, tem-se que só pode ser feito quando: (i) for consentido pelo titular, de forma específica e destacada; (ii) for necessário ao cumprimento de alguma obrigação legal por parte do controlador; (iii) se destinar à realização de estudos por órgão de pesquisa, (iv) for submetido à Administração Pública a fim de possibilitar a execução de políticas públicas, (v) for necessário à execução de contrato do qual o titular seja parte, a pedido deste, (vi) for necessário ao regular exercício de seus direitos, (vii) for necessário à proteção da vida ou incolumidade física do titular ou de terceiro, (viii) for requisito para realização de procedimento por profissionais da área da saúde ou por entidades sanitárias, (ix) for necessário ao atendimento dos interesses legítimos do controlador ou de terceiros, excetuando-se os casos em que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, ou (x) quando necessário à proteção do crédito, havendo a lei observado que tal situação inclui tudo aquilo disposto nas demais legislações pertinentes ao tema.

Nos moldes do GDPR, a LGPD prevê o livre acesso dos titulares a seus dados pessoais, como anteriormente mencionado, e também prevê a necessidade de as empresas que lidam com dados pessoais contratarem um *Data Protection Officer*, que na legislação brasileira, recebe o título de Encarregado. A este profissional, de forma análoga ao estabelecido pelo GDPR, caberá aceitar reclamações e comunicações provenientes dos titulares e das autoridades nacionais, e tomar as devidas providências. Além disso, deve orientar os funcionários e terceiros contratados pela entidade a respeito do correto tratamento dos dados pessoais e da necessidade em relação a este cuidado.

A LGPD prevê ainda a apresentação de um relatório de impacto a proteção de dados pessoais, cuja elaboração delegou à responsabilidade do controlador, e que deve ser requisitado pela Agência Nacional de Proteção de Dados (ANPD).

A criação da ANPD, vale mencionar, foi uma questão delicada quando da sanção da lei. Em sua primeira versão, a Lei Geral de Proteção de Dados contou com o veto presidencial à criação da agência, efetuado pelo então presidente Michel Temer, que

inclusive foi objeto de diversas críticas⁹. Na ocasião, o presidente também acabou por vetar diversas sanções previstas àqueles que descumprissem o estabelecido pela LGPD, vetos esses que reduziram drasticamente o poder de sanção por parte das autoridades. O veto presidencial acabou mantido pelo Congresso, e a ANPD acabou sendo criada somente a partir do advento da Medida Provisória nº 869 de 2018, editada pelo próprio Michel Temer, a três dias do encerramento de seu mandato.

A ANPD, vale dizer, será composta por um Conselho Diretor contando com 5 (cinco) membros, e um Conselho Nacional de Proteção de dados, contando com 23 (vinte e três) representantes. Será esta agência a responsável por prover normas a respeito da proteção de dados, dar interpretação a normas e deliberar acerca daquilo que foi considerado omissivo na legislação, fiscalizar, aplicar sanções, além de promover a comunicação institucional entre o Brasil e os demais países a respeito do tema, dentre outras competências.

A LGPD prevê também um fim ao tratamento de dados pessoais, que deve ocorrer quando a finalidade ao tratamento daqueles dados for extinta, quando o período previamente proposto para realização do tratamento findar, quando for requerido pelo titular ou quando for determinado pela ANPD. Além disso, quando do término do tratamento, a Lei determina que seja realizada a exclusão dos dados pessoais, elencando hipóteses específicas à sua conservação. Devem ser conservados os dados pessoais tão somente quando (i) estes forem necessários ao cumprimento de alguma obrigação legal, (ii) forem objeto de estudo realizado por instituto de pesquisa, (iii) for requisitada a transferência destes dados a terceiro, ou (iv) quando forem destinados a uso exclusivo do controlador, vedado o acesso de terceiros e somente quando anonimizados.

Para o poder público, a Lei estabelece algumas obrigações específicas, como a de que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral, ressalvando que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas. Veda a transferência de dados de entes públicos a particulares, estabelecendo algumas

⁹ Fonte: < <https://www.cartacapital.com.br/blogs/intervozes/veto-a-autoridade-coloca-em-risco-lei-de-protecao-de-dados-pessoais/>>. Acesso em 10.5.2019

exceções, em sua maioria ligadas à necessidade de compartilhamento com particulares para consecução do fim público.

A possibilidade de litigar ante a ANPD contra o controlador de seus dados é assegurada aos titulares. Nessa situação, quando houver infração à LGPD no concernente ao tratamento dos dados, a autoridade nacional poderá enviar informe com as medidas cabíveis, a fim de encerrar a violação. Além disso, o controlador poderá sofrer ação de reparação de danos. Com relação às sanções administrativas aplicáveis para aqueles que infringirem a lei, caberá: advertência; multa simples, no valor de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, com limite total de até R\$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total de R\$ 50.000.000,00 (cinquenta milhões de reais); publicização da infração após confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização ou sua eliminação.

Ademais, a lei prevê que os agentes de tratamento formulem regras de boas práticas e de governança que levem em consideração à natureza, o escopo, a finalidade do tratamento oferecido, bem como a probabilidade de vazamento bem como a gravidade dos riscos decorrentes desse tratamento. Esse conjunto de regras deve demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem seu cumprimento. Além disso, deve ser aplicável ao conjunto de dados pessoais que estejam sob seu controle, adaptado à estrutura, escala e volume de suas operações, além de proporcionar ao titular a sensação de que pode confiar na empresa com relação às questões de tratamento dos seus dados.

Com relação aos principais dispositivos capazes de interferir na atividade empresarial, destacam-se aqueles que regulam a forma com que os dados pessoais devem ser tratados, quais sejam, de que devem ser anônimos, e só devem ser identificáveis a partir de um cruzamento de informações, de maneira a resguardar a privacidade do usuário. Nesse sentido, a atuação empresarial fica adstrita aos dados recolhidos por meio de sua própria atividade, de maneira a proteger usuários de possíveis *data breaches*.

As legislações referentes à proteção dos dados pessoais e antitruste, desta feita, devem ser instrumentos suficientes para dar cabo das condutas anticompetitivas que permeiam também o uso e manipulação de dados pessoais. Nesse sentido, enquanto a regulação conferida pelas leis que protegem dados pessoais visa regular a relação entre

usuário e empresa, a legislação antitruste se coloca no sentido de impor sanções às empresas que fizerem uso de dados para adotar condutas que causem danos tanto a usuários quanto a outros competidores. A legislação referente à proteção de dados se faz importante ao impor *standards* ao que constitui ou não conduta que possa ser praticada por detentores de dados pessoais, de maneira com que a partir da interpretação desta legislação a autoridade antitruste consegue não apenas reconhecer eventual abuso, mas delimitar os limites ao uso de dados pessoais, entendendo quando constituírem abuso capaz de lesar os demais, sejam estes *players* ou consumidores.

1.3 – O antitruste e as legislações acerca da proteção de dados: repercussões em estruturas e condutas

Em primeiro lugar, considerando-se o poder que determinadas empresas possuem por sobre os dados de seus clientes, poder que, aliás, advém destes mesmos dados, bem como os impactos econômicos que a detenção de informações acuradas sobre os clientes podem trazer, a detenção de dados e o tratamento despendido a estes devem ser levados em consideração quando da análise levada a cabo naquilo que denominamos como Atos de Concentração, ocasião em que ocorre o “controle prévio” ou “controle de estruturas”¹⁰, por parte da autoridade antitruste – no caso brasileiro, por parte do Conselho Administrativo de Defesa Econômica - Cade. Na análise ocorrida sob essas circunstâncias, caberá à autoridade antever os possíveis impactos que a combinação de dados entre duas empresas poderá gerar, de maneira a evitar que os consumidores possam vir a sofrer algum tipo de abuso advindo da concentração entre essas duas empresas, ou que os demais agentes que atuam em determinado mercado sejam prejudicados, mantendo-se a concorrência longe de quaisquer ameaças, portanto.

¹⁰ “O pressuposto básico do controle de estruturas é o de que, para o adequado funcionamento do mercado, não basta o controle de condutas, que se realiza por meio da prevenção e repressão das infrações anticoncorrenciais. É necessário igualmente que se impeça a formação de estruturas empresariais que restrinjam indevidamente a livre concorrência, seja porque propiciam o exercício abusivo da posição dominante adquirida ou reforçada em virtude da operação, seja porque facilitam a colusão. Dessa maneira, o controle de estruturas apresenta propósito nitidamente preventivo e complementar ao controle de condutas, já que a sua finalidade não é a de impor nenhuma sanção, mas somente a de verificar se o ato de concentração submetido ao seu exame deve ser aprovado, rejeitado ou ainda aprovado com restrições. Parte-se da premissa de que a livre concorrência é um bem muito precioso para ser colocado em risco, até porque os danos causados por estruturas anticoncorrenciais podem ser irreparáveis. Não sendo o controle de condutas suficiente para assegurar a manutenção da ordem concorrencial, até em razão das conhecidas dificuldades para se identificar e punir condutas anticompetitivas, é inequívoca a importância do controle de estruturas [...]” FRAZÃO, Ana. Direito da Concorrência, pressupostos e perspectivas, Ed. Saraiva, 2017.

De acordo com o art. 90 da Lei 12.529/2011, realiza-se um Ato de Concentração quando:

- “(I) 2 (duas) ou mais empresas anteriormente independentes se fundem;
- (II) 1 (uma) ou mais empresas adquirem, direta ou indiretamente, por compra ou permuta de ações, quotas, títulos ou valores mobiliários conversíveis em ações, ou ativos, tangíveis ou intangíveis, por via contratual ou por qualquer outro meio ou forma, o controle ou partes de uma ou outras empresas;
- (III) 1 (uma) ou mais empresas incorporam outra ou outras empresas; ou
- (IV) 2 (duas) ou mais empresas celebram contrato associativo, consórcio ou joint venture.”

Vale ressaltar que o Cade possui uma resolução a fim de explicitar melhor do que tratariam os contratos associativos elencados no inciso IV, e que a própria lei traz a ressalva de que não serão considerados Atos de Concentração os contratos associativos quando destinados às licitações promovidas pela Administração Pública direta ou indireta, ou a contratos destas decorrentes.

O Cade, no entanto, não mantém sua atividade restrita à análise do dito controle de estruturas, mas faz ainda um tipo de controle que denominamos “controle de conduta”, posterior a um eventual dano concorrencial, e ocasionado por uma ou mais empresas que incorram em infrações à ordem econômica. Com relação às condutas que são objeto de análise por parte deste órgão, todas se encontram elencadas na Lei 12.529/2011.¹¹

¹¹ “Art. 36. Constituem infração da ordem econômica, independentemente de culpa, os atos sob qualquer forma manifestados, que tenham por objeto ou possam produzir os seguintes efeitos, ainda que não sejam alcançados:

I - limitar, falsear ou de qualquer forma prejudicar a livre concorrência ou a livre iniciativa;

II - dominar mercado relevante de bens ou serviços;

III - aumentar arbitrariamente os lucros; e

IV - exercer de forma abusiva posição dominante.

§ 1º A conquista de mercado resultante de processo natural fundado na maior eficiência de agente econômico em relação a seus competidores não caracteriza o ilícito previsto no inciso II do caput deste artigo.

§ 2º Presume-se posição dominante sempre que uma empresa ou grupo de empresas for capaz de alterar unilateral ou coordenadamente as condições de mercado ou quando controlar 20% (vinte por cento) ou mais do mercado relevante, podendo este percentual ser alterado pelo Cade para setores específicos da economia.

§ 3º As seguintes condutas, além de outras, na medida em que configurem hipótese prevista no caput deste artigo e seus incisos, caracterizam infração da ordem econômica:

I - acordar, combinar, manipular ou ajustar com concorrente, sob qualquer forma:

a) os preços de bens ou serviços ofertados individualmente;

b) a produção ou a comercialização de uma quantidade restrita ou limitada de bens ou a prestação de um número, volume ou frequência restrita ou limitada de serviços;

O direito da concorrência, neste prisma, e conquanto detentor da função e da finalidade de defender o consumidor e a inovação¹² tem nos tempos atuais a obrigação de entender esses novos mercados e proteger todos os seus múltiplos lados. Assim seu dever passa tanto pela proteção de agentes e consumidores dos eventuais abusos por parte daqueles que exploram os dados pessoais, quanto de assegurar que as inovações decorrentes dos mercados digitais continuem ocorrendo e facilitando a vida de todos os cidadãos.

-
- c) a divisão de partes ou segmentos de um mercado atual ou potencial de bens ou serviços, mediante, dentre outros, a distribuição de clientes, fornecedores, regiões ou períodos;
 - d) preços, condições, vantagens ou abstenção em licitação pública;
 - II - promover, obter ou influenciar a adoção de conduta comercial uniforme ou concertada entre concorrentes;
 - III - limitar ou impedir o acesso de novas empresas ao mercado;
 - IV - criar dificuldades à constituição, ao funcionamento ou ao desenvolvimento de empresa concorrente ou de fornecedor, adquirente ou financiador de bens ou serviços;
 - V - impedir o acesso de concorrente às fontes de insumo, matérias-primas, equipamentos ou tecnologia, bem como aos canais de distribuição;
 - VI - exigir ou conceder exclusividade para divulgação de publicidade nos meios de comunicação de massa;
 - VII - utilizar meios enganosos para provocar a oscilação de preços de terceiros;
 - VIII - regular mercados de bens ou serviços, estabelecendo acordos para limitar ou controlar a pesquisa e o desenvolvimento tecnológico, a produção de bens ou prestação de serviços, ou para dificultar investimentos destinados à produção de bens ou serviços ou à sua distribuição;
 - IX - impor, no comércio de bens ou serviços, a distribuidores, varejistas e representantes preços de revenda, descontos, condições de pagamento, quantidades mínimas ou máximas, margem de lucro ou quaisquer outras condições de comercialização relativos a negócios destes com terceiros;
 - X - discriminar adquirentes ou fornecedores de bens ou serviços por meio da fixação diferenciada de preços, ou de condições operacionais de venda ou prestação de serviços;
 - XI - recusar a venda de bens ou a prestação de serviços, dentro das condições de pagamento normais aos usos e costumes comerciais;
 - XII - dificultar ou romper a continuidade ou desenvolvimento de relações comerciais de prazo indeterminado em razão de recusa da outra parte em submeter-se a cláusulas e condições comerciais injustificáveis ou anticoncorrenciais;
 - XIII - destruir, inutilizar ou açambarcar matérias-primas, produtos intermediários ou acabados, assim como destruir, inutilizar ou dificultar a operação de equipamentos destinados a produzi-los, distribuí-los ou transportá-los;
 - XIV - açambarcar ou impedir a exploração de direitos de propriedade industrial ou intelectual ou de tecnologia;
 - XV - vender mercadoria ou prestar serviços injustificadamente abaixo do preço de custo;
 - XVI - reter bens de produção ou de consumo, exceto para garantir a cobertura dos custos de produção;
 - XVII - cessar parcial ou totalmente as atividades da empresa sem justa causa comprovada;
 - XVIII - subordinar a venda de um bem à aquisição de outro ou à utilização de um serviço, ou subordinar a prestação de um serviço à utilização de outro ou à aquisição de um bem; e
 - XIX - exercer ou explorar abusivamente direitos de propriedade industrial, intelectual, tecnologia ou marca” BRASIL, Lei 12.529 de 30 de novembro de 2011. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, 1º de novembro de 2011.

¹² FRAZÃO, Ana. Direito da Concorrência, pressupostos e perspectivas, Ed. Saraiva, 2017.

Já, inclusive, houve decisões que emanaram de autoridades tradicionalmente concorrenciais a tutelar questões ligadas à proteção de dados pessoais¹³, de maneira com que acabaram por preencher lacunas ainda remanescentes da incipiente tutela dos direitos relativos às questões ligadas à privacidade de dados pessoais. Essa interface e lacuna merecem ser analisadas, e é a tentativa de realização desta análise de que se trata este trabalho.

Muito embora a LGPD seja aplicável a qualquer empresa que detenha dados de usuários, ainda que estes não sejam parte de seu negócio, como ocorre com as *data-driven organisations*, o presente trabalho tratará apenas do último tipo empresarial, vez que, como ficará claro ao longo do desenvolvimento do trabalho, são estas as companhias que mais requerem atenção. A importância e necessária diferenciação na abordagem relativa às *data-driven organisations* deriva do caráter dessas companhias com relação ao inovativo uso dos dados pessoais a fim de auferir lucro com suas atividades.

Nesse sentido, considerando o escopo de análise relativo às *data-driven organisations*, um aumento na coleta de dados pessoais de usuários realizado por uma empresa, bem como o que poderíamos denominar como uma espécie de refino a respeito dos dados já coletados dos usuários de suas plataformas significaria um aumento de valor ao seu produto, o que, ao extremo, poderia ser comparável a um aumento de preço de um determinado produto de uma empresa tradicional. Assim, para as empresas de tecnologia, o aumento dos dados detidos significa um aumento de valor e, conseqüentemente, de seu poder de mercado, de maneira com que deve ser objeto das análises realizadas pela perspectiva antitruste.

A análise levada a cabo pelas autoridades concorrenciais, no entanto, nem sempre reconheceu a importância da proteção de dados pessoais, tampouco a relevância do Big Data. Foram três as principais fases pelas quais a teoria antitruste passou, a fim de que a nova realidade pudesse ser entendida em sua totalidade¹⁴. A primeira fase aconteceu quando da análise dos casos Asnef-Equifax (tentativa de financeiras de criar uma base de dados comum) e Google-DoubleClick, e não levou em consideração a questão atinente à proteção dos dados pessoais, vez terem as autoridades entendido se

¹³ Fonte: <<https://epocanegocios.globo.com/Empresa/noticia/2019/02/alemanha-restringe-coleta-de-dados-de-usuarios-do-facebook-no-pais.html>>. Acesso em 17 de fevereiro de 2019.

¹⁴ ZANFIR-FORTUNA, Gabriela; IANC Sînziana. “Data Protection and Competition Law: the Dawn of ‘uberprotection’”. 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824>. Acesso em 16 de junho de 2019.

tratar de questões paralelas, de maneira com que o Big Data não teria interferência relevante na dinâmica concorrencial dos mercados.

A segunda fase, ocorrida quando da análise da operação Facebook-Whatsapp já contou com o entendimento por parte das autoridades de que uma questão exerceria interferência na outra, muito embora também tenha sido considerado que tal interferência não seria capaz de trazer impactos concorrenciais relevantes.

A terceira fase, por fim, fase na qual atualmente nos encontramos inseridos, percebe a relevância da questão dos dados na análise concorrencial, considerando-a tanto do ponto de vista da análise de fusões e aquisições entre empresas, como do ponto de vista de condutas. Há inclusive recente decisão por parte da autoridade concorrencial alemã que determinou ao Facebook¹⁵ regras relativas à coleta e tratamento de dados realizados pela empresa, a despeito de uma possível atuação da autoridade de proteção de dados, decisão que confunde competência relativa à lei antitruste daquilo que é tutelado pela legislação atinente à proteção de dados pessoais.

A fim de entender, desta feita, as evoluções na análise das autoridades serão, nos capítulos subsequentes, analisadas de forma mais profunda duas operações, uma relativa à primeira fase (entre o Google e a Doubleclick) e a mais recente já finalizada (entre a Apple e o Shazam). Além disso, ao longo desta última década foi percebido que a questão relativa à exploração de dados pessoais e do Big Data estavam sendo usados para adoção de condutas anticompetitivas. Mais que isso, foi percebido que a atuação de algoritmos embasados em tais informações é propícia à formação de colusões que sequer seriam de intenção das empresas participar. Ainda, o alto valor adquirido por dados pessoais na dinâmica econômica torna este também um produto, coletado, tratado – às vezes até roubado – e vendido a companhias, a fim de que estas consigam melhor responder ao mercado e maximizar seus lucros.

Realizadas, assim, as considerações relevantes a respeito tanto da legislação que protege a privacidade dos dados pessoais quanto daquela protege a concorrência, os próximos capítulos irão se debruçar sobre as preocupações da academia acerca da intersecção entre esses dois temas, bem como de alguns casos concretos que exigiram da autoridade antitruste uma análise que levasse em conta as especificidades acerca da legislação pertinente à proteção de dados pessoais. No Brasil, muito embora já tenha

¹⁵ Fonte: < <https://www.correiodopovo.com.br/jornalcomtecnologia/alemanha-restringe-coleta-de-dados-de-usu%C3%A1rios-do-facebook-no-pa%C3%ADs-1.318529>>. Acesso em 16 de junho de 2019.

vido editada uma legislação acerca da proteção de dados pessoais, não há julgamento de muitos casos relevantes envolvendo o tema, de modo com que além do Cade, a atuação da Federal Trade Commission, órgão que faz análise concorrencial nos EUA, e da Comissão Europeia serão bastante explorados.

CAPÍTULO 2 - PROTEÇÃO DE DADOS E CONTROLE DE ESTRUTURAS

O tema referente à proteção de dados pessoais, desta feita, na medida em que passou a afetar toda e qualquer atividade empresarial, também passou a afetar a dinâmica dos mercados, e, conseqüentemente, passou a integrar o ramo dos itens obrigatoriamente observáveis no ramo do direito antitruste. Nesse sentido, à medida que a detenção e análise de dados passou a integrar fator capaz de diferenciar um concorrente de outro, o direito se viu obrigado a entender a alteração da dinâmica concorrencial provocada, bem como os principais efeitos gerados, vez que o uso de dados constitui mais um instrumento capaz de prejudicar a efetiva concorrência entre competidores e os próprios consumidores.

A academia, assim como órgãos internacionais - notadamente a OCDE - já se debruçaram sobre as questões atinentes à diferenciação da dinâmica mercadológica quando os casos em análise fizerem parte de data-driven markets. Um dos mais célebres textos sobre o tema é do professor Maurice Stucke, da Universidade do Tennessee, denominado “Should we be concerned about data opolies?”. A análise do professor Stucke perpassa pela maioria dos problemas que relacionam atos de concentração, Big Data e dados pessoais, e norteará a análise desenvolvida neste capítulo.

2.1 – O conceito de *data-opolies*

A primeira questão a ser levantada diz respeito ao atual conceito de monopólio do *Sherman Act*¹⁶, que define como ilegais a posse do poder de monopólio num mercado relevante determinado e a aquisição ou manutenção intencional desse poder por meios que não como consequência de um produto superior, da perspicácia empresarial da própria companhia ou de um evento histórico acidental. Tem-se assim que a detenção de um monopólio não é por si só ilegal, mas é sim ilegal o uso deste poder para limitar a competição, ou a aquisição de tal poder por meios que não decorram da eficiência da empresa em questão.

Com relação aos *data-opolies*, no entanto, é necessário destacar que o exercício do poder de monopólio é diferenciado – o professor Stucke afirma ser absolutamente

¹⁶ Denomina-se Sherman Act a primeira lei com objetivo de defender a concorrência a vigor nos Estados Unidos. Aprovada em 1890, ainda hoje, conjuntamente com o Clayton Antitrust Act e com o Federal Trade Commission Act, trata-se de lei que rege a prática concorrencial naquele país < <https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws>>. Acesso em 19 de março de 2019.

improvável um aumento de preços nesse tipo de mercado.¹⁷ Além disso, ressalta como a maior parte das abordagens entendem que se não há um aumento de preços, não há riscos ao consumidor, e que, inclusive, não há sequer que se falar em poder de monopólio. Tal conclusão, no entanto, especialmente com relação aos *data-driven markets* se mostra falaciosa, causando a perigosíssima sensação de que os *data-opolies* não oferecem riscos à dinâmica concorrencial.

Desmonta-se ainda o argumento de que em não havendo um aumento de preços, haverá uma queda na qualidade dos serviços providos. Não há interesse algum das plataformas em diminuir a qualidade do serviço prestado, vez que estas buscam a manutenção dos usuários. Em razão do efeito de rede que existe em tais mercados, uma diminuição no número de participantes de uma plataforma a torna menos interessante para os demais usuários, que assim tenderão a migrar para plataforma que seja mais atrativa, e que necessariamente contenha uma adesão maior por parte das pessoas. O efeito de rede inclusive assegura que produtores de conteúdo relevante, bem como programadores foquem sua atividade para um maior desenvolvimento de tais plataformas.

O autor considera ainda como efeito de rede a característica do *learning-by-doing*, mormente encontrada em sites de busca. Este mecanismo diz respeito à capacidade de “auto-aprimoramento” de alguns sites e plataformas, vez que quanto mais se usa a ferramenta, mais o algoritmo que a rege consegue aprender as preferências dos consumidores e assim refinar seus resultados de busca.

Abre-se pequeno espaço, no entanto, para uma breve discordância com relação ao enquadramento do *learning-by-doing* como efeito de rede. Em verdade, muito embora tal característica e aprimoramento decorram do uso massivo da ferramenta, certo é que, num eventual abandono desta por expressivo número de usuários, não haveria uma perda de atratividade imediata da plataforma, tampouco uma robusta queda em sua qualidade. Para que esta se tornasse obsoleta, haveria de ser necessário um intervalo temporal considerável, em razão de os dados anteriormente colhidos ainda

¹⁷ STUCKE, MAURICE E. Why should we be concerned about data-opolies?. Tennessee, 2018. “Data-opolies are unlikely to raise prices for their goods and services. No one alleged that Facebook, in acquiring WhatsApp or Instagram, would start charging users a fee. Instead, Facebook eliminated WhatsApp’s small fee in some countries for its texting app.³³ The presumption is that “lower prices improve consumer welfare (all else being equal).”³⁴ Since data-opolies are not raising prices above competitive levels (or reducing output below competitive levels), some may question if they even possess monopoly power.” p. 281

permanecerem em poder da companhia, que continuaria a utilizá-los a fim de melhor prover seu serviço.

É uma dinâmica bastante diferente daquela do Facebook, por exemplo. Na hipótese de um abandono massivo de usuários, os usuários restantes sentir-se-iam compelidos a também migrar de plataforma, vez que o conteúdo anteriormente produzido pelos usuários que optaram por migrar e que constituiriam um atrativo ao uso do Facebook deixaria de existir. Parece, portanto, que o *learning-by-doing* estaria mais próximo do conceito de escala, ou de eficiência, que de um efeito de rede.

A provável ausência de uma queda na qualidade do serviço fornecido pelas *data-driven companies*, no entanto, não quer dizer que a conclusão de um Ato de Concentração está livre de problemas que envolvam os parâmetros anteriormente aplicados ao serviço. É altamente provável, por exemplo, que a concentração destas companhias seja acompanhada de uma queda no nível de privacidade anteriormente detido pelos usuários. Os usuários, por sua vez e em decorrência do anteriormente mencionado efeito de rede, acabam cedendo por uma maior “invasão” com relação a seus dados pessoais a fim de que possam permanecer fazendo uso de determinada plataforma. Ao usuário não é vantajosa a migração, vez que o conteúdo da plataforma lhe interessa justamente por seus amigos utilizarem-na. Assim, esta é relevante a partir do nível de engajamento de todas as pessoas envolvidas em seu círculo social, de maneira com que não há qualquer interesse por parte do usuário em efetuar uma migração ante um maior “abuso” com relação ao uso de seus dados pessoais.

Desta feita, diferentemente do que argumentou Eric Schmidt, então presidente do conselho do Google ao Senado americano em 2012, de que os concorrentes do Google¹⁸ estariam a somente “clique de distância”, em verdade existem *switching costs* na migração, estritamente ligados ao efeito de rede, que, embora bastante baixos, existem, vez que trocar de plataforma implica, necessariamente, em sacrificar as interações ali realizadas.

Nesse sentido, faz-se estritamente necessária a observação do papel dos dados na dinâmica concorrencial, e o reconhecimento de que um *data-opoly* pode trazer enormes prejuízos a competidores, devendo empresas com potencial para tanto serem

¹⁸ Fonte: <https://exame.abril.com.br/revista-exame/o-google-no-banco-dos-reus/cli>. Acesso em 15 de março de 2019.

tratadas pelo antitruste de acordo com as peculiaridades – e potencial perigo – que apresentam.

2.2 – Dados como ativos das empresas

É fato que muitas das empresas de tecnologia são apenas plataformas, e constituem mercados de dois ou múltiplos lados. Um bom exemplo de empresa deste tipo de mercado é o Facebook: de um lado temos os usuários, que, a fim de obter o serviço prestado pela rede social (qual seja, de se conectar com e receber atualização de seus amigos) fornecem dados. Na outra ponta da plataforma, o Facebook faz uso desses dados para que empresas dos mais variados setores possam anunciar em seu site de forma eficaz, atingindo assim um público com maior probabilidade de efetivamente adquirir seu produto, mais inclinado a tal.

Nesse sentido, há que se concordar com o fato de que, conquanto de um lado a troca entre o “cliente” e a empresa dá-se por meio do dinheiro – entre as empresas que desejam anunciar e o Facebook -, na outra ponta a moeda de troca são os dados pessoais do usuário, que os fornece em troca do serviço prestado. Nestes termos, torna-se nítido que o faturamento bruto ou o valor do volume de vendas realizadas pelo Facebook não mais conseguem traduzir o tamanho ou poder econômico detido pela companhia.

De acordo com o relatório da OCDE sobre Big Data¹⁹, os dados pessoais detidos por uma empresa devem ser encarados como um ativo destas, capazes de serem usados em práticas exclusionárias, e concluem que a massiva acumulação e detenção de dados pessoais de usuários, bem como a intensiva análise e utilização destes provocam um aumento do poder de mercado detido pela companhia, bem como tem o potencial de proporcionar um efeito lock-in aos consumidores e de criar barreiras a novas entradas. Dessa forma, a OCDE ressalta que as autoridades devem sempre ter em mente o impacto que os dados exercem na dinâmica concorrencial em um mercado que envolve empresas de tecnologia, ou que fazem uso da coleta, análise e tratamento de dados pessoais dos consumidores.

Ademais, a OCDE destaca uma segunda abordagem com relação à aquisição das *data-driven companies*, relativo à uma queda na qualidade dos serviços, vez que boa parte dos serviços fornecidos por tais empresas, em um dos lados do mercado ao menos,

¹⁹ CAPOBIANCO, ANTONIO. Relatório da OCDE sobre Big Data - Big Data: Bringing Competition Policy to the Digital Era, 2017.

são gratuitos. Além disso, uma vez que os dados ocupam um papel que de modo simétrico poderia ser comparável ao que o dinheiro ocupa na outra ponta do mercado, também é aventada a possibilidade de que haja um maior abuso no uso desses ativos a fim de que a empresa consigo utilizá-los para melhor monetizar sua atividade na outra ponta.

2.3 - Proteção de dados como diferencial competitivo das empresas

Um outro aspecto que deve ser levado em conta quando da análise de Atos de Concentração que envolvam empresas capazes de armazenar uma grande quantidade de dados pessoais de seus usuários passa pela segurança dada ao tratamento de tais dados. Em primeiro lugar, uma empresa com massivo volume de informações, na hipótese de ocorrência de um *data breach*, seria responsável pela exposição de milhares de usuários.

A história nos mostra que a ocorrência de *data breaches* em gigantes detentores de diversas informações sensíveis, é algo que pode ser considerado tanto quanto recorrente. Organizações ligadas à saúde²⁰, ao sistema bancário e financeiro²¹, ao sistema de justiça²², grandes empresas de tecnologia²³ e até mesmo universidades²⁴ já foram vítimas deste tipo de violação. Do ponto de vista daqueles que tem interesse em roubar dados de usuários, é até mais interessante que tais dados estejam concentrados.

Ademais, quando há a concentração em mercados envolvendo dados pessoais, o usuário acaba sem muita opção de migração para outras empresas, que consigam apresentar o diferencial competitivo de respeito à privacidade de seus dados pessoais.

Um outro aspecto bastante preocupante acerca da concentração de dados diz respeito à venda de dados pessoais a governos e empresas. O escândalo referente ao Facebook e a Cambridge Analytica²⁵ foi uma pequena amostra do tamanho estrago que um data-opoly pode desencadear. Naquela ocasião, foram vazados dados de 50 (cinquenta) milhões de usuários, utilizados posteriormente para realização de

²⁰ Fonte: < <https://www.natlawreview.com/article/oh-no-not-again-chalk-yet-another-health-data-breach>>. Acesso em 15 de março de 2019

²¹ Fonte: < <https://www.idtheftcenter.org/data-breaches/>>. Acesso em 15 de março de 2019.

²² Fonte < <https://www.pcmag.com/news/286024/antisech-breach-yields-huge-amount-of-law-officers-personal>>. Acesso em 15 de março de 2019

²³ Fonte < <https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-breach>>. Acesso em 15 de março de 2019

²⁴ Fonte < <https://www.foxnews.com/tech/data-breach-affects-80000-uc-berkeley-faculty-students-and-alumni>>. Acesso em 15 de março de 2019

²⁵ Fonte < <https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml>>. Acesso em 15 de março de 2019

propaganda de cunho político, de maneira a predizer quais eram os tipos de conteúdo o usuário estava mais apto a acreditar, e, desse modo, resultando numa propaganda política direcionada, capaz de comprovadamente exercer influência no resultado final das urnas.

Tem-se a forte impressão de que os usuários de sites como o Google e o Facebook tem ciência de que todos os dados pessoais por eles fornecidos no âmbito desses sites são vendidos e utilizados para realização de publicidade direcionada por parte de diversas outras empresas. A grande surpresa do escândalo entre Cambridge Analytica e Facebook, no entanto, que fez com que Mark Zuckerberg depusesse no Senado americano²⁶ e que provocou uma perda de 35 (trinta e cinco) bilhões de dólares de valor da empresa, diz respeito ao fato de que a maior parte dos dados coletados assim o eram sem a anuência do titular.

Com relação à remuneração dos *data-opolies*, há discussões acerca de uma possível assimetria quanto ao pagamento ofertado por tais empresas aos usuários. Como já abordado, os usuários fornecem seus dados pessoais a fim de obter o serviço prestados por *data-driven companies*. Ademais, aqueles sites que funcionam como plataformas – com é, mais uma vez, o caso do Facebook – furtam-se da necessidade de produzir conteúdo criativo para atrair consumidores a seus sites. A plataforma é, em realidade, alimentada por outros usuários, que nada recebem pelo conteúdo produzido e disponibilizado, exceto, talvez, a visibilidade e a possibilidade de grande alcance, possibilidade esta que não se concretiza para a grande massa de usuários, que ainda assim, sem qualquer retorno diferente da aprovação daqueles que constituem sua rede de contatos, permanecem produzindo conteúdo.

Existem, no entanto, exemplos de empresas que conseguiram quebrar com este círculo vicioso que finda na ausência de remuneração ao produtor de conteúdo - é o caso do YouTube e do Spotify, para citar apenas alguns. No caso do YouTube²⁷, a propaganda é exibida antes e até mesmo durante a reprodução dos vídeos, e o criador de conteúdo pode aderir ao YouTube Partner Program. De acordo com este, se o produtor está localizado em qualquer dos países que fazem parte do programa e desde que atingidos alguns outros critérios - Ter mais de 4 mil horas de exibição pública nos

²⁶ Fonte: <<https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml>> Acesso em 17 de março de 2019

²⁷Fonte:<<https://sambatech.com/blog/insights/monetizacao-no-youtube/>
<https://support.google.com/youtube/answer/72851?hl=pt-BR>> Acesso em 17 de março de 2019

últimos 12 meses; ter mais de mil inscritos em seu canal; ter uma conta do Google AdSense vinculada; dentre outros – o site remunera o criador de conteúdo a depender de seu número de visualizações, bem como de inscritos no canal, em valores que variam a depender desses dois quesitos. O Spotify²⁸, por sua vez, também possui um programa de remuneração aos artistas que disponibilizam seu conteúdo na plataforma, que é de um valor fixo para cada mil reproduções. Vale ressaltar ainda que de modo semelhante agem seus concorrentes, sendo o mercado de música streaming uma exceção à regra da ausência de remuneração a criadores de conteúdo.

Não é possível, no entanto, obter qualquer tipo de avaliação a respeito do quão justa é a remuneração oferecida aos criadores de conteúdo. Certo é que há uma pública briga de artistas que chegam a limitar seu conteúdo em determinadas plataformas por considerarem que estas não oferecem uma remuneração adequada. É o caso²⁹ de Neil Young, Taylor Swift e Beyoncé com o Spotify, a título de exemplo.

Voltando aos problemas que envolvem privacidade e uma possível concentração entre empresas detentora de dados pessoais, a perda de confiança acerca dos dados fornecidos é mais um provável efeito deletério. Ora, uma vez conhecido que algoritmos fazem discriminações entre usuários, uma forma de se proteger do prejuízo sem, no entanto, deixar de fazer uso do serviço é simplesmente mentir acerca de seus dados, especialmente aqueles mais sensíveis – como orientação sexual e religiosa. Tal comportamento criaria uma cadeia de desconfiança, que, traria prejuízos aos mercados.

Nesse sentido, muito embora haja discussões acerca do limiar sob o qual a maioria das pessoas aceitaria fornecer seus dados em troca de determinado serviço, fato é que os assuntos atinentes à proteção de dados pessoais, bem como dos possíveis prejuízos gerados a consumidores, estão cada vez mais em voga. Assim, de forma consequencial, mais atentas as pessoas parecem ter ficado com relação ao assunto, de maneira com que também tem agido no sentido de exigir maior proteção com relação aos dados de que são titulares, de modo com que, muito embora não seja possível mensurar até que ponto, a proteção dos dados pessoais vem constituindo um diferencial relevante na escolha e no uso de serviços de uma empresa em detrimento de outras.

²⁸ Fonte: <<https://tecnoblog.net/239268/valores-streaming-musica-spotify-apple-2017/>> Acesso em 17 de março de 2019

²⁹ Fonte: <<https://www.techtudo.com.br/listas/noticia/2015/07/tres-artistas-que-tiraram-suas-musicas-do-spotify-e-o-caso-tidal.html>> Acesso em 17 de março de 2019

Tal afirmação tanto é verdade que existem empreendedores investindo nesse diferencial ao entrar no mercado: é o caso, por exemplo, do DuckDuckGo³⁰, buscador rival do Google que apresenta como diferencial uma maior proteção de dados pessoais, vez que promete a não retenção destes. Cabe ao futuro dizer se a não retenção conseguirá fazer frente aos serviços fornecidos com base na retenção e análise de dados.

Os pontos elencados até o momento, muito embora sejam importantes aos fins de uma análise concorrencial, dizem respeito às características de tais empresas. Diante de tais pontos, faz-se necessário entender como tais questões são tratadas pelas autoridades concorrenciais. A análise em si, no entanto, se inicia a partir da notificação de possível operação entre tais companhias, e deve observar a realidade para além dela, antevendo os possíveis futuros impactos. Vale refletir que o tratamento depreendido passa desde o filtro inicial relativo às operações que devem ou não ser notificadas, que possuem os requisitos considerados mínimos para que a dinâmica concorrencial de um mercado seja alterada, até a análise desenvolvida e posteriores resultados. Procurar-se-á, a partir desse entendimento, explorar os pontos atinentes a todas essas etapas, iniciando, assim, apelos critérios de notificação.

2.4 – Critérios de notificação de Atos de Concentração e Big Data

O primeiro tipo de controle levado a cabo pelas autoridades antitruste a ser abordado nesta análise será o prévio, também denominado de controle de estruturas. Conforme também já abordado, o controle de estruturas é aquele realizado pela autoridade por ocasião de fusões, aquisições, incorporações ou formação de *joint-ventures* entre empresas. O controle da autoridade antitruste, no entanto, só se realiza mediante o preenchimento pela operação de alguns critérios. No caso brasileiro, tais critérios se encontram elencados no art. 88 da Lei do Cade, a Lei 12.529 de 2011. De maneira geral, os critérios de notificação dizem respeito a um faturamento mínimo obtido pelas empresas envolvidas na operação – qual seja de que ao menos uma das empresas envolvidas na operação apresente faturamento bruto anual ou volume de negócios total no país, no ano anterior à notificação, equivalente ou superior a R\$ 750.000.000,00 (setecentos e cinquenta milhões de reais), e a outra de ao menos R\$ 75.000.000,00 (setenta e cinco milhões).

³⁰ Fonte: <<https://www.techtudo.com.br/noticias/2019/01/o-que-e-duckduckgo-concorrente-do-google-promete-mais-privacidade.ghtml>>. Acesso em 3 de maio de 2019.

Além do critério de faturamento das empresas, vale ressaltar que o Cade possui dois procedimentos principais a fim de realizar o controle prévio de operações, sendo um deles denominado ordinário e o outro sumário, sendo este segundo destinado a procedimentos mais simplificados. As hipóteses de enquadramento no procedimento sumário estão elencadas nas resoluções de nº 2 e 9 do Cade. De maneira geral, as operações que (i) resultem em *joint-venturs* em mercados não horizontal ou verticalmente relacionados às empresas participantes da operação; tratem (ii) de uma consolidação de controle ou de (iii) uma substituição de agente econômico, ou que acarrete numa sobreposição horizontal e (iii) resulte numa baixa participação de mercado, de *share* abaixo de 20% ou (iv) numa variação de HHI inferior a 200 desde que valor de *share* não ultrapasse 50%, devem ser objeto de procedimento sumário.

Nota-se, desta feita, que a lei trouxe critérios bastante objetivos de notificação, econômicos. Ocorre, no entanto, que a realidade econômica advinda junto à era digital não mais responde aos critérios anteriormente elencados como suficientes para dirimir questões concernentes à concorrência.

Um exemplo que ilustra muitíssimo bem o cenário de descompasso entre os atuais critérios de notificação e o funcionamento dos mercados digitais é o concernente às empresas mavericks. Ora, quando ainda se encontram incipientes, tais empresas mesmo antes de serem capazes de atingir os atuais critérios de faturamento já costumam ser alvo de empresas de maior porte, sendo adquiridas por estas. As empresas de maior porte, ao enxergar o potencial de desenvolvimento das companhias melhores, assim, entendem vantajoso adquiri-las para não apenas desenvolver seus produtos, mas, ainda eliminar uma empresa que possivelmente venha a, num futuro, ainda que não imediato, constituir uma concorrente, uma ameaça a seu modelo de negócio – ou seja, empresas maiores, como forma de melhor manterem-se como dominantes, ou mesmo como empresas relevantes dentro de determinado mercado, acabam adquirindo outras a fim de eliminar sua concorrência potencial.

A partir da compreensão do conceito relativo à concorrência real, pode-se melhor entender do que se trata a concorrência potencial³¹. Enquanto a concorrência

³¹ HASENCLEVER, LIA; KUPFER DAVID. Economia industrial, Fundamentos teóricos e práticas no Brasil. Editora Elsevier, 2ª Edição revista e ampliada, 2003. Disponível em: <<https://books.google.com.br/books?id=hisDwAAQBAJ&pg=PT146&dq=concorr%C3%Aancia+potencial&hl=pt-BR&sa=X&ved=0ahUKewiQoIiM-5DhAhW1LLkGHevXCBSQ6AEILDAA#v=onepage&q=concorr%C3%Aancia%20potencial&f=false>> acesso em 20.03.2019

real diz respeito ao número e tamanho relativo das diversas empresas que constituem um mercado, a potencial diz respeito a competição por lucros entre empresas já estabelecidas em num mercado, bem como às novas empresas interessadas em iniciar uma operação em determinado mercado. A concorrência potencial possui base numa perspectiva mais clássica econômica, de acordo com a qual se uma empresa apresenta lucros elevados, o previsto é que novas empresas queiram entrar neste mercado, a fim de compartilhar desses lucros obtidos. De forma complementar, um mercado deficitário tenderá ao encerramento de atividade das empresas, a fim de que se movam para mercados mais atraentes.

Os mercados superavitários, que atraem novos entrantes, contarão com um aumento na oferta de produtos, e, conforme posto pela Lei da oferta e demanda, os preços referentes aos produtos que constituem tal mercado deverão baixar, tornando-o um mercado eficiente. De maneira complementar, os mercados deficitários contarão com uma retração da entrada, que levará a um consequente aumento de preço por parte daqueles agentes que se mantiveram, elevando os lucros destes.

Nesse sentido, a ameaça potencial de que uma companhia “capture” os recursos de outra, de que possa a ser uma ameaça a seus lucros, ao total de lucro que possa ser extraído, faz com que empresas acabem comprando outras, com o intuito de cessar tal ameaça. Além da dificuldade em mitigar operações que minem a concorrência potencial, que, muito embora se constitua num problema concorrencial relevante não abarca a questão dos dados pessoais, questão à qual se quer dar enfoque. Assim, importante notarmos outros problemas concernentes à objetividade dos critérios de notificação, e verificar, além dos elencados, quais outras dificuldades merecem ser abordadas a fim de mitigar eventuais problemas concorrenciais gerados pela ausência de uma efetiva e eficaz proteção de dados pessoais.

Um caso bastante célebre acerca da problemática referente aos critérios de notificação que envolvem as empresas de tecnologia é o referente à aquisição do Instagram pelo Facebook. As empresas, à época da aquisição, no ano de 2012, não possuíam faturamento suficiente para que a compra fosse submetida à análise das autoridades concorrenciais. De lá para cá, no entanto, juntou-se ao grupo de aplicativos detidos pelo Facebook a plataforma do WhatsApp, e a viabilidade de unir as bases de

dados relativos ao coletado por estes três gigantes foi objeto de manchetes internacionais³².

A Comissão Europeia, no entanto, muito embora tenha realizado a análise, em 2014, da aquisição do WhatsApp pelo Facebook, já aplicou multa com relação às companhias por considerar que estas não haviam fornecido todas as informações que deveriam relativas à proteção de dados³³. Naquela ocasião, as empresas tinham afirmado não ser possível o reconhecimento de usuários de uma plataforma para outra, de maneira com que seria impossível a integração das contas e dos dados ligados a elas.

Anos depois, em fevereiro de 2019, o grupo anunciou a integração dos aplicativos de mensagens relativos às suas três principais plataformas, quais sejam o Instagram, o Facebook e o WhatsApp³⁴, que passariam até 2020 a atuar de forma integrada. Nesse sentido, um usuário ativo do Facebook poderia receber uma mensagem enviada por um usuário do WhatsApp, ainda que não tivesse conta registrada na plataforma referente ao WhatsApp. Tal anúncio, também vale elencar, foi alvo de providências por parte de autoridades do mundo inteiro, incluindo o Brasil³⁵ que levarão a cabo investigações a respeito da integração desses dados.

Além dos já conhecidos problemas advindos das concentrações econômicas, no âmbito das *data-driven organisations* a situação ainda conta com dois outros possíveis agravantes: a possibilidade de retração de inovações, tendo em vista o poder de mercado das Big Techs. Outro enorme agravante, que deve ser levado em conta quando da notificação de Atos de Concentração diz respeito à conduta das empresas que, a fim de minar uma possível concorrência, logo compram start-ups inovadoras e eficientes, antes que essas adquiram porte mínimo, a um só tempo incorporando suas inovações e deixando de se preocupar com a possível ameaça que tal novidade possa vir a oferecer a seu modelo de negócio.

³² Fonte: <<https://www.techtudo.com.br/noticias/2019/02/facebook-whatsapp-e-instagram-serao-integrados-confirma-zuckerberg.ghtml>>. Acesso em 3 de maio de 2019.

³³ Fonte: <<https://www.theguardian.com/business/2017/may/18/facebook-fined-eu-whatsapp-european-commission>>. Acesso em 7 de maio de 2019.

³⁴ Fonte: <<https://www.techtudo.com.br/noticias/2019/02/facebook-whatsapp-e-instagram-serao-integrados-confirma-zuckerberg.ghtml>> Acesso em 7 de maio de 2019.

³⁵ Fonte: <<https://link.estadao.com.br/noticias/empresas,mp-abre-investigacao-sobre-integracao-de-messenger-instagram-e-whatsapp,70002751682>> Acesso em 7 de maio de 2019; <<https://www.theguardian.com/technology/2019/jan/28/eu-data-watchdog-raises-concerns-facebook-integration>> Acesso em 7 de maio de 2019.

2.5 - Risco de perda de inovações e demais problemas ligados às *data-driven companies*

Com relação ainda às companhias movidas a dados, no concernente às aquisições de empresas envolvendo Big Data, muitos dos riscos enfrentados dizem respeito às inovações nestes mercados. Isso porque, diante de inovações que signifiquem uma maior invasão a seus dados pessoais, usuários podem sentir-se ameaçados, fazendo com que a empresa opte por utilizar algoritmos que impliquem nesta invasão, sem necessariamente patenteá-los ou torná-los públicos.

Além disso, com acesso a dados produzidos por usuários em todo o mundo, as *data-driven companies* poderiam, por exemplo, por meio do monitoramento de pesquisas feitas, perceber a iminência do ingresso de uma nova tecnologia, antever outra inovação, e até mesmo percorrer os mesmos caminhos de potencial concorrente a fim de chegar a tal inovação antes dos demais, ou até mesmo antes do ingresso dessa nova tecnologia no mercado. Além disso, não se pode excluir a possibilidade de que tais empresas percebam um aumento no acesso a outros sites, ainda incipientes, pelos usuários, e se movam no sentido de adquiri-los e evitar um grande futuro enfrentamento a esta empresa como competidora em seu mercado de atuação.

Por fim, os maiores problemas futuros com os *data-opolies* dizem respeito, em verdade, a questões morais, éticas e políticas. Sabe-se que estas empresas trabalham com algoritmos capazes de prever eventos de nossas vidas³⁶, bem como qual tipo de conteúdo ou produto estamos mais inclinados a aderir e adquirir³⁷, e assim monetizam sua atividade direcionando propagandas que nos sejam mais “atrativas” e “úteis”, destes produtos que estamos mais inclinados a adquirir. Assim, há uma preocupação bastante importante com relação aos *data-opolies*, de que estes sejam capazes de prever nossos passos e nos entender a um ponto que percamos a autonomia, de maneira com que nosso futuro seja cada vez mais determinado pelo que tais empresas nos sugerem e apresentam.

Há diversos casos, que haverão de ser tratados mais a frente, acerca da possibilidade de o Google restringir a competição por meio da forma com que dispõe produtos em seu site de busca. Uma vez que os primeiros resultados seriam aqueles a

³⁶ Fonte: <<https://www.nytimes.com/interactive/2018/06/21/opinion/sunday/facebook-patents-privacy.html>> Acesso em 21 de março de 2019

³⁷ Fonte: <<https://www.bbc.com/portuguese/geral-43493673>> Acesso em 15 de março de 2019

primeiro serem verificados pelo usuário, há acusação de que o Google direciona usuários ao consumo de produtos de sua plataforma em detrimento das demais³⁸.

A eleição de 2016 nos Estados Unidos da América mostra um cenário em que o conhecimento a respeito dos dados dos usuários poderia não apenas influenciar no resultado final das urnas³⁹, como determiná-lo. Naquela ocasião, o mundo experimentou pela primeira vez uma eleição tomada por *fake news*, que, embora em sua maioria trouxessem conteúdo absolutamente absurdo como sendo real, levaram as pessoas a acreditar nestes e se alardearem, e tomarem posições baseadas em tais inverdades. O mesmo, aliás, foi experimentado na eleição de 2018 aqui no Brasil, ocasião em que diversas notícias falsas espalhadas especialmente por WhatsApp levaram a uma polarização de certa parcela da população⁴⁰. A epidemia relativa às *fake news* somada à possibilidade de se discriminar e direcionar tais notícias podem trazer efeitos absolutamente desastrosos para o mundo como um todo.

As empresas poderiam, inclusive, direcionar notícias, pesquisas e estudos em seu próprio benefício, selecionando aquilo que lhe é mais favorável a respeito de determinado cenário, agindo de modo a não apenas vender a outras empresas tais vantagens, como fazer uso dessas práticas para manter seu poder de mercado, influenciando decisões tanto na esfera privada quanto nas esferas nacionais e internacionais.

2.7 - Aquisições estratégicas de empresas como instrumento de obtenção de bases de dados e a evolução da análise pela autoridade europeia: Do caso Google/DoubleClick ao caso Apple/Shazam

Com relação às aquisições efetuadas no âmbito dos setores ligados aos dados pessoais e tecnologia, tem-se a possibilidade da realização de tais aquisições com o intuito de integrar a base de dados de um concorrente à sua, como já tratado anteriormente. Tais aquisições poderiam, como também apontado, permitir a criação de *data-polies*, espécies de concentrações capazes de trazer imensos prejuízos, numa

³⁸ Fonte: <<https://www.valor.com.br/empresas/5666281/uniao-europeia-prepara-maior-multa-contra-o-google>> Acesso em 21 de março de 2019

³⁹ Fonte: <<https://forbes.uol.com.br/negocios/2016/11/como-boatos-ajudaram-a-eleger-donald-trump-nos-eua/>> Acesso em 21 de março de 2019

⁴⁰ Fonte: <<https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml>> Acesso em 21 de março de 2019

proporção com que a experiência já vivida nesses mercados ainda não consegue ser capaz de mensurar.

A aquisição de empresas de tecnologia por outras em que a questão relativa aos dados constituiu enorme preocupação, já foram objeto de apreciação e análise por boa parte das autoridades concorrenciais no mundo. Abaixo, assim, tenta-se tratar das análises realizadas por autoridades concorrenciais, a fim de perceber sua evolução no tratamento do tema. Para tal fim, escolheu-se tratar da mais antiga aquisição com características ligadas ao tratamento e aquisição de dados pessoais (entre o Google e a Doubleclick) e da operação mais recente finalizada (entre a Apple e o Shazam), de modo com que a comparação na abordagem possa ser mais palpável.

2.7.1 – Operação Google/Doubleclick

Pois bem, uma das primeiras aquisições de empresas envolvendo companhias detentoras de grande quantidade de dados foi a realizada pelo Google com a aquisição da DoubleClick, empresa fornecedora de serviços publicitários online, operação esta ocorrida entre os anos de 2007 e 2008, aprovada pelas autoridades antitruste ao redor do mundo.

É importante perceber a enorme dimensão de tal aquisição, que, à época, não apenas permitiu ao Google uma expansão em sua base de dados, como ainda garantiu um aperfeiçoamento dos serviços de propaganda do Google. Nesse sentido, a empresa garantiu a capacidade de colher mais dados, a fim de melhor analisá-los e devolver uma resposta mais eficiente para o anunciante e para o consumidor. Desta feita, com maior acesso e análise de dados, bem como com a expansão do serviço e tipo de propaganda fornecido, o Google passou a anunciar produtos mais relevantes a seus consumidores, aumentando concomitantemente a chance de que os produtos anunciados fossem adquiridos, fazendo crescer, portanto, o número de vendas e lucro daqueles que contrataram o serviço de anúncio do Google.

Muito embora tal operação tenha tido essa magnitude para o Google, sua abordagem em verdade se consubstancia em razão de ter sido uma das – se não a – primeiras grandes operações envolvendo Big Data e análise de dados pessoais a enfrentar o crivo de autoridades anticoncorrencias. Naquela ocasião, portanto, a questão relativa aos dados pessoais constituía uma novidade e uma característica importante a

mais a ser considerada para possíveis fins, impactos e resultados na concorrência efetuada entre as empresas do mercado tratado, bem como na assunção do bem-estar e proteção dos consumidores.

O Google fornecia, ao tempo da operação, espaço publicitário em seus próprios sites e/ou em sites parceiros. Dessa maneira, a maior parte da receita do Google era proveniente da venda de espaços para publicidade online destinados a anúncios de texto em seu próprio site, bem como anúncios de texto na rede de outros editores, que utilizam os programas de publicidade e busca do Google para colocar anúncios relevantes em seus websites quando realizada uma busca.⁴¹

O Google teria, em verdade, dois produtos para anunciantes, o “AdWords” e o “AdSenses”. No primeiro, os anunciantes calculavam o valor que desejavam pagar por “clicks” em determinadas palavras chaves. O mecanismo automatizado do Google, então, escolheria os anúncios a serem veiculados nas pesquisas por tal palavra chave baseados no preço pago por click. Quando o usuário iniciava uma pesquisa no Google usando uma das palavras chave do anunciante, o anúncio aparecia próximo às páginas de resultado da busca.

O "AdSense", outro serviço oferecido pelo Google, representava um produto para agentes divulgadores, por meio do qual o Google veiculava anúncios de textos e de imagens relevantes que fossem relacionados com o conteúdo do site do agente de divulgação. Desse modo o agente de divulgação ao adicionar uma caixa de busca do Google em seu site, concordaria em permitir que fossem veiculados anúncios de textos relevantes que fossem relacionados com as páginas de resultado de busca geradas pelo pedido do usuário⁴².

Na outra ponta da operação, se encontrava a DoubleClick, empresa especializada no fornecimento de serviços ligados à oferta de impressões de anúncios ilustrados, isto é, à visualização de anúncios em uma página da web. Tal serviço é mais ligado à venda de espaço publicitário. Em suma, os anunciantes criam anúncios e os enviam para o servidor de publicidade para anunciantes. Caso o editor de website concordasse – de forma direta ou através de uma rede de anúncios e de troca - em exibir os anúncios criados em seu website, este firmava os termos da campanha para o anúncio (por exemplo, alocação, preço, critério de destinação, etc.) com o servidor de

⁴¹ Fonte: Parecer nº 06612/2Q07/RJ COGCE/SEAE/MF, constante do Ato de Concentração nº 08012.005304/2007-11

⁴² Fonte: Formulário de notificação ao CADE do Ato de Concentração nº 08012.005304/2007-11

publicidade para editores. O editor também identificava os diferentes espaços disponíveis, direcionando os locais em que tais anúncios eram dispostos nas páginas.

Assim, no momento em que um usuário acessava a página do editor, o código de identificação requisitava ao servidor de publicidade para editores a visualização do anúncio. O servidor de publicidade para editores registrava a requisição para visualização, determinava qual anunciante usar e, a menos que o anúncio não exigisse servidor, era efetuada uma solicitação ao servidor de publicidade para anunciantes, que, por sua vez, selecionava o anúncio apropriado e o disponibilizava ao espaço apropriado na página da web.

No momento em que o anúncio era visualizado na página do editor, tais sistemas permitiam que o arquivo de texto fosse colocado no navegador do usuário – um cookie –, que geravam relatórios ao anunciante acerca da eficiência de sua campanha. O cookie, desta feita, possibilitava elaboração de relatórios de monitoramento da atividade do usuário em seu site nos dias subsequentes à visualização do anúncio. Estes relatórios permitiam aos anunciantes que tomassem decisões mais embasadas sobre estratégia de publicidade e de compra de espaço em meios de comunicação. A DoubleClick à época da operação, portanto, vendia soluções tecnológicas a anunciantes, agências publicitárias e editores da web para o oferecimento de anúncios ilustrados nos websites e para o gerenciamento e apresentação de relatórios sobre a eficiência daqueles anúncios.⁴³

Quando da análise desta operação, a Comissão Europeia entendeu que os mercados relativos a cada um dos sites não estariam diretamente relacionados⁴⁴. Essa conclusão deu-se em primeiro lugar porque o Google forneceria uma publicidade agregada, não direcionada, enquanto a DoubleClick, a partir do uso de cookies, conseguia exercer um direcionamento publicitário. Para chegar nesta conclusão, a comissão analisou que⁴⁵ (i) o preço nos serviços ofertados por uma delas não

⁴³ Fonte: Parecer nº 06612/2Q07/RJ COGCE/SEAE/MF, constante do Ato de Concentração nº 08012.005304/2007-11

⁴⁴ “While the “products” that the parties offer do not compete directly, the combination of these products are substitute solutions from the point of view of publishers and advertisers.”. Decisão da Comissão Europeia acerca da operação, parágrafo 193.

⁴⁵ The main reasons why the Commission does not believe that the parties' constrain each other in a “horizontal” sense are set out below: (i) the cost of ad serving services represents a very small part of the total cost of unbundled solutions and therefore, the degree to which the parties' product did constrain each other's pricing pre-merger was minimal; (ii) DoubleClick faces strong competition from other ad serving companies and these direct competitors are the main constraint on DoubleClick's pricing; and (iii)

influenciava de forma significativa o preço praticado pela outra; (ii) a DoubleClick enfrentava uma concorrência direta por parte de outras empresas pouco mais pesada que aquela exercida pelo Google, concorrência que aí sim influenciava no preço praticado por essa; e (iii) o Google fornecia espaço publicitário a anúncios a fim de que estes aparecessem em pesquisas - contextuais, portanto - elencados na página e visualizados a partir da efetuação de uma busca. A Double Click, de outro modo, fornecia publicidade baseada em anúncios gráficos, não contextuais. A presença do Google na intermediação do tipo de anúncio, mormente veiculado pela DoubleClick, notadamente os de anúncios gráficos, sequer correspondia, à época da operação, a 1% do mercado analisado, conforme a decisão.

Com relação à análise referente à concorrência potencial entre as duas empresas, a decisão tomada no âmbito da Comissão Europeia ressaltou que para a realização de tal análise, seria necessário o preenchimento de dois requisitos por uma das empresas, quais sejam (i) a existência de uma significativa probabilidade de o potencial concorrente se tornar uma força competitiva efetiva e (ii) haver um número insuficiente de outros concorrentes capazes de manter uma pressão concorrencial suficiente após a concentração⁴⁶. Entendeu-se, assim, que muito embora a DoubleClick pudesse crescer de maneira a preencher o primeiro critério, ela enquanto nova entrante não encararia somente o Google neste mercado, mas também outros concorrentes de peso, tais como Microsoft, AOL, Yahoo!, TradeDoubler, Zanox, AdLink, Interactive Media, Tomorrow Focus, Oridian, dentre outros.⁴⁷

Google's bundled solution and an unbundled solution including DoubleClick's products are not close competitors. *Idem*, parágrafo 194

⁴⁶ “The relevant question however is whether the elimination of DoubleClick as a potential competitor in the market for online ad intermediation and in the provision of bundled online ad intermediation and ad serving services may significantly impede effective competition. To this purpose, it must be noted that the guidelines on the assessment of horizontal mergers¹²⁶, in paragraph 60, clearly indicate that two conditions must be fulfilled: first, there must be a significant likelihood that the potential competitor would have grown into an effective competitive force and second, that there would be an insufficient number of other competitors left which could maintain sufficient competitive pressure after the merger”. *Idem*, parágrafo 224.

⁴⁷ “It can be concluded from the above that, despite Google's strong market position in intermediation, the proposed merger does not have significant anticompetitive effects with a view to the elimination of DoubleClick as a potential competitor of Google. While it is not excluded that DoubleClick would have grown into an effective competitive force in online ad intermediation services, it is rather likely that a sufficient number of other competitors would be left in the market which could maintain sufficient competitive pressure after the merger. DoubleClick would still be a new entrant which would face not only Google, but also other companies such as Microsoft, AOL, Yahoo!, TradeDoubler, Zanox, AdLink, Interactive Media, Tomorrow Focus, Oridian and ValueClick who also possess strong advantages, including, for some of these players, (in-house) ad serving technology, and are far more advanced in the development of their intermediation services”. *Idem*, parágrafo 278

Com relação à possibilidade de entrada do Google no mercado mormente dominado pela DoubleClick, entendeu-se que uma entrada seria improvável, em razão de o Google até aquele momento ainda não dominar a tecnologia utilizada pelos demais agentes ao direcionamento de propagandas⁴⁸. Além disso, ainda que o Google entrasse neste mercado, ele também contaria com uma pesada concorrência para se estabelecer⁴⁹.

Assim, entendeu-se que não haveria concorrência real ou potencial entre as duas companhias, e, por isso, por não pertencerem a um mesmo mercado, não havia que se falar na ocorrência de sobreposição horizontal ou qualquer efeito.

Analisada a primeira hipótese de fechamento, baseada na posição ocupada pelo Google em seu respectivo mercado relevante, a Comissão entendeu que o Google se assim quisesse agir, dado seu poder de mercado, poderia o fazer mesmo sem adquirir a DoubleClick, de maneira com que a operação não geraria efeitos negativos neste cenário⁵⁰. Com relação à hipótese de fechamento de mercado baseada na posição da DoubleClick, a autoridade entendeu que a empresa não estaria apta a exercer poder de mercado, que os *switching costs* envolvidos num eventual abandono da plataforma eram gerenciáveis, que o serviço oferecido de veiculação de anúncios representaria uma pequena porção dos custos e receitas envolvidas na atividade desta empresa e que os efeitos de rede, neste caso, não seriam suficientemente fortes⁵¹.

A Comissão Europeia verificou a possibilidade de adoção de estratégias fechamento de mercado baseadas tanto na posição ocupada pelo Google no mercado de busca e intermediação de anúncios, quanto na posição da DoubleClick. Além disso,

⁴⁸ “The technology used in Google’s existing advertising business is different from the technology used in publisher and advertiser ad serving products like GFA and GFP.”. Idem, parágrafo 281.

⁴⁹ “Even if Google’s display ad serving products under development were to succeed, they would become one of many competitors acting in the display ad serving.” Idem, parágrafo 285.

⁵⁰ “As Google could do the same already today, the merger does not change Google's incentive to engage in this wider form of bundling to any significant extent.” Idem, parágrafo 355

⁵¹ “To sum up, the Commission has examined the potential for anti-competitive foreclosure arising from the acquisition by Google of DoubleClick, a leading ad serving tool provider. The theories of harm were based on both the vertical and conglomerate dimensions of the merger and focused on strategies through which the new entity might use the leading position of DoubleClick to enhance the market position of Google's intermediation platform at the expense of rivals and ultimately of consumers. These theories of harm relied on a number of assumptions regarding the characteristics of the markets under consideration, such as DoubleClick's degree of market power, the level of switching costs, the presence of direct and indirect network effects and the share of ad serving in the costs of intermediation. The market investigation has revealed that DoubleClick is not able to exercise a significant degree of market power, that switching costs are manageable, that ad serving represents a small proportion of ad costs/revenues and a limited proportion of intermediation revenues and that network effects are not strong enough to induce tipping. In such circumstances, it is unlikely that the new entity would have the ability or incentives to engage in foreclosing strategies and that any such strategy, if implemented, would lead to the marginalisation of rival ad networks and ad exchanges to the detriment of consumers.”. Idem, parágrafo 329.

também explorou a possibilidade de fechamento baseadas na integração dos ativos das duas companhias, afastada pela improbabilidade de que a operação trouxesse maior tráfego de propagandas ao Google, que excluísse concorrentes ou de que houvesse um significativo aumento nos preços dos serviços fornecidos.

A análise levada a cabo pela Comissão Europeia, muito embora considerando a questão ligada a privacidade dos dados dos usuários, acabou por não se aprofundar muito no tema, entendendo que os dados coletados pelas empresas da operação, diante da quantidade de dados detidos por todos os agentes do mercado e diante da obrigatoria submissão das partes às regras referentes à privacidade de dados pessoais em vigor na época, não constituiria ponto de maior atenção⁵². Uma análise distinta, no entanto, foi feita pela Federal Trade Commission (FTC), autoridade responsável pela análise atinente ao controle de estruturas nos EUA.

O FTC, após 8 (oito) meses investigando a questão concluiu que questões ligadas à privacidade de dados não tinham a força necessária para impedir a aprovação desta operação⁵³. O FTC entendeu que todas as preocupações direcionadas à questão da privacidade de dados levantadas por terceiros com relação à operação, em verdade travestiriam o medo dos concorrentes de que o Google, após a aquisição da DoubleClick, passasse a oferecer um produto superior. Além disso, frisaram que tais

⁵² “Internet service providers can track all of the online behaviour of their users, following them to every website they visit. Particularly large internet service providers could thus try to team up with advertisement companies to make use of this data under the restrictions imposed by privacy rules, but they could also try to use this data with their customers' consent, for instance in exchange for lower prices. Several companies offer appliances for "deep packet inspection" of network traffic routed through internet service providers in order to extract information that is meaningful for ad targeting¹³⁸. Data collected in this way is potentially much broader and richer than data collected by DoubleClick (or even the merged entity) or any of its rivals because contrary to the merged entity's data collection efforts, this data source covers every page on every site a user visits.” Idem, parágrafo 271. “In any event, this Decision is without prejudice to the obligations imposed onto the parties by Community legislation in relation to the protection of individuals and the protection of privacy with regard to the processing of personal data, in particular Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ¹⁸⁵ and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)¹⁸⁶ and Member States implementing legislation, which apply to the processing of personal data activities performed by the parties to the merger and by the entity resulting from the merger operation. Irrespective of the approval of the merger, the new entity is obliged in its day to day business to respect the fundamental rights recognised by all relevant instruments to its users, namely but not limited to privacy and data protection.” Idem, parágrafo 368

⁵³ “we investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy. We have concluded that the evidence does not support a conclusion that it would do so. We have therefore concluded that privacy considerations, as such, do not provide a basis to challenge this transaction.” Idem, parágrafo 369

dados não influenciaram nenhuma das duas companhias a adquirirem as posições detidas em seus respectivos mercados à época da operação.⁵⁴

O Cade, por sua vez, por ocasião da análise deste Ato de Concentração no Brasil, decidiu pela aprovação sem restrições, entendendo não haver qualquer sobreposição horizontal ou evidências acerca da possibilidade de possíveis efeitos nocivos advindos da integração entre ambas, havendo o Conselheiro Relator Fernando Furlan citado as análises americana e europeia para embasar sua conclusão.

Fato é, no entanto, que o Google de fato acabou por adotar condutas abusivas relativas ao direito à privacidade de seus usuários, que passaram a ser rastreados por meio de cookies sem seu consentimento. O próprio FTC em 2012 aplicou uma multa no valor de US\$ 22,5 milhões de dólares por conta do abuso em serviços do Google envolvendo a utilização de cookies – tecnologia adquirida e explorada pela empresa somente a partir da aquisição da DoubleClick.⁵⁵ Restou-se assim evidenciada a incapacidade das autoridades antitruste de, naquele contexto, perceberem a nocividade intrínseca ao tratamento de dados pessoais de usuários para fins anticompetitivos, pois mesmo tendo sido realizada uma análise acerca da questão relativa aos dados pessoais, as autoridades antitruste não conseguiram prever problemas que dali a dois anos ensejariam uma condenação ao Google.

Fato é que nestes quase 12 anos após a notificação da operação entre o Google e a DoubleClick, o mundo não apenas começou a atentar-se para questões relativas aos dados pessoais de usuários, como ainda passou a entender diversas questões ligadas ao assunto, de forma com que hoje diversos países já possuem legislações que tratam do tema e estabelecem parâmetros mínimos a fim de mitigar os problemas relativos aos Data-polies. Passemos, assim, à análise de operação realizada já durante a vigência do GDPR.

⁵⁴ “At bottom, the concerns raised by Google’s competitors regarding the integration of these two data sets – should privacy concerns not prevent such integration – really amount to a fear that the transaction will lead to Google offering a superior product to its customers. Yet, the evidence indicates that neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product. A number of Google’s competitors have at their disposal valuable stores of data not available to Google. For instance, Google’s most significant competitors in the ad intermediation market, Microsoft, Yahoo!, and Time Warner have access to their own unique data stores. These firms own popular search engines, and will have access to consumer information from their internal ad servers, ad intermediation services, other web properties, and software. The entry and expansion of these well-financed competitors has transformed the ad intermediation marketplace over the last six months. All of these firms are vertically integrated, and all appear to be well-positioned to compete vigorously against Google in this new marketplace.” Idem, parágrafo

⁵⁵ Fonte: <<https://nakedsecurity.sophos.com/pt/2012/11/20/judge-approves-22-5m-google-fine-for-violating-safari-privacy/>> Acesso em 15 de março de 2019

2.7.2 – Operação Apple Music/Shazam (2018)

Dada a análise e os resultados fornecidos a partir da operação entre Google e Doubleclick, muito aconteceu e mais casos envolvendo a proteção e dados pessoais foram ocorrendo. Como é objeto de discussão durante todo este trabalho, nem todas as operações ocorridas passaram por análise concorrencial, tendo em vista o não preenchimento de critérios de notificação, como aquele relativo ao faturamento, a título de exemplo. Tal característica, no entanto, não torna estas operações desprovidas de potencial lesivo, de maneira com que as autoridades do mundo inteiro ainda estão, a partir de tais experiências, delimitando *standards* ao tratamento de dados pessoais. Nesse sentido, busca-se neste tópico realizar a análise da operação mais recente já finalizada pelas autoridades antitruste, e que, ao mesmo tempo, precisem passar pela análise dos impactos relativos à proteção de dados pessoais e ao Big Data.

A mais recente aquisição entre gigantes da tecnologia, portanto, aconteceu com a aquisição do aplicativo Shazam pela Apple, aprovada no âmbito da Comissão Europeia em 6 de setembro de 2018. Tal operação, no entanto, não foi objeto de análise pela autoridade antitruste brasileira e pelo FTC, de maneira com que a análise aqui levada a cabo se limitará a elencar os principais pontos da decisão tomada pela Comissão Europeia.

Em primeiro lugar faz-se necessário entender os mercados de atuação de cada uma das empresas. A Apple é uma empresa que atua nos mercados de design, desenvolvimento e manufatura de dispositivos de comunicação móvel e mídia (tal qual o “iPhone”, o “iPad” e a “Apple Tv”, por exemplo) quanto computadores pessoais (o “iMac”). Além disso, atua no mercado de desenvolvimento de sistemas operacionais, aplicativos, assistentes pessoais (como é a “Siri”) e de conteúdo digital, oferecendo, ainda, serviços de streaming musical por meio da “Apple Music”.

No outro lado da operação, o Shazam atua como desenvolvedor e distribuidor de um aplicativo para *smartphones*, *tablets* e computadores pessoais capaz de reconhecer músicas diversas. A receita deste aplicativo era, ao tempo da operação, gerada por meio (i) de propagandas constantes do display do aplicativo, (ii) parcerias com terceiros, (iii) comissões recebidas por meio de usuários de serviços de streaming –

como a Apple Music – licenciamento de dados musicais bem como serviços de análise de tais dados.⁵⁶

A Comissão Europeia, desta feita, promoveu uma análise do mercado de distribuição e streaming digitais de música, concluindo que as duas empresas não pertenciam a um mesmo mercado relevante.⁵⁷ De acordo com a análise, a indústria do *streaming* foi a responsável pelo reerguimento de toda a indústria musical, tornando-se uma lucrativa solução digital à transformação do mercado, que não mais faturava a partir de outros produtos anteriormente relevantes, como os CDs.⁵⁸ O mercado de streaming, assim, adquire lucro por meio de propagandas feitas no meio da reprodução àqueles usuários que usufruem do serviço de forma gratuita, tendo a opção de que o usuário adquira um pacote Premium, por meio do qual, mediante uma contribuição mensal, possui acesso às músicas constantes com algumas outras regalias, como o de não ter seu streaming interrompido por propaganda, poder realizar o download de uma quantidade de material, dentre outros. Além disso, é considerado um mercado em expansão.⁵⁹

A referida investigação também se debruçou no mercado em que atua o Shazam, que usa o microfone dos dispositivos para reconhecer conteúdos de áudio e vídeo, possibilitando que o som possa ser identificado em meio a uma grande base de

⁵⁶ “Apple designs, manufactures and sells mobile communication and media devices (such as the "iPhone", the "iPad", the "Apple TV") as well as personal computers (the "Mac"). It also develops a variety of operating systems ("OSs"), which are installed on the hardware of the devices and personal computers ("PCs") it sells ("macOS" for Macs, iOS for smart mobile devices, “watchOS” for smart watches and “tvOS” for smart TVs), as well as other software solutions and mobile application software solutions (“apps”), including for example a virtual assistant software solution ("Siri"). Moreover, Apple sells services, peripherals, networking solutions, and third-party digital content. In particular, Apple sells and delivers digital content online through the "iTunes Store", the "App Store", the "iBook store" and the "Mac App Store", and offers the music and video streaming service through the app "Apple Music".” “Shazam is a developer and distributor of music recognition apps for smartphones, tablets and personal computers, branded “Shazam”. 5 It generates revenues from (i) the display of online advertising, (ii) partnerships with third parties, (iii) commissions earned on referrals of users to digital music streaming and download services, such as Apple Music, and (iv) licensing of music data and analytics services.” Fonte: Decisão da Comissão Europeia, parágrafos 3 e 4.

⁵⁷ “The industry sector on which the Commission has assessed the impact of the Concentration on competition is the digital music sector, where both Parties are active players, albeit with different roles (as further explained in the following subsections).” Idem, parágrafo 19.

⁵⁸ “After more than a decade of declining revenues in music distribution, the global recorded music industry has in recent years recovered and experienced continuous growth, with total revenues rising from USD 14.2 billion in 2013 to USD 17.3 billion in 2017. s growth was largely driven by digital music streaming services, whose revenues surpassed those of digital music downloads in 2016.” Idem, parágrafo 28.

⁵⁹ “During the market investigation, several market respondents, such as [...]31 and [...]32 , explained that at this stage of the market, growth typically comes from first-time subscribers to music streaming services rather than users who were previously subscribers of competing music streaming services. Also [...] considered that its main strategic focus was acquiring new users rather than attracting competitors' users to its service.”

dados, o que, como resultado final, vai permitir que o usuário saiba a proveniência daquilo que escuta sem ter um conhecimento prévio anterior acerca daquele material.

Na análise levada a cabo pela Comissão Europeia referente a essa operação apresenta uma abordagem tanto quanto distinta dos dados envolvidos daquela levada a cabo pelo mesmo órgão na análise da fusão entre o Google e a DoubleClick. Em primeiro lugar a Comissão identificou os tipos de dados que os aplicativos do mercado relacionado à distribuição digital de música eram capazes de recolher, sendo estes (i) os ligados ao dispositivo, como o tipo de sistema operacional, o número de dispositivos ligados a uma mesma conta, dentre outros, (ii) dados demográficos, relativos a por exemplo o gênero e idade dos usuários, e (iii) dados comportamentais, ligados à quantidade de tempo gasta pelos usuários com o uso de seus dispositivos, bem como os artistas que mais escutam, gênero, dentre outros. Ainda de acordo com a Comissão, tais dados são utilizados para quatro finalidades distintas, quais sejam (i) o desenvolvimento de novos métodos e tecnologias para entrega do produto ao usuário, (ii) a geração de dados para análise do mercado, (iii) a possibilidade de o artista entender seu desempenho ante os usuários (iv) a identificação e previsão do que será tendência o do que será “hit”, (v) maior entendimento da predileção dos usuários para direcionamento de conteúdo, em como (vi) para o direcionamento de publicidade.⁶⁰ Tais são os dados recolhidos pelo Apple Music. O Shazam por seu turno reconhece, mormente, dados relativos (i) à identidade do usuário, (ii) o título, o artista de uma música reconhecida em como o momento e a localização em que tal reconhecimento ocorreu⁶¹.

⁶⁰ “As described in Section 6.2, the music industry is undergoing a significant change with a shift from physical to digital distribution. In this environment, user data already plays an important role today and that role is likely to grow in the future in the music industry. Such data may include: (i) device data (for example, unique device identifier, device language, operating system), (ii) demographic data (for example, name, gender, age); and (iii) behavioural data (for example, user's clicks in app, the time users spend in various screens, microphone volume level, track titles, artists, time and location of when a song has been played, the reason why a song stopped playing, social media activity). (65) The user data gathered by the players in the music industry has several different uses, including but not limited to: (i) development of new methods for delivering music to consumers; (ii) generation of data analytics; (iii) helping artists to understand their performance; (iv) identification of new music trends and prediction of future music hits; (v) understanding the music tastes of listeners in order to offer personalised playlists and provide music recommendations; and (vi) targeting advertising.” parágrafos 64 e 65

⁶¹ “Shazam currently collects (i) a set of information regarding the user's identity, which varies depending on whether the individual user opts to be anonymous⁵³ or to access the Shazam app through a registered account;⁵⁴ (ii) [...] ; 55 (iii) the user's recognition activity performed through the Shazam app which includes, for each song recognized by the user, the track title, the artist, the time at which the song was recognized, and the location where the app was used (if the user has given this permission, otherwise only information on the country where the song was recognized is collected) (the data collected on the user's recognition activity is referred to in this Decision as “Shazam's User Behavioural Data”); and (iv) which buttons or features within the Shazam app itself the user clicks on. 56 In this Decision, the data described in (i) to (iv) is referred to as “Shazam User Data.” Idem, parágrafo 69

Definidos os usos dos dados recolhidos, a Comissão definiu os mercados relevantes de cada aplicativo, quais sejam: com relação à Apple, o mercado de design, desenvolvimento e manufatura de dispositivos de comunicação móvel e mídia, de computadores pessoais, além de provisão e distribuição de conteúdo musical digital, conquanto o Shazam atua no mercado de soluções de softwares envolvendo aplicativos de reconhecimento musical. A Comissão, no entanto, identificou atuação de ambos – portanto, sobreposição horizontal – nos mercados de licenciamento e análise de dados ligados à indústria musical, bem como de publicidade digital⁶². Do ponto de vista geográfico, a Comissão definiu tais mercados como abrangendo ao menos toda a União Europeia, deixando, no entanto, a definição da maior parte deles em aberto. Nesse sentido, a Comissão entendeu que a operação em análise seria caracterizada por sobreposições horizontais nos dois mercados supracitados, bem como por integrações verticais nos mercados complementares de soluções de softwares envolvendo aplicativos de reconhecimento musical e o de distribuição de conteúdo ligado à música digital, bem como com o de fabricação de dispositivos de comunicação móvel e mídia, e de computadores pessoais⁶³. Ademais, a Comissão entendeu que em nenhum dos mercados envolvidos, qualquer das partes deteria um *market share* superior a 30%⁶⁴.

Assim a Comissão acabou por entender que a operação não traria preocupações concorrenciais nos mercados em que há sobreposição horizontal entre as duas empresas. As duas companhias teriam participação no mercado de publicidade online, entretanto, na instrução do processo todos aqueles que responderem ao questionário da comissão, relataram que a operação não levantaria preocupações com relação a este mercado. Além disso, foi analisada uma possível segmentação deste mercado referente à publicidade online para o segmento musical, mercado sobre o qual a comissão concluiu

⁶² “For the assessment of the Concentration, the following business activities of the Parties are relevant: (1) Apple develops OSs for its smart mobile devices (tablets and smartphones), PCs, smart watches and smart TVs, for which third parties can develop software solutions and apps; (2) Shazam is active in the provision of ACR software solutions, including music recognition apps; (3) Apple is active in the provision of digital music distribution services, which are offered through apps; (4) both Parties are active in the licensing of music data; and (5) both Parties are active in the provision of online advertising services.” Idem, parágrafo 75.

⁶³ “In this context the Commission notes that the Concentration mainly combines Apple's and Shazam's complementary services (software solutions platforms and digital music streaming services for Apple and ACR software solutions, and in particular music recognition apps, for Shazam). While both Apple and Shazam are active in licensing music data and both provide some online advertising services, these activities are not their core business. Hence, the Concentration only gives rise to limited horizontal overlaps while, at the same time, giving rise to some nonhorizontal relationships.” Idem, parágrafo 144.

⁶⁴ Idem, parágrafos 146 a 165.

que em verdade a Apple não teria atividade, e, portanto, não haveria que se falar em sobreposição.

Por fim, com relação especialmente aos problemas envolvendo o compartilhamento de dados entre tais empresas, a Comissão concluiu não haver maiores problemas caso a Apple tentasse usar seus dados para fortalecer o Shazam, ou para melhor direcionar sua publicidade. Isso porque haveria uma concorrência bastante efetiva no setor de publicidade online, briga que incluiria gigantes como Google e Facebook, de maneira com que os problemas de ordem concorrencial estariam mitigados pela intensa rivalidade.⁶⁵

Com relação às elencadas possibilidades de fechamento de mercado, que poderiam ser levadas a cabo como consequência da operação, é esclarecido que tal possibilidade só é factível quando a operação é dotada da possibilidade de que tais empresas provoquem um aumento de preço em mercados *downstream*, impedindo o acesso de algum agente a determinado insumo; quando a união das duas empresas é capaz de alavancar a posição da empresa resultante da operação em mercados relacionados por meio de práticas exclusionárias; ou quando a operação possibilita o acesso por parte de uma companhia a informações comercialmente sensíveis que possam resultar em práticas que ameacem a competição. Pois bem.

Com relação ao terceiro ponto, concernente ao acesso a informações comercialmente sensíveis, a Comissão ressaltou que o aplicativo Shazam rastreia atividade dos usuários que estão em uso de outros aplicativos, particularmente dos aplicativos que oferecem o serviço de streaming de músicas, e colhe informações destes aplicativos, como por exemplo os nomes das listas de reprodução acessadas por um usuário, bem como do endereço de email usado para o perfil, dentre outros. Assim, levantou-se a possibilidade de que a operação resultasse no acesso pela Apple a dados comercialmente sensíveis de seus concorrentes.⁶⁶

⁶⁶ “In this case the Concentration would allow Apple to gain access to certain information on Apple Music’s rivals. As explained in recitals (196) to (199), the Shazam app currently collects: (a) information about the presence of non pre-installed digital music streaming apps on the mobile device where the Shazam is installed: in the EEA this currently relates to approximately [...] million monthly active users of the Shazam app on Android devices and [...] million users on iOS devices; 150 (b) with respect to Spotify’s users who have connected their account with the Shazam app, information about the fact that the user has connected the Shazam account to his/her Spotify account and potentially other, more granular pieces of information, based on Spotify’s API. 151 In the EEA this currently relates to approximately [...] million monthly active users of the Shazam app on Android devices and [...] million users on iOS devices.” Idem, parágrafo 210.

A comissão, no entanto, concluiu que o acesso pela Apple aos dados do Shazam não deveriam trazer efeitos anticompetitivos, e embasou tal decisão numa série de razões. A primeira delas teria relação com o fato de que o Shazam abriu mão de alguns de seus dados coletados a fim de se adequar à legislação europeia vigente acerca da proteção de dados pessoais, o GDPR.

Como elencado no capítulo anterior, conforme as regras estabelecidas pelo GDPR (e também pela LGPD no contexto brasileiro), qualquer empresa que detenha e realize o tratamento de dados pessoais de usuários tem de elencar a este usuário quais os fins para os quais está utilizando seus dados, bem como deve contar com a permissão deste usuário para que seus dados sejam utilizados aos fins descritos. Além disso, o GDPR proíbe que tais dados sejam usados para qualquer outro objetivo que não aquele especificado pela companhia, tampouco ser transmitido a um terceiro sem que haja a cessão desses dados de forma consentida pelo titular. Além disso, também para fins de respeito ao GDPR, cabe às empresas demonstrarem e assegurarem que a transmissão de dados pessoais realizadas de uma companhia à outra segue todos os parâmetros de segurança e os princípios impostos pela legislação⁶⁷.

Também é pontuado pela Comissão que o Shazam só consegue captar dados de outros aplicativos porque o sistema operacional permite que o aplicativo assim proceda. Nesse sentido, com relação aos usuários do sistema Android, a captação depende da autorização de uma empresa que não está sob o controle da Apple, e tal empresa pode a qualquer momento suspender esse procedimento por parte do Shazam⁶⁸.

Ainda com relação à coleta de dados efetuada pelo Shazam de informações de concorrentes da Apple Music no mercado de streaming de músicas – a Comissão tratou especificamente do Spotify neste ponto - esta coleta é efetuada com base em termos acordados pelo Shazam (e demais aplicativos que utilizam estes dados) e pelo Spotify. Tais termos incluem as obrigações de (i) apenas solicitar aos usuários do Spotify os

⁶⁷ “Shazam (and Apple post-Transaction) are accountable to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. In particular, they must ensure the lawfulness of the processing of personal data collected by Shazam and transmitted to Apple and comply with the principles relating to the processing of personal data, including the principles of purpose limitation, fairness and transparency.” Idem, parágrafo 232

⁶⁸ “Second, with regard to the Customer App Information, the Commission notes that Shazam is able to access data about which apps are installed on a user’s Android device because the Android Developer Guidelines allow it to do so.¹⁶⁴ This situation could change at any point in time in the future and is not controlled by Apple” Idem, parágrafo. 236

dados necessários para operar o aplicativo; (ii) não enviar e-mail aos usuários do Spotify sem consentimento explícito; e (iii) divulgar de forma completa e precisa as práticas e políticas de privacidade que eles aplicam em seu aplicativo ou site. Além disso, este contrato também impede o uso de dados de usuários do Spotify para finalidade de concorrer com o aplicativo de streaming. Nesse sentido, a Apple após a operação estaria contratual e legalmente limitada no uso dos dados que foram adquiridos com a compra do Shazam.

A Comissão durante a instrução também notou que as vantagens relativas a dados conseguidas por meio da operação em realidade poderiam ser adquiridas pela Apple por meio de outros sites, que fornecem serviços de direcionamento (como por exemplo, o Facebook e o Google), serviços estes que estão disponíveis aos demais concorrentes da Apple. Nesse sentido, a operação não alteraria a dinâmica concorrencial⁶⁹.

Com relação aos outros pontos elencados, acerca da probabilidade de fechamento de mercado após a operação, e acerca das possíveis práticas que possam vir a ser adotadas como consequência desta, Comissão concluiu que em realidade a probabilidade de que uma prática seja levada a cabo e afete a concorrência, prejudicando os demais agentes, é bastante baixa, tendo em vista os dados do Shazam não são considerados como dados chave às atividades de nenhum dos concorrentes, e que estes já possuem uma ampla gama de dados suficientes para suas atividades produzidos no âmbito do funcionamento do próprio aplicativo, do próprio serviço de streaming de música.

Muito embora seja possível ver uma enorme evolução por parte da autoridade antitruste europeia na questão concernente à transferência de dados pessoais e Big Data, importante ressaltar que há ainda muito a ser percorrido. Diferentemente da análise realizada na ocasião da aquisição da DoubleClick pelo Google, a Comissão conseguiu

⁶⁹ “even if Apple were to gain access to the Customer Information, its ability to target subscribers of competing music streaming services post-Transaction is not set to increase materially. Indeed, the market investigation confirmed the Notifying Party's claim that there exist several providers, including, but not limited to Facebook, Google and Twitter, which allow for the targeting of “music enthusiast” audiences (including some players allowing targeting of audiences of users of digital music streaming distributors, such as “Spotify app users”) which Apple could rely upon to target such users already pre-Transaction. Further, the ability to target subscribers of competing music streaming services post-Transaction would not be limited to Apple, as Apple Music's rivals could also rely on the same third party services post-Transaction (as well as pre-Transaction)” Idem, parágrafos 172 e 173.

avançar no reconhecimento da importância e centralidade do tema para análise concorrenciais, e, a partir do GDPR, firmar parâmetros mínimos que permitam uma melhor análise, vez que esta legislação instituiu práticas mínimas ao tratamento de dados capazes e suficientes à proteção da população, do cidadão comum.

A despeito de tal evolução a academia vem tentando estabelecer pontos a serem observados quando da análise de operações envolvendo *data-driven organisations*. O renomado economista David Evans, ao se debruçar sobre pontos que as autoridades antitruste devem considerar na análise de operações envolvendo plataformas, que, tradicionalmente, constituem mercados digitais e lidam com coleta e análise de dados, elencou três principais pontos, quais sejam (i) o bem-estar dos consumidores de todos os lados da plataforma, (ii) a interdependência entre os consumidores, de maneira com que a tensão natural entre estes não seja alterada, além de (iii) reconhecer que tais plataformas possuem incentivos ligados à assunção de lucros, e que se aproveitam de falhas de mercado para tanto.

Com relação aos problemas que ainda podemos visualizar na análise das operações atuais, talvez o maior deles resida na ausência de troca entre as autoridades antitruste e de proteção de dados. Embora seja comum a troca de informações entre agências reguladoras e autoridades antitrustes ao redor do mundo inteiro, é latente – especialmente no caso Apple-Shazam - a ausência de pronunciamento e troca de informações e auxílio entre a Comissão e a autoridade de proteção de dados europeia (European Data Protection Board – EDPB), que já se encontra em pleno funcionamento.

Sabe-se que o EDPB lançou um comunicado público⁷⁰ requerendo participação na investigação levada a cabo pela autoridade antitruste europeia no caso Apple/Shazam, mas a Comissão Europeia não fez nenhuma menção a qualquer documento ou contribuição elencada pela autoridade de dados em sua decisão final.

Faz-se necessário refletir assim, acerca da importância da interação interinstitucional entre as mais diversas agências reguladoras a fim de que estas consigam explicar o funcionamento destes mercados mais peculiares e com características próprias a fim de que a autoridade antitruste consiga oferecer respostas satisfatórias às questões concorrenciais. Tal interação já acontece com agências ligadas

⁷⁰ Fonte: < <https://www.migalhas.com.br/dePeso/16,MI298556,81042-Protecao+de+dados+defesa+da+concorrenca+ANPD+e+CADE+consideracoes>>. Acesso em 30 de março de 2019

a outros setores econômicos, e é preciso que todas as autoridades ao redor do mundo entendam o quanto antes a necessidade e os benefícios advindos deste tipo de interação.

CAPÍTULO 3 - PROTEÇÃO DE DADOS E CONTROLE DE CONDUTAS

O mundo do antitruste, conforme relatado no capítulo inicial, não diz respeito somente ao controle feito por ocasião da compra de empresas, já analisada. Tenta também mitigar as condutas que desencadeiem num ambiente de concorrência não saudável. Com a introdução dos dados nessa equação, ou seja, com a possibilidade de usar dados a fim de prejudicar seus concorrentes e/ou consumidores, abriu-se um enorme leque de possibilidades na adoção de condutas por empresas que possuem informações relativas aos dados pessoais de usuários. Além disso, problemas que já constituíam debates importantes dentro do antitruste foram amplificados no contexto atual, de mercados com empresas detentoras de dados pessoais.

Pretende-se, assim, elencar as principais condutas já experimentadas no antitruste – seja de modo acadêmico, conjecturando acerca de possíveis implicações, sejam aquelas de fato ocorridas – bem como trazer à luz os principais problemas a serem enfrentados quando da análise de cada uma delas.

3.1 – A discricionariedade e a avaliação do conjunto probatório em condutas concorrenciais

O primeiro ponto a ser considerado, que já constitui um enorme debate dentro do antitruste, diz respeito à valoração das provas realizadas quando da análise de condutas – especialmente de cartéis. Isso porque um, cenário que já apresentava problemas vê-se agora ainda mais agravado pela possibilidade de utilização de novas tecnologias, de maneira com que a autoridade deverá tomar extremo cuidado na análise caso a caso, sob o risco de incorrer em punições demasiadamente severas a agentes que não tinham intenção de levar a cabo qualquer conduta, ou de deixar passar condutas que sejam prejudiciais à dinâmica concorrencial e aos consumidores.

A configuração de uma infração antitruste, mais que nos campos atinentes ao direito penal, é enormemente discricionária. Isso porque, na configuração de um ilícito, três são as características que permitem isso: trata-se de um tipo aberto, cuja punição não necessariamente depende de que haja efeitos no mundo concreto – para o caso dos

ilícitos *per se* - e que dispensa a culpa em seu sentido psicológico, considerada no âmbito do direito penal⁷¹.

Uma das condutas mais clássicas tipificadas, responsável pela promoção de lesão aos consumidores, é a conduta de cartel. O cartel, como também já trazido, trata-se de da combinação de preço entre diversos agentes, a fim de que estes consigam maximizar seus preços e lucros, obtendo a maior vantagem possível dos consumidores.

Tal conduta, desta feita, para que fosse devidamente punida, contava com a necessidade de que houvesse reunião de material probatório da prática de cartel. Vale, neste ponto, traçar um aspecto bastante sensível dos ilícitos que são objeto do Direito Concorrencial, qual seja aquele atinente à dificuldade de provar a ocorrência da conduta. Desta feita, os ilícitos concorrenciais possuem toda uma forma diferenciada de se tomar um conjunto probatório, tendo em vista a dificuldade em se conseguir provar a real combinação de preços.

Nesse sentido, muito embora o Direito Concorrencial, tendo em conta seu caráter sancionador, partilhe diversos entendimentos tomados pelo Direito Penal, certo é que no Antitruste os indícios desempenham enorme papel para que haja condenação, para que seja configurada conduta.

Conforme esclarecido por Ana Frazão⁷², com base no raciocínio exposto por Luiz Guilherme Marinoni, a dificuldade de se provar uma conduta de maneira cabal requer a flexibilização da sistemática probatória, de maneira com que seja possível ao menos o uso de indícios, ou seja, em alegações sobre fatos secundários que, quando postos em contexto, permitem a racionalização e conclusão de que houve um ilícito.

Recente voto exarado pelo Conselheiro Maurício Bandeira Maia tratou de forma bastante satisfatória a problemática envolvendo a avaliação de um conjunto probatório no Direito Antitruste. Sua manifestação ocorreu por ocasião do julgamento do processo 08012.001376/2006-16, que condenou empresas por formação de um cartel internacional relativo ao mercado de aparelhos eletroeletrônicos de direcionamento de fluxo de energia elétrica com isolamento a gás (*gas insulated switchgear* – GIS). Nesse Voto, ressaltou o conselheiro a necessidade de se condenar não só com base em provas indiretas e inconclusivas, realizando ao longo do documento a análise de cada item utilizado à condenação, vez que as principais provas naquele caso advinham de Acordo

⁷¹ FRAZÃO, Ana. Direito da Concorrência, pressupostos e perspectivas, Ed. Saraiva, 2017, p. 246

⁷² FRAZÃO, Ana. Direito da Concorrência, pressupostos e perspectivas, Ed. Saraiva, 2017, p. 298

de Leniência. Após, concluiu o Conselheiro que as provas eram suficientes, diretas e comprovariam a participação das empresas em cartel no setor de energia elétrica, ressaltando que tais provas seriam robustas o suficiente⁷³.

Um robusto conjunto probatório de determinada prática, como será visto adiante, torna-se ainda mais difícil quando falamos de mercados digitais. Isto porque além de toda a dificuldade supramencionada, é possível que nos mercados digitais haja colusão sem que sequer seja essa a intenção dos agentes de mercado. Algoritmos programados para fins semelhantes, ou mesmo o uso de um mesmo algoritmo por mais de um agente são práticas legais que podem levar à formação de um cartel, causando efetivas lesões ao consumidor. Ademais, a própria coleta e análise de dados traz todo um novo mundo de possibilidades que podem sim ser utilizadas para fins anticoncorrencias. É a partir de tais ideias, portanto, que se pretende tratar das condutas lesivas à concorrência, tendo por base estudos de autores reconhecidos.

3.2 – Condutas tradicionais na era do Big Data e as mudanças que devem ser objeto de atenção pelo antitruste

Antes da era do big data e da internet como um todo, em que a comunicação era feita de outros modos, para que um cartel ocorresse era necessário que pessoas físicas se encontrassem e combinassem os preços a serem praticados, além de que estas verificassem os ganhos auferidos. Hoje em dia, no entanto, diversos são os meios de se incorrer numa conduta colusiva. Há a crença, por exemplo, de que, com as novas tecnologias, a colusão não mais precisará de que pessoas físicas intentem contra a um ambiente dotado de concorrência efetiva e combinem entre si alguma prática. Além disso, se efetuado por máquinas, a natural tensão existente nos cartéis desapareceria. É uma amostra dos pontos que serão tratados abaixo.

Os pesquisadores Ariel Ezrachi e Maurice Stucke^{74, 75} exploram bem os tipos de cartéis que podem advir da análise de dados pessoais e dos algoritmos utilizados para

⁷³ Voto do Conselheiro Maurício Bandeira Maia no Processo de nº 08700.012018/2014-82. Fonte: <https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQAh8mpB9yMoz3EHGU6jzRZ_LHgmllf-ckFHjbb3tMleK2I08CkedfWFeRwCIkK7j0Cz4qzc2wyVDp5Xr-OIoHrmK_85Sw>. Acesso em 7 de maio de 2019.

⁷⁴ COELHO, Maria Camilla Arnez Ribeiro. “Algoritmos, colusão e “novos agentes”: os quatro cenários de Stucke e Ezrachi sob a ótica da legislação antitruste brasileira”. 2018. Disponível em: <

realização de tal análise. De acordo com os autores, as condutas atuais não se encontram tanto “preto no branco”, no sentido de que, para cada ação e contexto a conduta pode ser considerada mais ou menos reprovável.

Pela análise entoada, assim, por Stucke e Ezechí quatro seriam os principais tipos de condutas – e espécies de cartéis - possíveis de serem formados no âmbito dessas novas relações digitais:

- (a) Mensageiro;
- (b) Hub and Spoke;
- (c) Agente previsível; e
- (d) Máquina autônoma

Passaremos assim à análise de cada tipo em separado.

3.2.1 – Formação de cartel com computador como mensageiro

Nesse primeiro cenário, as pessoas físicas envolvidas fariam uso do computador para que este execute suas ordens de forma direta. Neste tipo, portanto, partiriam das pessoas físicas à vontade e as instruções para que fosse formado um cartel. Nesse sentido, trata-se de um tipo que, muito embora passe pelo uso da tecnologia e facilite a dinâmica para que efeitos anticoncorrenciais sejam produzidos, não se faz necessária uma abordagem mais atenta a fim de condenar aqueles que incorreram em tal prática.

O conjunto probatório, neste caso, possuiria os mesmos desafios já comuns às provas utilizadas na condenação de qualquer outro cartel. A tecnologia seria capaz de, no entanto, facilitar a execução do ilícito, vez que os algoritmos poderiam ser programados de modo a monitorar e analisar todos os participantes, facilitando com que todos permanecessem e dotassem um mesmo padrão de preços, auxiliando, inclusive, na percepção e punição dos agentes que apresentem comportamentos não condizentes com o acordado pelos membros.

<http://www.direitorp.usp.br/wp-content/uploads/2018/10/Mulheres-no-Antitruste-Volume-I-V.-Final.pdf>
>. Acesso em 19 de junho de 2019.

⁷⁵ STUCKE, Maurice, EZRACHI, Ariel. “Artificial intelligence & collusion: when computers inhibit competition”. 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2591874>. Acesso em 19 de junho de 2019

Neste caso, em se tratando o cartel de um ilícito per se, a mera prova de que houve ações para implementação da conduta colusiva já seria suficiente a uma possível condenação, devendo ser desconsiderado pelas autoridades a produção de efeitos no mundo concreto, ou se tal acordo de fato causou prejuízo a consumidores e demais concorrentes.

3.2.2 – Formação de cartel Hub and Spoke

O cartel do tipo Hub and Spoke, bem antes da introdução do Big Data às análises concorrenciais, já era analisado. O Cartel do tipo Hub and Spoke⁷⁶ trata das situações fáticas em que a prática num nível da cadeia comercial só é possível por meio da atuação de uma empresa verticalmente relacionada. A essencialidade deste tipo de conluio seria, assim, a ausência de contato direto entre os agentes participantes do cartel.

Nos mercados digitais, este tipo de cartel seria caracterizado não pela utilização de um terceiro que coordenasse as informações entre os agentes, mas o uso de um mesmo algoritmo para assunção deste fim. Assim, tal algoritmo se constituiria no elemento vertical capaz de promover o alinhamento entre os agentes de uma cadeia a jusante.

Como maneira de exemplificar a ocorrência de um cartel deste tipo, os autores Ariel Ezrachi e Maurice Stucke trazem a tona o caso do Uber. Sendo este um aplicativo que equaliza e determina os preços a serem cobrados de usuários a partir da demanda pelos serviços e da oferta disponível, de maneira com que sempre vai prover o preço competitivo a ser praticado, não o preço de mercado. Nesse sentido, segundo defendem os autores, havendo conhecimento acerca do funcionamento do algoritmo, e, tendo em vista o crescente número de usuários, existe um incentivo à manipulação de seu funcionamento e à adoção de condutas coordenadas, ainda que os agentes não tenham “combinado” isso entre si.

⁷⁶ COELHO SARTO, Elisa Santos. “Cartéis hub-and-spoke: coordenação horizontal por meio de restrições verticais”. Revista de Defesa da Concorrência, V.5, n. 2. 2017. Disponível em: <<http://revista.cade.gov.br/index.php/revistadedefesadaconcorrência/article/view/329>> . Acesso em: 19 de junho de 2019.

A possibilidade de ocorrência deste tipo de cartel já foi tratada pela Professora Ana Frazão em artigo o veículo Jota⁷⁷. Em sua abordagem, no entanto, a análise entendeu que este tipo de conduta ocorreria em qualquer comércio efetuado por meio de uma plataforma de dois lados. Segundo defende, a neutralização das condições de rivalidade entre os agentes do mercado atuantes em determinada plataforma influenciaria na adoção de condutas coordenadas por parte dos prestadores de serviço, de maneira semelhante ao que associações e sindicatos fazem, e que resultam em condenações por parte da autoridade concorrencial. O CADE, inclusive, sequer possui histórico de aceitar a integração entre agentes horizontalmente relacionados ainda que tal organização tenha o condão principal de equiparar tais agentes a grandes empresas com as quais estas devem negociar. Um exemplo bastante clássico a esse respeito trata da associação de médicos e hospitais frente aos planos de saúde⁷⁸, para que consigam negociar melhores condições e pagamentos.

O caso mais recente com possível característica de cartel *hub and spoke* julgado pelo Cade tratou dos mercados de distribuição de combustível na região de Belo Horizonte e Betim. Naquela ocasião foram condenados 27 postos e 2 distribuidoras, que estariam incorrendo na prática de colusão. De acordo com o apurado, os postos combinavam preços e puniam aqueles que apresentassem precificação distinta da combinada, havendo tal prática sido induzida por meio da atuação das distribuidoras, que figuram em cadeia mercadológica acima daquela dos postos, característica deste tipo de cartel⁷⁹.

Vale ressaltar, no entanto, que muito embora seja possível a concordância entre diversos agentes de mercado com relação ao uso de um mesmo algoritmo, tal adoção não significa que os agentes também se propuseram a combinar e fixar preços por seus serviços. O que promove esse tipo de acordo é o uso simultâneo e em paralelo por todos os agentes. Para este tipo de análise, portanto, seria necessário que um especialista entendesse o algoritmo utilizado a fim de entender se o design deste previa algum tipo de acordo de preços, ou se tal resultado veio a partir da programação de que este gere

⁷⁷ Fonte: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dilema-antitruste-o-uber-forma-um-cartel-de-motoristas-12122016>. Acesso em 9 de maio de 2019.

⁷⁸ Processos Administrativos de nº 53/92 e de nº 61/92.

⁷⁹ Fonte: <<https://g1.globo.com/mg/minas-gerais/noticia/2019/04/10/cade-multa-postos-e-distribuidoras-de-combustiveis-por-formacao-de-cartel-na-grande-bh.ghtml>>. Acesso em 9 de maio de 2019.

eficiências, ou se mesmo a partir da uniformização como resultante da análise de todos os dados a que este se dispôs tratar e analisar.

3.2.3 – Formação de cartel baseado num agente previsível pela dinâmica do mercado

Com relação a este tipo de conduta, a tentativa é desenhar um algoritmo que seja capaz de reagir conforme a dinâmica de mercado vá se modificando. Nesse sentido, o que se tenta é prever a produção de resposta a partir da alteração das condições econômicas e mercadológicas. Nesse sentido, cada empresa trabalharia no desenvolvimento de um algoritmo de modo independente. O desenvolvimento unilateral não exclui, no entanto, a possibilidade de que tais algoritmos ajam de modo parecido e assim acabem por criar efeitos anticompetitivos. Ora, se estes visarem a perseguição de um objetivo incomum, não seria absurdo que todos estes provocassem ações similares, de maneira a promover paralelismo entre os diversos agentes.

Neste ponto cabe, no entanto, esclarecer do que se trata o paralelismo entre agentes de um mesmo mercado, e como o paralelismo pode ser tão prejudicial quanto um cartel, muito embora não seja tomado pelas autoridades com a mesma dimensão de um cartel ainda que produza os mesmos efeitos, vez que não há culpa nem intenção na prática, mas tão somente a reação com base nas ações tomadas pelos demais *players*.

Pois bem, um exemplo clássico trata-se alguém que é dono de um pequeno negócio, e, a fim de se tornar mais competitivo, faz uma pequena pesquisa de preço ante seus concorrentes. Assim toma conhecimento dos preços praticados e pode tanto se adequar a eles, quanto tentar promover algum tipo de promoção, a fim de se diferenciar e auferir maiores lucros que seus concorrentes. Boa parte da possibilidade de se incorrer num paralelismo diz respeito à facilidade em ter acesso às ações praticadas pelos concorrentes deste mercado, ou seja, à transparência das informações.

No caso de cartelização envolvendo diferentes algoritmos, portanto, os algoritmos seriam capazes de promover dois tipos de condutas anticoncorrencias: a primeira diz respeito à capacidade de diferentes algoritmos chegarem a uma mesma conclusão, promovendo uma coordenação tácita, tendo em vista que partiriam dos mesmos dados a fim de promover a análise de mercado e assumiriam uma mesma estratégia sendo também aptos a, inclusive, promover um boicote ou uma espécie de

“contra-ataque” com relação aos agentes que apresentassem comportamento desviante daquele do referido cartel. A segunda possibilidade será explorada no subtópico que segue. Vale expressar, por fim, que as condutas aqui tomadas não seriam comprovadas por meio de provas cabais ou indiciárias, mas o conjunto probatório poderia ser utilizado de modo a sustentar que há uma motivação e certo grau de consciência de que as interações entre as máquinas neste ambiente promoveriam paralelismo.

3.2.4 – Formação de cartel baseado na autonomia da máquina.

Pois bem, a segunda possibilidade de colusão envolvendo algoritmos distintos, diria respeito à possibilidade de que todos os algoritmos promovessem respostas semelhantes aos comportamentos dos rivais. A diferenciação entre estes dois tipos de colusão residiria no fato de que, enquanto a primeira reação possui um viés de retaliar ou dissuadir o agente que apresenta comportamento desviante, no segundo tipo a resposta adotada seria individual e racional, criando um cenário capaz de influenciar à adoção de comportamento coordenado sem que, no entanto, haja a conduta orientada de alguma forma se atentar contra a concorrência, havendo tão somente o desincentivo aos agentes para que forneçam melhores ofertas e preços.

Dessa forma, diferente das outras duas categorias em que houve certa participação por pessoas físicas: seja no intento de usar a tecnologia para promover, monitorar e punir acordo entre concorrentes, seja no uso consciente de uma plataforma utilizada por todos os demais, neste caso não há qualquer elemento intencional para que haja colusão, e sim a mera utilização da tecnologia a fim de maximizar sua atividade. Assim, ao delegar as decisões concernentes aos preços empregados aos computadores, há uma facilitação do conhecimento acerca dos demais agentes, levando a uma estabilização do mercado. Muito embora a utilização de algoritmos na precificação de serviços não seja ilegal e diga respeito tão somente à adoção de mecanismo a fim de melhor racionalizar as decisões tomadas, talvez algum tipo de intervenção possa fazer sentido a fim de proteger o ambiente concorrencial.

Aqui o desafio reside no fato de que a adoção de conduta que levaria a um paralelismo entre os players advém do próprio mecanismo de funcionamento dos algoritmos, baseados em *machine learning*. Não haveria, por exemplo, prova de conduta ilícita ou sequer algum tipo de acordo entre os agentes, fato tal de que dificultaria muito

qualquer tipo de punição, a despeito dos prejuízos causados ao ambiente concorrencial e aos consumidores.

3.3 – Possíveis novas condutas na era do Big Data e o papel do antitruste

Tem-se visto ultimamente que as repercussões do uso e análise de dados na esfera econômica não serviram tão somente para inovar os meios com que já se praticavam algumas condutas, como também abriu possibilidade para que novas ações sejam tomadas com o fim de prejudicar a concorrência nos mercados.

Há, no entanto, certo grau de obscuridade quanto ao que caberia à tutela das autoridades antitruste, bem como se deve ser criada uma autoridade de dados nos diversos países que atue nos moldes da autoridade antitruste – decisão, como posto em capítulo anterior, tomada pelo Brasil e pela União Europeia, que tem autoridades com competência para punir agentes que violem as regras estabelecidas em suas respectivas legislações acerca da proteção de dados pessoais.

3.3.1 – *Data Breaches*

O primeiro tipo de conduta inédito que pode causar danos à competição diz respeito ao caso dos *Data Breaches*. Pois bem, trata-se de nada mais nada menos que a invasão e posterior exposição ou roubo de dados de uma empresa, conseguido a partir da ação de hackers que se aproveitam de falhas no sistema de segurança de grandes empresas. Um exemplo bastante recente e capaz de demonstrar a gravidade deste tipo de ocorrência diz respeito ao Facebook. Em abril de 2019, foi noticiado na imprensa o vazamento de dados de cerca de 540 milhões de usuários, que tiveram seus dados expostos para a Amazon em razão da utilização de um aplicativo conjugado ao Facebook⁸⁰.

Vale ressaltar que, como anteriormente explorado por este trabalho, dados podem ser entendidos como ativos pertencentes a uma empresa, de maneira com que um compartilhamento de tal magnitude significaria uma perda enorme para uma empresa ante seu competidor, caso tal vazamento tivesse ocorrido entre companhias atuantes num mesmo mercado relevante – no caso concreto, tal situação não se configura em

⁸⁰ Fonte: <<https://g1.globo.com/economia/tecnologia/noticia/2019/04/04/dados-de-540-milhoes-de-usuarios-do-facebook-ficam-expostos-em-servidor.ghtml>> Acesso em 9 de maio de 2019.

razão de, grosso modo, a Amazon atuar com e-commerce e o Facebook com redes sociais e publicidade.

Em junho de 2015, a FTC já percebia a sensibilidade atinente à questão dos *Data breaches*, e começou a discutir os possíveis impactos e medidas que deveriam ser tomados no âmbito antitruste, de maneira com que não houvessem maiores prejuízos⁸¹. Naquela ocasião, o FTC tinha passado por dois casos envolvendo a proteção de dados⁸² pessoais, que acabaram por dar início ao entendimento de quais seriam os standards a serem seguidos quando da análise envolvendo problemas com dados pessoais.

3.3.2 – *Third Party Tracking*

Outra conduta recentemente abordada diz respeito ao denominado *Third Party Tracking*⁸³. Algumas empresas possuem como modelo de negócio o monitoramento da atividade de usuários. Assim, tais companhias sobrevivem da coleta de todos os dados relativos ao uso da internet por um indivíduo, de maneira a saber quais aplicativos essa pessoa faz *download*, ou quais sites visita. Tais informações são associadas a um usuário, e após utilizadas para, por exemplo, serem vendidas. Vale ressaltar que nem sempre essas informações são trocadas especificamente por valores monetários. O Google Analytics, por exemplo, fornece aos próprios sites análises relativas a seu desempenho, em troca da obtenção dos dados de usuários.

Nesse sentido, nem sempre a avaliação dessa atividade a partir dos seus aspectos e danos monetários faz-se razoável. Assim as autoridades deveriam focar-se

⁸¹ BERGSIEKER, Ryan T., CUNNINGHAM, Richard H., YOUNG, Lindsey. The Federal Trade Commission's Enforcement of Data Security Standards, 2015. Disponível em: <<https://www.gibsondunn.com/wp-content/uploads/documents/publications/Bergsieker-Cunningham-Young-FTC-Data-Security-Enforcement-06.2015.pdf>>. Acesso em: 9 de maio de 2019.

⁸² Tratam-se dos casos LabMD vs. FTC. e Wyndham VS FTC. O primeiro diz respeito à ocasião em que um trabalhador da LabMD, contra as políticas da empresa, instalou o LimeWire e expor informações sensíveis acerca da saúde de milhares de pacientes. Nesse caso, após grande imbróglio judicial, as autoridades acabaram não condenando a empresa, muito embora considerassem sua política de proteção de dados negligente, em razão da ausência de normativos que estabelecessem diretrizes sobre o tema. Com relação ao caso Wyndham, em que dados bancários de muitos clientes foram expostos devido a uma falha na segurança, a autoridade americana conseguiu a manutenção da condenação da empresa nas demais instâncias e tribunais. A diferença no tratamento desses dois casos deu-se em razão de, no primeiro, o FTC ter tentado impor uma política de segurança cibernética. Os tribunais consideram que, muito embora o FTC seja competente para investigações a respeito do uso de dados, não caberia a ele a imposição de qualquer conjunto de regras aos tutelados. Fonte: <<https://www.alston.com/en/insights/publications/2018/07/labmd>>. Acesso em 16 de junho de 2019.

⁸³ BINNS, Reuben, BIETTI, Eletra. Acquisitions in the Third Party Tracking Industry: Competition and Data Protection Aspects. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269473>. Acesso em 16 de junho de 2019.

mais nos mercados em que tal conduta é passível de acontecer – como de propaganda online, em vez de focar na atividade de coleta, tratamento e venda de dados em si.

A dimensão do possível dano que possa ser causado por companhias baseadas nesse modelo de negócio dizem respeito a dois aspectos: de prevalência e proeminência. A primeira diz respeito à quantidade de locais de onde a companhia coleta dados, e a segunda relativa ao número de usuários que visitam a página de onde se extrai tais dados.

A lesividade relativa a tal modelo de negócio não parece reconhecível a primeira vista, mas existe. Em primeiro lugar, as *Third Party Trackers* serão sempre capazes de estar um passo a frente das demais companhias, pois estas não só criam eficiência e escala a partir da manutenção de seu *software* de rastreamento, como ainda agregam informações recebidas de diversos outros locais, conseguindo um perfil mais amplo e refinado dos usuários.

Mais recentemente uma decisão do Bundeskartellamt, a autoridade concorrencial alemã, restringiu a coleta de dados realizada pelo Facebook⁸⁴, empresa que atua com base no modelo de negócio atinente às *Third Party Trackers*. Para que um usuário pudesse fazer parte do Facebook, este deveria concordar com que a empresa monitorasse e coletasse dados acerca de sua atividade inclusive em sites fora da plataforma. Nesse sentido, a autoridade concorrencial alemã, ante a falta de concorrentes efetivos ao Facebook, considerou que tal coleta de dados constituiria uma violação ao GDPR bem como o exercício de abuso de poder dominante. Não haveria, segundo avaliado, qualquer opção ao usuário que queira o tipo de serviço disponibilizado pelo Facebook que não passasse por concordar com a venda de seus dados, o que contribuiria ainda para a consolidação e manutenção da companhia como dominante.

Tal decisão representou um marco na análise concorrencial das questões envolvendo dados pessoais por permitir reflexões acerca das competências das autoridades de dados e concorrenciais – muito embora, a primeira vista, pareça problema atinente só a uma possível atuação de autoridade ligada à proteção de dados pessoais, fato é que tal conduta também provoca impactos na dinâmica concorrencial, e

⁸⁴ Fonte: <<https://istoe.com.br/alemanha-restringe-coleta-de-dados-de-usuarios-do-facebook-no-pais/>>. Acesso em 16 de junho de 2019

tornando ainda mais latente a necessidade de interação entre essas duas autoridades, necessidade já anteriormente mencionada neste trabalho.

A professora Ana Frazão ao analisar o caso⁸⁵, para além de tais reflexões também elencou o quanto as falhas da metodologia proposta pela Escola de Chicago – baseadas tão somente na eficiência - para análises antitruste, sustentando que caberia às autoridades sempre levarem em conta o bem-estar do consumidor ante a eficiência proposta pelo pensamento predominante da referida Escola, de maneira com que sempre se faça cumprir a finalidade do antitruste que é ligada ao bem-estar social geral, que, neste caso, abrange o bem estar dos usuários e consumidores como um todo. Nesse sentido, quando da efetivação do controle de condutas, é para este ponto que a autoridade deve se atentar, para a proteção dos usuários e consumidores que, em todas essas relações, constituem o lado mais fraco.

⁸⁵ FRAZÃO, Ana “Violação de dados pessoais pode ser um problema antitruste?”, 2019. Disponível em <http://anafrazao.com.br/files/publicacoes/2019-02-21-Violacao_de_dados_pessoais_pode_ser_um_problema_antitruste_A_recente_decisao_da_autoridade_correncial_alema_que_considera_ilicito_antitruste_a_politica_de_tratamento_de_dados_do_Facebook.pdf> Acesso em 9 de maio de 2019.

CONCLUSÃO

A partir dos conceitos e pontos suscitados neste trabalho, é possível, em primeiro lugar, concluir que as especificidades características dos mercados digitais que possuem funcionamento embasado na coleta, análise e exploração de dados pessoais de usuários, não permitem a tradicional análise realizada pelas autoridades antitruste, uma vez que essa não garante a efetividade da competição entre os mercados, tampouco garantem o bem-estar dos consumidores.

Com relação à análise realizada na aquisição de empresas, foi possível perceber o quanto o uso de dados pessoais tem-se tornado importante, seja como ativo e/ou insumo para que as empresas consigam maximizar seus lucros e se tornarem mais eficientes, seja como modo de se diferenciar, de maneira com que uma coleta e posterior efetiva proteção aos dados coletados podem tomar importância suficiente para que seja considerado como diferencial competitivo. Ademais, foi possível perceber a evolução na abordagem do tema por parte das autoridades que fiscalizam as aquisições realizadas por empresas: da percepção de separação completa entre tais temas, entendidos como paralelos, ao reconhecimento da interferência de um sobre o outro, a ponto de que seja indispensável uma interação entre as autoridades competentes a ambos os assuntos.

Ademais, junto a este novo mundo abriu-se um leque amplo de possibilidades que dizem respeito às possíveis condutas prejudiciais à concorrência possíveis de serem tomadas. Das novas possibilidades de colusão sem que, inclusive, haja vontade dos agentes econômicos para tanto, ao roubo de dados pessoais para venda, ou mesmo com relação a adoção de um modelo de negócio baseado no rastreamento de toda a atividade online do usuário, diversos são os novos desafios antitruste.

Nesse sentido, uma primeira solução para a problemática envolvendo o uso de dados e concorrência dá-se a partir do conhecimento por parte das autoridades dos conceitos ligados a tais mercados, de maneira com que os pontos sensíveis relacionados aos dados pessoais possam ser observados nas análises efetuadas.

Além disso, tais mercados contam com um novo tipo de insumo – os dados pessoais – que nem sempre se traduz em ganho monetário exclusivamente. Nesse sentido, os critérios tradicionalmente utilizados para notificação de operação tornaram-se insuficientes, de maneira com que novas discussões a esse respeito devem ser travadas, de maneira com que não escape do crivo das autoridades concorrencias

operações que sejam relativas a mercados digitais, baseados na análise de dados pessoais de usuários.

Em segundo lugar - e talvez principalmente - deva ser considerado ponto que diz respeito à cooperação entre as autoridades antitruste a relativas aos dados pessoais, criadas na maior parte dos países com o advento dos respectivos marcos regulatórios sobre o tema. É essencial ao bom entendimento de tais mercados bem como à proteção e ao bem-estar dos consumidores que tal troca institucional seja efetuada, e que o seja de forma efetiva.

Outro ponto bastante relevante a ser notado diz respeito às condutas anticoncorrenciais impetradas. Muito embora a Lei 12.529 considere passível de punição a mera ocorrência de dano aos consumidores ou competidores, fato é que nos mercados relativos às *data-driven organizations* deverá ser realizada uma análise um tanto quanto mais apurada, tendo em vista a possibilidade de ocorrência de colusão sem que sequer seja este o intuito das empresas. Ademais, será necessário perceber caso a caso – se possível adotando parâmetros para tanto - no que haveria a autoridade de se embasar para concluir a ausência de tal elemento, ou mesmo se empresas podem ser punidas ainda que a formação de colusão não houvesse sido objetivada.

Outra reflexão bastante importante diz respeito a uma possível ampliação com relação aos poderes das autoridades, a fim de que estas fossem capaz de ter um maior *enforcement* com relação às possibilidades de colheita de provas, tendo em vista que uma mera busca e apreensão em empresas talvez seja insuficiente nesse novo contexto. Assim, será necessário ao CADE não apenas possuir acesso aos mecanismos, aplicativos e algoritmos que regem determinados mercados, como ainda ser equipado de corpo técnico com especialização suficiente para que os códigos que formam os algoritmos sejam decodificados e percebidos como voltados à consecução de práticas anticoncorrenciais.

Certo é que nesse mundo novo que só recentemente passamos a experimentar como sociedade, muitos são os desafios postos ao antitruste, e ainda poucas são as respostas, de maneira com que não apenas a pesquisa acadêmica, mas também as experiências das autoridades mundo afora e os resultados das decisões tomadas devem ser objeto de muita atenção, pois é somente com base nessas duas vias que o antitruste conseguirá se manter eficaz e eficiente à manutenção da defesa da concorrência.

BIBLIOGRAFIA

WU, Tim. “The Attention Merchants: the epic scramble to get inside our heads. Nova York: Alfred A. Knopf.

MENDES, Laura. “Privacidade, proteção de dados e defesa do consumidor”. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva. 2014. Série IDP.

ALEMANHA. BUNDESKARTELLAMT; FRANÇA. AUTORITÉ DE LA CONCURRENCE. “Competition Law and Data”. 2016. Disponível em: <<http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf>>.

OECD. “Data-driven Innovation for Growth and Well-being”. Interim Synthesis Report. 2014. Disponível em: <https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf>.

EVANS, David S. SCHMALENSSEE, Richard. The Antitrust Analysis of Multi-sided Platform Business. NBER Working Paper Series. Working Paper 18783. Disponível em: <http://www.nber.org/papers/w18783>.

STUCKE, Maurice E.; GRUNES, Allen P. “No Mistakes About It: The Important Role of Antitrust in the Era of Big data”. University of Tennessee Legal Studies Research. Paper No. 269. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600051.

SCHIMIDT, Cristina. “Hipster Antitruste: poder de mercado e bem-estar do consumidor na Era da Informação”. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/coluna-da-cristiane-alkmin/hipster-antitrust-poder-de-mercado-e-bem-estar-do-consumidor-na-era-da-informacao-28122018>.

STUCKE, Maurice E. “Reconsidering antitrust’s goals”. Boston College Law Review. v. 53, p. 551-629. 2011.

FRAZÃO, Ana. “Direito da Concorrência: pressupostos e perspectivas”. São Paulo: Saraiva. 2017.

WU, Tim. “After consumer welfare, now what? The protection of competition standard on practice”. Antitrust Chronicle. April. V. 1. 2018. Disponível em: www.competitionpolicyinternational.com/wp-content/uploads/2018/05/AC_APRIL.pdf.

HOVENKAMP, Herbert. Federal antitrust policy: the law of competition and its practice. Cap. 4. Thomson West, 3rd ed., 1994.

KERBER, Wolfgang. Digital markets, data and privacy: competition law, consumer law and data protection.

SALOMÃO FILHO, Calixto. Direito concorrencial: as estruturas. 2ª ed. São Paulo: Malheiros, 2002.

FORGIONI, Paula. Os fundamentos do Direito Antitruste. 8ª ed. São Paulo: RT, 2015.

STUCKE’S, Maurice. No Mistake About It: The Important Role of Antitrust in the Era of Big Data, 2015 (with Allen Grunes) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600051>

STUCKE’S, Maurice. Debunking the Myths Over Big Data and Antitrust, 2015 (with Allen Grunes) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612562>

STUCKE’S, Maurice. Big Data and Competition Policy, Oxford University Press, 2016 (with Allen Grunes) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598128>

STUCKE'S, Maurice. Should we be concerned about data-opolies?, 2018
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045>

SAKOWSKI, Patricia. A Rainha Vermelha no Antitruste, 2018. Disponível em
< <https://economiadeservicos.com/2018/10/16/a-rainha-vermelha-no-antitruste/>>