O SEGREDO DO NEGÓCIO DE EMPRESAS *VERSUS* O DEVER DE PORTABILIDADE DE DADOS PESSOAIS NA LGPD

Rodrigo Cantarino Carneiro Garcia[1]

RESUMO

O artigo procura estabelecer uma relação entre segredos de negócio e o recém-criado direito de portabilidade de dados pessoais, examinando, assim, um possível conflito normativo entre o acordo internacional TRIPS (Decreto nº 1355/1994) e a Lei Geral de Proteção de Dados Pessoais – também conhecida pelo acrônimo LGPD (Lei nº 13.709/2018). Para realizar o trabalho, optou-se por uma metodologia de pesquisa exploratória, analisando-se análise da doutrina especializada, inclusive estrangeira, em especial da doutrina europeia, dado a inspiração brasileira no regulamento da União Europeia sobre proteção de dados pessoais.

Palavras-chave: Propriedade Intelectual; Segredo de Negócio; LGPD; GDPR

COMPANIES' TRADE SECRETS VERSUS THE RIGHT OF DATA PORTABILITY DEMANDED BY BRAZILIAN LAW N° 13.709/2008

ABSTRACT

The article establishes a correlation between companies` trade secrets and the recently created right to data portability of personal data, examining a possible normative conflict between the TRIPS agreement (Decree no. 1355/1994) and the Brazilian General Data Protection Law (Law no. 13,709/2018). In order to write this paper, an exploratory methodology was used, drawing knowledge from specialists on the field, including using foreign doctrine, specially European, given that the Brazilian legislation was inspired by European`s General Data Protection Regulation.

---

1 Universidade Federal do Rio de Janeiro – Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação (PROFNIT).

Key-words: Intellectual Property, Trade Secrets, Brazilian Data Protection Law, GPDR

EL SECRETO DE NEGOCIO CONTRA EL DERECHO DE PORTABILIDAD GARANTIDO POR LA LEY BRASILENÃ Nº 13.709/2008

RESUMEN

El presente artículo establece una correlación entre los secretos de negocio de empresas y el recen creado derecho de portabilidad de datos personales, analizando el posible conflicto normativo entre el tratado internacional TRIPS (Decreto no. 1355/1994) y la Ley Brasileña de Protección de Datos Personales (Ley no. 13,709/2018). Para este artículo, utiliza-se una pesquisa exploratoria que busca el conocimiento de especialistas sobre el asunto, incluyendo en la doctrina extranjera, especialmente europea, visto que la ley brasileña fue inspirada en la Regulación General de Protección de Datos de la Unión Europea.

Palabras-llaves: Propiedad Intelectual, Secreto de Negocio; LGPD, GDPR

INTRODUÇÃO

Atualmente, percebemos um avanço gradativo no que tange à proteção normativa de dados pessoais. A aprovação da Lei n° 13.709/2018, chamada de Lei Geral de Dados Pessoais (LGPD), representa este avanço no cenário nacional. A nova legislação, que atualmente se encontra em período de vacância, é abertamente baseada na regulamentação europeia sobre o tema, a *Regulation (EU) 2016/6*, ou Regulamento Geral de Proteção de Dados Pessoais da Europa – também conhecido como GDPR (sigla do regulamento em inglês, *General Data Protection Regulation*).

A LGPD procura devolver ao cidadão brasileiro o "poder sob seus dados", o que pode ser sumarizado pelo princípio da Autodeterminação Informativa. Ao mesmo tempo, a lei pretende não inviabilizar a evolução tecnológica, uma vez que o atual momento tecnológico da sociedade indica uma sociedade baseada exatamente nos dados pessoais.

A LGPD brasileira e mesmo a regulamentação europeia podem gerar impacto na proteção do segredo de negócio, na forma como definida pelo acordo internacional "TRIPS" (*Trade-related Aspects of Intellectual Property Rights*) em seu artigo 39: uma informação confidencial que

proporciona ao seu titular uma vantagem econômica e cujo segredo é objeto de cuidado mediante medidas razoáveis por parte de seu titular. O acordo TRIPS passou a ser legalmente aplicável no Brasil a partir de sua promulgação, por meio do Decreto Presidencial número 1.355/1994 – e também é protegido em solo brasileiro pela Lei n° 9.279/1996, a Lei de Propriedade Industrial (LPI), em seu artigo 195, incisos XI e XII, que trata como crimes de concorrência desleal os atos que violam, de maneira ilícita, estes segredos de negócio.

Assim, o presente trabalho procurou averiguar se existe um possível conflito aparente de normas (TRIPS x LGDP) sobre a proteção dos segredos de negócios. Muito embora seja possível realizar uma análise detida da relação entre o segredo de negócio e diversos direitos da LGPD, como por exemplo o direito de explicação de decisões totalmente automatizadas, o presente artigo foca em apenas um destes direitos: o da portabilidade de dados pessoais, que acentua ainda mais a autodeterminação informativa, ao mesmo tempo que coloca em risco os segredos de negócio, em especial o que deveria estar sujeito a este dever de portabilidade dentro de um panorama em que um conjunto de dados pessoais (o *Big Data*) possa potencialmente ser considerado um segredo de negócio.

Esse estudo trata-se de um artigo científico, requisito para obtenção do grau de mestre no programa de mestrado profissional do Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação (PROFNIT), cujas linhas de pesquisa são a Propriedade Intelectual e a Transferência de Tecnologia, sendo esse artigo voltada ao estudo da primeira linha citada, na perspectiva da proteção do segredo de negócio, ativo intangível importante para o desenvolvimento econômico nacional (art.5º, XXIX da Constituição Federal e 2 da LPI), sendo que é objetivo dos Núcleos de Inovação Tecnológica (NITs) buscar meios de atuar na geração de desenvolvimento tecnológico e econômico nacional (art.1º, I, da Lei de Inovação).

Portanto, o estudo dos segredos de negócio em um cenário de inovação tecnológica no que tange à proteção de dados pessoais em um sistema jurídico em que se faz mandatória a observância de determinados deveres advindos da Lei Geral de Proteção de Dados Pessoais está de acordo com as linhas de estudo do programa. Sua relevância é demonstrada a partir do momento em que o exercício deste direito em específico poderá pôr em risco todo o investimento que é feito em prol da criação, do desenvolvimento e da manutenção de segredo que exigem o segredo de negócio.

A proteção do segredo de negócio, contudo, não é uma estratégia trivial, sendo extremamente vantajosa quando feita corretamente, tanto para empresas quanto para Núcleos de Inovação Tecnológicas (NITs) que fazem a ponte entre universidades e as empresas.

Sendo assim, trabalho se dividirá em dois momentos: primeiramente, será investigada a existência de uma relação entre segredos de negócio e dados pessoais, especialmente no que tange à tecnologia do *Big Data*. Feita esta análise, e, se confirmada a relação, será avaliado de que maneira o direito à portabilidade pode pôr em risco a proteção do ativo do segredo de negócio o que demandará do intérprete da lei (seja o NIT, o empreendedor ou o agente estatal localizado na Autoridade Nacional de Proteção de Dados) uma aplicação diferenciada do princípio da transparência (artigo 6º VI, da LGPD).

Para tanto, o estudo pretende abordar como objetivo geral o eventual conflito entre a proteção do segredo de negócio, em especial os fatores essenciais para sua proteção (artigo 39 do TRIPS) e a LGPD, especialmente no que tange o direito da portabilidade de dados pessoais (artigo 18, V, da citada lei), procurando ao possível motivação (*mens legis*[2]) do legislador pátrio. Este mesmo conflito pode ser visto também como uma ponderação constante entre dois fundamentos da LGPD: a Autodeterminação Informativa e o desenvolvimento econômico (artigo 2º, incisos II e V desta lei),

A partir deste objetivo geral, derivam-se os seguintes objetivos específicos:

- Indicar o conceito de segredo de negócio, sua forma de proteção na legislação nacional e princípios norteadores, o objetivo dessa proteção e sua importância.
- Analisar se há possibilidade de proteção por meio deste ativo para dados em formato de *Big Data*;
- Analisar o direito a portabilidade na Lei Geral de Proteção de Dados, buscando para tanto compreender a perspectiva do legislador ao aprovar tal lei no Congresso Nacional.
- Discorrer sobre eventual conflito entre o artigo 39 do acordo TRIPS e o artigo 18, V, da LGPD, concluindo pela existência ou não de conflito normativo, apontando possível desfecho para tal;

2 O espírito, a finalidade da lei.

Os objetivos destacados acima são de fundamental importância para compreender a questão de pesquisa: poderia o exercício do direito à portabilidade ser considerado um potencial risco ao segredo de negócio de empresas?

O trabalho foi desenvolvido a partir de pesquisa exploratória. Desse modo, como método, utilizou-se a revisão bibliográfica e legal e pesquisa documental, à luz da legislação vigente, instruções normativas e doutrina, com forte marcação teórica no GDPR haja vista a atual ausência de regulamentos da Autoridade Nacional de Proteção de dados (ANPD) para dar substância a este tema por meio de atos regulatórios da LGPD de cunho administrativo.

A verificação da existência de conflito normativo se deu com base na obra de Diniz (1998). Utilizando-se dos conceitos apresentados pela autora, é possível questionar a existência de uma antinomia real entre a LGPD e o acordo TRIPS, no que tange à regra dos segredos de negócio. Tal status antinômico pode ser percebido pois há incompatibilidade entre o princípio da Transparência da LGPD com a necessidade da manutenção no segredo para a existência do segredo de negócio, gerando assim uma indecisão sobre o que aplicar (a não revelação do segredo de negócio, frente à necessidade de transparência e eventual portabilidade), o que gerará, nos casos concretos, uma necessidade de decisão. Há uma lacuna de regras de solução, principalmente na ausência (ao menos temporária) de um ato normativo da ANPD para determinar de que forma deve ser interpretado tal conflito.

Para atingir os objetivos pretendidos, o presente trabalho foi organizado em dois capítulos: o primeiro procura examinar o conceito de Segredos de Negócio no ordenamento jurídico brasileiro, e posteriormente adentra em uma investigação a respeito da possibilidade ou não da proteção por via deste ativo para questões envolvendo dados pessoais, em especial no que tange o *Big Data*.

A partir daí, trabalharemos no segundo capítulo com a proteção de dados pessoais no território nacional. A fim de explorar o direito a portabilidade, primeiramente se faz necessário, contudo, avaliar o contexto de criação da LGPD, especialmente em contraste com a tradição europeia, possibilitando assim um panorama cuja comparação, embora não se pretenda definitiva, servirá como parâmetro de análise para o direito brasileiro. É importante mencionar que o direito a portabilidade possui diversas questões que merecem especial atenção, como por exemplo as dificuldades de questões de interoperabilidade de dados pessoais, porém estas questões serão postas

aparte no presente artigo para que se foque, especificamente, no potencial conflito do direito com os segredos de negócio.

1 SEGREDOS DE NEGÓCIO E DADOS PESSOAIS

Como dito, esta primeira sessão se dedicará ao segredo de negócio e suas possíveis intersecções com dados pessoais em si.

1.1 DEFINIÇÃO DE SEGREDO DE NEGÓCIO

Antes de mais nada, é necessário passar pela questão da nomenclatura dada ao instituto em questão no título. Isto porque, há muito, havia uma dicotomia entre os segredos de indústria, como questões que envolvem Pesquisa e Desenvolvimento, e os de comércio, que estão ligados mais ao mercado em si. Tal dicotomia é superada ao se adotar a nomenclatura mais ampla, denominada "segredo de negócio", que funciona como gênero para as duas espécies acima descritas (FEKETE, 2018).

Desta forma, ao longo do presente *paper*, será utilizada a nomenclatura segredo de negócio, ou mesmo seu sinônimo, segredo de empresa, para denominar este importante instituto da Propriedade Industrial.

A proteção do segredo de negócio no Brasil tem como base a repressão à concorrência desleal. Constitucionalmente, sua proteção se fundamenta no direito fundamental de proteção as criações intelectuais, (artigos 5º, XXIX, da Constituição Federal), além da proteção da intimidade e do sigilo da correspondência (FEKETE, 2018).

Além da garantia constitucional, esta proteção remonta ao acordo internacional administrado pela Organização Mundial de Comércio, denominado *Trade-Related Aspects of Aspects of Intellectual Property Rights* (TRIPS). Este tratado, ratificado pelo Brasil pelo decreto presidencial n° 1.355/1994, elenca em seu artigo 39, parágrafo segundo, os elementos essenciais para a proteção do segredo de negócio: (a) ser um segredo, ou seja, não ser de conhecimento acessível àqueles que teriam mais domínio técnico para obter aquela informação; (b) ter um valor comercial advindo justamente pelo fato de ser segredo; e (c) que a empresa detentora tome as precauções razoáveis para que o fato continue um segredo.

A leitura destes requisitos nos remete, exatamente, à definição de Fekete (2018) do instituto do segredo de negócio, qual seja, "conhecimento utilizável na atividade empresarial, de caráter industrial ou comercial, de acesso restrito, provido de certa originalidade, lícito, transmissível, não protegido por patente, cuja reserva representa valor econômico para o seu possuidor, o qual exterioriza o seu interesse na preservação do sigilo através de providências razoáveis".

Interessante notar a observação de Fekete (2003, p. 73) com relação ao elemento do segredo: diz a autora que é mantida a característica secreta quando o objeto de segredo não está "disponível para pessoas que se encontrem fora do círculo de confiança estabelecido pelo proprietário".

Com relação ao segundo requisito, da relevância econômica, Fekete (2003, p. 78) lança mão de um duplo teor valorativo: os gastos da empresa para obter aquele objeto do segredo e o que denomina de valor de raridade, ou seja, quanto aquilo vale.

Estes dois primeiros elementos são classificados como elementos objetivos do segredo. O terceiro elemento seria, então, o elemento subjetivo: é preciso querer manter em segredo, ou, em outras palavras, "[…] não se exige necessariamente que o titular tenha declarado expressamente sua vontade de manter o processo em segredo, é suficiente que sua vontade resulte claramente dos fatos" (FEKETE, 2003, p. 73).

A fim de incorporar as regras internacionais trazidas pelo TRIPS em uma lei nacional, pouco tempo depois da ratificação deste tratado foi sancionada a Lei n° 9.279/96, chamada de Lei de Propriedade Industrial (LPI). Para adequar-se à proteção contra atos de concorrência desleal, foi destacado o artigo 195 deste diploma, estipulando, em seu inciso XI, o crime contra utilização ou exploração não permitida de segredo de negócio a qual se teve acesso em razão de relação contratual ou empregatícia, enquanto o inciso posterior pune a divulgação e exploração de segredos obtidos por meio de espionagem industrial.

Barbosa (2002) salienta que os núcleos do tipo descritos acima configuram um crime, enquanto outras ações que não abarcadas por este tipo penal estariam relegadas apenas a ilícitos de natureza cível. Em se tratando de ilícitos civis, o artigo 209 da LPI garante direito de reparação por perdas e danos contra atos de concorrência desleal.

Cumpre informar que o artigo 195 da LPI é o único artigo que trata de segredos de negócio no Brasil, o que significa dizer que não há uma definição clara e precisa sobre o que pode ser um

segredo de negócio seja no diploma pátrio, ou no diploma internacional: que tipos de informações, conhecimentos ou dados confidenciais? Sua definição é propositalmente ampla de forma a garantir que o diploma não se tornasse anacrônico.

O que torna o segredo de negócio único frente a outros bens intangíveis é a inexistência de uma propriedade sobre o bem. Protege-se contra o ato de se obter de maneira ilícita o segredo – motivo pelo qual sua proibição se encontra disposta no rol dos crimes de concorrência desleal. Sua obtenção de forma lícita, contudo, é perfeitamente plausível e lícita.

1.2 SEGREDO DE NEGÓCIO E DADOS PESSOAIS: a dinâmica do *Big Data*

Após detalhamento a respeito da definição de segredos de negócio, esta sessão trata a discussão a respeito de uma possível interseção entre este ativo intangível e a proteção de dados pessoais, dando especial atenção para os dados que compõem o chamado *Big Data*.

1.2.1 O que é *Big Data* e como algoritmos criam maiores *insights*

Para explicar o *Big Data*, costuma-se lançar mão de certas palavras-chave, os "Vs" do *Big Data*. Inicialmente, falava-se nas três principais características da tecnologia: Volume, Variedade e Velocidade (RUSSON, 2011). Posteriormente, outras características foram adicionadas a estas três iniciais, havendo quem mencionasse variabilidade, valor e veracidade (GANDOMI; HAIDER, 2015). Há quem afirme, contudo, a existência de dez variáveis (SUN, 2018).

Isso mostra apenas que a tecnologia do *Big Data* ainda está sendo explorada, suas características essenciais ainda estão sendo descobertas e mais atributos essenciais à tecnologia são adicionados conforme seu estudo progride.

Segundo Mayer-Schönberger e Cukier (2013), o *Big Data* se refere a operações feitas com grandes quantidades de dados, como inferências probabilísticas, verificando relações entre diferentes informações. O Instituto McKinsey, em pesquisa voltada ao tema, entendeu que o termo se refere a um conjunto de dados cuja magnitude é muito maior do que a maioria dos sistemas poderia processar e analisar (MANYIKA, 2011). Há, portanto, uma convergência de entendimentos no que tange à quantidade e a escalabilidade do *Big Data* – a partir de grandes

quantidades de dados pessoais, é possível inferir ainda mais dados pessoais de grande valia para empresas.

Um algoritmo funciona como uma receita de bolo: cria-se um conjunto de instruções que devem ser seguidas para se chegar a um resultado. Há o conteúdo inicialmente submetido ao algoritmo, denominado *input*, o processo em si que o algoritmo realiza e o resultado final daquela operação, denominado *output*.

A evolução da ciência da computação possibilitou, então, o aprimoramento destes algoritmos, de modo a observar tendências, criando assim inferências probabilísticas capazes de dar ainda mais detalhamento da caracterização de indivíduos. Este processo pode ainda ser aprimorado com algoritmos de aprendizado de máquina (*machine learning*), que analisa as variáveis e, de acordo com o treinamento dado pelo algoritmo (dependendo, então, dos *inputs*), calcula uma infinidade de combinações probabilísticas em busca do melhor resultado – e aquela correlação passa, então, a ser o modelo com o qual a máquina analisará novos *inputs*, pois descobriu, em tese, o melhor padrão (BRAUNEIS; GOOMAN, 2018).

Levando em consideração a dinâmica entre os dados pessoais e os algoritmos, se faz necessário observar os tipos de dados pessoais que estão contidos no *Big Data*, em uma separação que, longe de ser meramente explicativa, implica diretamente no exercício do direito a portabilidade que será analisado mais adiante.

De acordo com um estudo da OCDE, há quatro tipos diferentes tipos de dados, a depender da forma como foram obtidos: fornecidos, observados, derivados e inferidos. O primeiro diz respeito a dados obtidos do próprio individuo em uma situação em que há certeza que os dados estão sendo transmitidos; dados observados dizem respeito a informações que foram observadas por terceiros e gravadas em formato digital (como os *cookies*); enquanto dados derivados são gerados de outros dados em uma lógica de padrão matemática, os dados inferidos são os mais complexos, baseados em análises probabilísticas e resultam na predição de comportamentos (ORGANIZATION…, 2014).

Assim, podemos perceber que o *Big Data* é composto, na verdade, por tipos de dados pessoais diferentes – nem todos fornecidos pelos próprios titulares. Sendo assim, como funciona sua relação com segredos de negócio?

1.2.2 *Big Data* como Segredo de Negócio

Antes de atestar qualquer avaliação do *Big Data* como segredo de negócio, se faz necessário endereçar uma questão fundamental, que é a possível proteção do *Big Data* como direito autoral a bancos de dados.

Conforme disposto na Lei n° 9.610/1998, em seu artigo 7º, inciso XIII, é protegido sob direito autoral, as coletâneas ou compilações, bases de dados e outras obras similares, desde que o valor artístico esteja imbuído justamente nesta compilação. Esta disposição também segue diretamente um comando do já citado TRIPS, que determina que deve haver tal proteção em seu artigo 10.2.

Dar às bases de dados uma proteção autoral, é bom que se diga, rende pesadas críticas de especialistas notórios como Ascenção (1997), que afirma que o critério que orienta a criação de uma base de dados não pode ser entendido como uma criação do espírito humano. Este *paper*, contudo, não entrará nos méritos de tal discussão. Fato é que os segredos de negócio e os direitos autorais tutelam questões distintas de um bem, sendo ao menos em teoria perfeitamente possível uma coexistência de ambos os fatores em um objeto

Vencida esta etapa, há que se questionar se, dada a elasticidade do conceito de privacidade de dados para alcançar aqueles dados que são públicos, eles já não seriam, desde logo, excluídos da proteção de segredos de negócio. Afinal, muitas bases de dados são formadas, ou incorporadas, com dados que possuem um acesso facilitado. A respeito deste tema, é preciso compreender, primeiramente, que a proteção de dados pessoais rompe com a dicotomia público-privado no que tange à privacidade, alcançando até dados públicos de acesso mais facilitado (BIONI, 2019).

Inicialmente, poderia se considerar que não haveria nenhum conflito entre o direito a portabilidade e os segredos de negócio, uma vez que apenas dados pessoais de um titular em si talvez não fossem criar real problemática para o segredo de negócio da empresa. Esta afirmação, contudo, não pode ser feita de maneira leviana, haja vista a classificação de dados que foi vista no tópico anterior. Enquanto a portabilidade de dados obtidos ou observados talvez não venha a ferir os segredos de negócio quando há uma transmissão de dados de apenas um titular, o mesmo pode não ser verdade para dados inferidos. A obtenção de dados inferidos, por sua natureza comportamental, é de essencial valor para empresas, e, contraditoriamente, só pode ser obtido um

dado de qualidade ao se analisar e contrastar tipos distintos de dados de diversos titulares, ou seja, efetivamente fazer uso do *Big Data* como um todo para se chegar aos dados inferidos.

Sendo assim, faz-se necessário examinar o caráter de segredo de negócio da base de dados como um todo, uma vez que apenas a partir desta será possível a obtenção do dado cuja portabilidade é uma real ameaça a vantagem competitiva empresarial, o dado inferido.

É bom que se note, primeiramente, que não há que se falar aqui em uma diferenciação entre dados públicos e privados. A união de dados públicos e privados, inclusive, já foi considerada um segredo de negócio em um caso americano, em que se disputava se o conhecimento geral de partes de um segredo de negócio prejudicavam sua qualificação como tal. A questão, discutida no Kansas, foi decidido pelo tribunal que "*[k]ansas law recognizes that, even though individual features of a broader feature combination might exist in the market, the combination of those features nonetheless may qualify as a trade secret provided that the combination itself satisfies the requirements of the trade secret statute*".[3]

Há neste julgado a citação de um segundo, também sobre segredo de negócio, em que se afirma: "um segredo de negócio pode existir em uma combinação de componentes, cada um destes, por si só, em domínio público, sendo a sua combinação um segredo".[4]

A análise dos conceitos para aplicação do segredo de negócio a esta tecnologia também é muito trabalhada no âmbito da União Europeia. Novamente, antes de se adentrar nesta questão, é preciso garantir que a proteção deste ativo no bloco econômico segue os mesmos padrões brasileiros.

Isto pode ser observado ao constatarmos a Diretiva Europeia de Segredo de negócios, adotada em 2016, a *Directive (EU) 2016/943*. Apesar de os requisitos do segredo de negócio serem, de fato, muito similares àqueles adotados pelo acordo TRIPS (e, portanto, pelo Brasil), é importante notar um fato que dá ao diploma europeu mais facilidade interpretativa do que no caso brasileiro: a presença de exemplos e considerações – chamado no direito europeu de *Recitals*, que, assim

---

3 UNITED STATES DISTRICT COURT OF VIRGINIA. **Beacon Wireless Solutions, Inc. et al v. Garmin International, Inc. et al, No. 5:2011cv00025 - Document 38 (W.D. Va. 2011)**. Disponível em: https://law.justia.com/cases/federal/district-courts/virginia/vawdce/5:2011cv00025/80396/38/. Acesso em: 1 jun. 2019.

4 SUPREME COURT OF KANSAS**. Mann v. Tatge Chem. Co.** Disponível em: https://law.justia.com/cases/kansas/supreme-court/1968/45-031-0.html. Acesso em: 03 jul. 2019.

como no Brasil, não possuem força de lei, mas somente força interpretativa (WACHTER; MITTELSTADT; FLORIDI, 2017).

Neste sentido, há alguns *consideranda* que chamam atenção para os fins deste trabalho: o segundo, que explicitamente dá o exemplo de "dados sobre os consumidores" como formas de segredo de negócio. Esta declaração entra em aparente contradição com aquela apresentada por dois outros *consideranda*: o de número 34, em que a diretiva declara que obedece à Carta da União Europeia de Direitos Humanos, incluindo o direito fundamental à privacidade de dados, e o considerando número 39, em que se diz, especificamente, que a diretiva não deve afetar adversamente qualquer outro direito.

O conflito surge a partir do momento em que, no GDPR, por diversas vezes há a determinação que os direitos à privacidade encontram uma limitação nos segredos de negócio. Ou seja, mesmo no âmbito europeu há aparente contradição entre a diretiva de segredos de negócio europeia e a regulamentação europeia de proteção de dados. Este conflito se mostra tão aparente que, ao analisar os impactos do *Big Data* para os dados pessoais, o *European Data Protection Supervisor* (2015) sugeriu que lidem com a dualidade transparência *versus* segredo tenham a participação das autoridades nacionais de proteção de dados.

Ao analisar este conflito aparente, Malgieri (2016) apresenta importante reflexão: a princípio, em um conflito direto, os direitos à privacidade parecem prevalecer, mas um olhar mais detido permite compreender que há, tão somente, uma situação de não-prevalência imediata entre um e outro, devendo, efetivamente, ser analisado caso a caso qual direito deve prevalecer (MALGIERI, 2016).

Esta digressão à diretiva europeia de segredos de negócio, contudo, serve apenas para demonstrar que há, em tese, possibilidade do *Big Data* ser considerado um segredo de negócio, inclusive contando com exemplos da própria diretiva europeia sobre o tema. Partamos, então, para analisar as situações em que esta proteção lhe socorrerá, ou seja, analisando os três requisitos essenciais com base no TRIPS.

Primeiramente, é preciso fixar o parâmetro básico de ser um segredo. Para o cumprimento deste fator há um incentivo, ou um poder-dever, do próprio detentor destes dados pessoais de mantê-los sob segredo, devido às legislações de proteção de dados (BANTERLE, 2016).

Este dever de segredo se manifesta em diversos dispositivos das leis de proteção de dados, inclusive na LGPD, como por exemplo: o dever de manter padrões de segurança da informação a

níveis adequados para evitar ao máximo vazamentos; a limitação do direito de transferência de dados pessoais a terceiros; e até mesmo a personalização do direito de acesso, no sentido que cada titular só poderá requisitar acesso a dados referentes a si mesmo, nunca de terceiros (o que, a princípio, elimina a possibilidade de eliminação de segredo do bloco de dados como um todo, mas não reduz a problemática dos dados inferidos ou observados).

Há também na doutrina um questionamento referente ao efetivo segredo do dado, de modo que há *data sets* que seriam de fácil acesso a qualquer pessoa, criando assim um conflito com a exigência do TRIPS de que ele não deve ser facilmente acessível (RADÓN, 2015-2016). Compreendemos este argumento, contudo seria teoricamente possível argumentar, em contrapartida, em favor até mesmo destes dados, uma vez que o poder computacional para reter toda esta quantidade de dados não seria prontamente acessível a todos, além de que, como visto nos julgados mencionados acima, até mesmo dados públicos podem ser considerados partes de um segredo de negócio.

Com relação ao segundo requisito, qual seja, a valoração ou potencialidade econômica do ativo por ser segredo, pouco poderia se questionar a respeito. Em uma economia que gira em torno dos dados, fazer uso destes para gerar inferências e observações tem sido o maior ativo de diversas empresas, e mesmo governos, quando se fala em cidades inteligentes.

Solove (2011) chega a incluir em sua obra (ainda que não fale especificamente sobre segredos de negócio neste momento), que o importante não é a informação, mas sim o conhecimento que é separado e analisado, sendo o real valor do dado obtido apenas quando processamos a informação e podemos utilizá-la produtivamente. O que seria esta afirmação senão uma ratificação do segundo requisito do segredo de negócio? É este trabalho em cima dos dados que gera um conhecimento valioso – e ele só é valioso justamente por seu segredo, pois se fosse de fácil obtenção, seria uma informação não valiosa *per se* (e neste raciocínio podemos incluir o conglomerado de dados ou até mesmo apenas dados inferidos).

Cumpre notar, ainda sobre este requisito, que não há uma definição do que deveria ser este valor econômico, ou qualquer mensuração, sendo algo de fato abstrato, fazendo com que ele seja, usualmente, presumido, uma vez que as medidas de proteção sejam observadas (RADÓN, 2015-2016).

Com relação a medidas adequadas, a doutrina faz referência a um teste de proporcionalidade – uma vez que o nível de adequação é algo fluido, a depender de diversos fatores. O teste é

composto por diversas fases, quais sejam: (i) tamanho da empresa, (ii) importância da informação, (iii) setor da empresa, (iv) experiência prévia com segredos de negócio, (v) tipo e número de empregados, e (vi) medidas internas de proteção (DREYFUSS; STRANDBURG, 2011). Outros autores apontam que as próprias leis de proteção de dados (inclusive a LGPD) já determinam estas medidas adequadas como *default* (BANTERLE, 2016). No caso brasileiro, alguns exemplos destas medidas seriam o acesso dos dados pessoais feitos apenas por equipe autorizada e normas de segurança como senhas fortes.

Por fim, conforme dito anteriormente, cumpre mencionar que a proteção de segredos de negócio para os dados inferidos também seria possível: Gervais propõe o exemplo de um *data set* de *Big Data* utilizado gerar uma base de correlações entre pessoas e suas preferências (o que, como vimos, são considerados dados pessoais inferidos), este novo corpo de dados (somente de dados inferidos) pode ser considerado segredo de negócio (GERVAIS, 2019).

Chega-se à conclusão que Pasquale estava correto quando identificou que as famosas caixas-pretas da sociedade de informação são, muitas vezes, o próprio segredo de negócio [PASQUALE 2015].

Vistos os três requisitos, conclui-se pela possibilidade que o bloco de dados de *Big Data* seja um segredo de negócio, inclusive pelas leis brasileiras – haja vista uma referência nacional indireta ao diploma internacional TRIPS para buscar por seus requisitos.

2 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E O DIREITO DE PORTABILIDADE

Feitas as considerações na seção anterior a respeito da possibilidade da proteção dos segredos de negócio para bases de dados como o *Big Data*, que possuem considerável quantidade de dados pessoais, partimos então para uma análise da proteção de dados pessoais em si. Para tanto, será primeiramente traçado um breve panorama desta proteção jurídica, apontando para uma aproximação brasileira com o pensamento europeu e, posteriormente, analisaremos a Lei Geral de Proteção de Dados Pessoais em si.

2.1 UM POSSÍVEL DIREITO FUNDAMENTAL A PRIVACIDADE E A INFLUÊNCIA EUROPEIA

É quase impossível falar em dados pessoais sem citar o artigo de Samuel Warren e Louis Brandeis, publicado em 1890, em que eles constroem a fundamentação do Direito à Privacidade nos Estados Unidos – defendendo o direito de ser deixado só, ou em paz, e sua invasão sendo uma infração (WARREN; BRANDEIS, 1890).

A tradição europeia, contudo, é a que certamente mais influencia o Brasil até os dias atuais. No velho continente, talvez o julgado mais eloquente que passa a tratar de dados pessoais tenha ocorrido em 1983, ano em que a corte alemã julgou um caso a respeito de um censo que estava sendo realizado naquele território. Naquele julgado, o tribunal, de maneira progressista, afirma veementemente a existência de um direito do cidadão de autodeterminação informativa, sendo um direito fundamental de poder ao indivíduo de "determinar sobre a divulgação e uso de seus dados pessoais"[5].

Tamanha é a importância da autodeterminação informativa que, passados trinta e cinco anos, aparece como fundamento legal da LGPD, em seu artigo segundo. A partir deste dispositivo, procura-se devolver ao cidadão o poder sobre seus dados (VAINZOF, 2019). A este fundamento foram agregados outros, tal como o desenvolvimento econômico e tecnológico e a livre iniciativa. É este diálogo entre o detentor da tecnologia com o titular dos dados pessoais que a LGPD pretende realizar, de modo a balancear uma relação que se encontrava, até então, deficiente.

Além disso, cumpre mencionar que o direito a proteção de dados pessoais é alçado, na União Europeia, a categoria de direito fundamental[6], sendo inclusive apartado do direito a personalidade devido a sua especificidade[7]. Rodotá (2008, p. 18) afirma, ao tratar especialmente sobre o caráter essencial deste direito, que o mesmo deve ter limites, sem, contudo, ferir o núcleo duro do direito fundamental a proteção de dados pessoais.

---

5 BVerfGE 65, 1 – Volkszahlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die ¨ mundliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 ¨ in den Verfahren uber die Verfassungsbeschwerden. Decisão traduzida disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 04 jul. 2019.

6 Para leitura detalhada a respeito deste direito fundamental, constante no artigo 8º da Carta de Direitos Humanos da União Europeia, recomenda-se a leitura de RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar. 2008. p. 17-19.

7 A respeito da necessidade de separação entre estes dois princípios, recomenda-se a leitura de BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 100.

É a partir desta reflexão sobre quais seriam os limites aceitáveis que nos debruçamos sobre o direito a portabilidade e a limitação promovida pelos segredos de negócio – especialmente porque o *status* de direito fundamental para a proteção dos dados pessoais tramita atualmente no Congresso Nacional como Proposta de Emenda à Constituição brasileira (BRASIL, 2019).

Cria-se, assim, um diálogo com Alexy (2006, p. 103), em sua célebre diferenciação entre regras (o "tudo ou nada") e princípios, verdadeiros mandados de otimização. Com efeito, há uma necessidade de sopesamento entre o este futuro direito fundamental da proteção de dados pessoais e o princípio da livre iniciativa, basilar para o segredo de negócio. Ao analisarmos a LGPD em específico, tal necessidade de sopesamento aparece explicitamente diversas vezes, como na definição do princípio da transparência e mesmo na delimitação do direito de portabilidade, onde, em ambos os casos, o legislador determinou a observação do segredo de negócio.

Esta interpretação, contudo, apresenta-se como um desafio para o panorama nacional, haja vista que o Brasil não possui um histórico robusto de proteção de dados pessoais (ao passo que o GDPR veio substituir a antiga diretiva europeia de proteção de dados pessoais, aprovada em 1995, o que demonstra maturidade e experiência do bloco para tratar da questão).

Propõe-se, contudo, um meio de analisar o direito a portabilidade no Brasil: como visto acima, é notória a inspiração na legislação europeia que se busca para legislar sobre o tema de dados pessoais no Brasil. Sendo assim, é possível ao menos vislumbrar uma hipótese de inspiração nas interpretações europeias sobre o direito de portabilidade, o que justifica uma análise do diploma estrangeiro para procurar lançar uma luz sobre o novo direito em solo nacional. Antes, porém, faz-se necessária breve introdução sobre o processo legislativo da LGPD, para então analisarmos o direito de portabilidade.

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS

A partir do presente tópico, analisaremos de maneira detida a Lei Geral de Proteção de Dados Pessoais no Brasil. Esta análise visa dar subsídios para um enfoque mais detalhado no direito da portabilidade de dados, previsto na lei, cujo enfoque será dado ainda nesta sessão.

2.2.1 Processo Legislativo: a importância de uma Autoridade Nacional Regulamentadora

A LGPD foi sancionada em agosto de 2018 pelo ex-presidente Michel Temer. O Projeto de Lei, cuja trajetória no Congresso Nacional foi marcada por diversos diálogos com a sociedade civil, inicialmente previa uma Autoridade Nacional de Proteção de Dados Pessoais – ANPD, mas as disposições a respeito deste órgão foram vetadas pelo *staff* presidencial entender que havia ali uma inconstitucionalidade na criação, por parte do poder executivo, de uma autoridade administrativa[8]. Este problema foi sanado pelo próprio Michel Temer, que, em dezembro de 2018, publicou a Medida Provisória no. 869/2018 – que, após reformulações no Congresso Nacional, gerou um Projeto de Lei de Conversão, sancionado em 08 de julho de 2019, gerando a Lei no. 13.853/2019.

A ANPD é peça-chave no desenvolvimento de um ambiente regulatório de proteção de dados pessoais, sendo encarregada (tanto pela lei brasileira quanto na de diversos países, ou quanto a União Europeia) de emitir guias, interpretações, fiscalizar e aplicar sanções com relação à proteção de dados pessoais. Aponta-se, contudo, para a falha da MP em colocar a ANPD diretamente sob o comando administrativo da Presidência da República, fato que foi amplamente criticado pela doutrina especializada (DONEDA, 2018).

Em alteração proposta pelo Congresso Nacional à Medida Provisória e sancionada pelo Presidente, tal necessidade foi capturada, determinando que o *status* da ANPD como órgão da presidência seja somente transitório: será possível transformá-la em ente autárquico federal independente no período de 2 anos de sua criação.

Além disso, houve uma alteração pontual no que tange o direito de portabilidade, alterando a ordem onde a regulamentação da ANPD é mencionada – dando agora a entender que o que a Autoridade regulamentará será a forma como a portabilidade deve ser realizada, e não como os segredos de negócio devem ser observados. Ao mesmo tempo, o Projeto de Lei de Conversão manteve como uma das atribuições principais da Autoridade o zelo pelos segredos de negócio – a segunda atribuição, logo após a proteção de dados pessoais, o que, topograficamente, tem um grande significado. Por esta razão, pode-se depreender que a alteração na ordem das palavras do inciso relativo ao direito de portabilidade não significa, necessariamente, um detrimento ao ativo de propriedade intelectual.

---

8 Uma digressão precisa e detalhada a respeito do processo legislativo pode ser encontrada em BIONI, Bruno R. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **JOTA**, 02 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em 02 de jun. 2019.

2.2.2 O Direito de Portabilidade

Visto o processo legislativo, e o importante papel que a ANPD terá neste ecossistema, partamos então para a análise do direito de portabilidade de dados pessoais. Interessante notar que este direito poderia ser interpretado (e provavelmente o será) em prol do titular, quando seus interesses forem sopesados com os dos controladores de dados. Aqui possivelmente veremos, portanto, uma aplicação da lógica do *favor debilis*, tão presente em nosso direito do consumidor, em que se interpreta um direito com base no elo mais vulnerável da relação negocial – no caso, o titular de dados pessoais (MARQUES, 2011).

Apontando para este caminho (embora não com as estas palavras), Maldonado (2019) explica que o direito à portabilidade é essencial contra uma prática conhecida no mercado como *vendor lock-in*, que vinculava o usuário por excessivo custo para realizar a modificação do prestador do serviço (MALDONADO, 2019).

Dessa forma, este direito (tanto no diploma europeu quanto no diploma brasileiro) O direito a portabilidade, nos moldes do GDPR – assim como no Brasil – visa dar maior enfoque no poder de decisão do titular de proteção de dados a respeito do que deve ser feito com aqueles dados que o representam. O *Working Part* 29, ao emitir *guidelines* sobre o tema, demonstra tal incentivo ao mencionar que tal meio é uma prevenção ao *lock-in* comercial (ou seja, reter um cliente meramente por conta de domínio de seus dados), além de promover oportunidades de inovação aberta por meio de um compartilhamento regulado de dados pessoais, sob demanda dos próprios consumidores (ARTICLE, [2017], p. 5).

Conforme apontado por Graef, Purtova e Husovec (2018, p. 1369), no entanto, não existe uma condição limitante para se realizar esta portabilidade, seja comercial ou social. Isto significa que, no caso do GDPR (assim como no caso da lei brasileira), não há necessidade de se explicar uma razão para requisitar a portabilidade, sendo apenas um exercício do direito, de maneira imotivada. Haveria, então, em tese, a possibilidade de o consumidor querer simplesmente repassar suas informações até mesmo em detrimento de investimentos das empresas em elaboração estudos e técnicas de análise de dados pessoais para conhecer melhor sua clientela – sendo assim potencialmente um segredo de negócio.

Para evitar interpretações neste sentido, o GDPR incluiu uma cláusula limitante ao direito de portabilidade – não poder atingir, inadvertidamente, direitos de terceiros. A LGPD, por sua vez,

utilizou uma abordagem menos genérica, ao explicitamente constar que deve ser observado o segredo de negócio.

2.2.2.1 A perspectiva europeia

O direito de portabilidade, na forma como regulado pelo GDPR, em seu artigo 20, pode ser exercido de duas maneiras distintas: uma portabilidade para si (ou seja, transferir todos os dados para o titular), e para outro controlador. Esta transmissão deve ser feita sem afetar direitos e liberdades de terceiros.

2.2.2.1.1 Quando a portabilidade afeta direitos de terceiros

Há uma centralização da figura do titular no exercício do direito de portabilidade. Esta centralização, muito embora aponte para a autodeterminação informativa, pode, por outro lado, significar em um detrimento do próprio segredo de negócio da empresa (TARKOMA, 2018, p. 64).

Para ilustrar este possível efeito desestimulante do mercado, Vanberg e Ünver (2017) relembram o caso de um modelo de negócios que é baseado em encontrar melhores tamanhos para suas roupas, compartilhando tal medida com lojas que comercializam tais roupas. Caso o direito a portabilidade seja aplicado, todo o modelo de negócio desta empresa se perderia pelo simples exercício regular do direito dos titulares de dados.

De modo a evitar que este direito cause prejuízos, o próprio GDPR tratou de incluir uma salvaguarda em seu artigo 20, determinando que o direito de portabilidade não deverá afetar de maneira negativa direitos e liberdades de terceiros. O hoje extinto *Article 29 Working Party* (2017, p.12), compreendendo que tal direito poderia ferir exatamente os direitos de segredo de negócio de empresas, alerta em parecer hoje adotado pelo EDPB que o direito a portabilidade não pode ser utilizado para ferir práticas leais de mercado ou violar direitos de propriedade intelectual.

A forma como o direito de portabilidade pode entrar em choque com o segredo de negócio assume três frentes distintas: mina com a vantagem competitiva do dado acumulado, exige o compartilhamento do que antes era exclusividade, e pode terminar com um lucro por licenciamento de dados daquela qualidade (GRAEF; PURVOTA; HOSOVEC, p. 1378). Malgieri (2018, p. 193-203) complementa que não deve ser criada uma limitação injusta, medida esta que acabará sendo

decidida de acordo com o caso concreto, possivelmente levando em consideração fatores como a forma como os dados são utilizados, expectativas razoáveis a respeito do dado, e salvaguardas adicionais.

Não obstante, questiona-se o que de fato deve ser transferido. O direito a portabilidade apenas garante a transferência dos dados fornecidos pelo próprio titular, de acordo com a determinação do GDPR, mas o EDPB entende que dados observados pelas atividades do usuário também se encaixariam nesta modalidade, o que é distinto de dados inferidos, que não deveriam ser repassados[9]. A doutrina especializada tende a entender tal limitação como uma forma de proteger o segredo de negócio[10], porém não podemos deixar de questionar se uma portabilidade dos dados observados não seria desaconselhável, partindo do pressuposto que imprime-se certo esforço em coletar, armazenar e mesmo utilizar como *input* estes tipos de dados para gerar melhores dados inferidos.

Com ou sem a transferência de dados observados, entendemos ser um parâmetro essencial para efetivamente aplicar uma adequada salvaguarda aos direitos de portabilidade, haja vista que uma portabilidade completa de dados resultaria em um direito onde não mais se justificaria o investimento em ferramentas e técnicas preditivas, haja vista que tal vantagem competitiva desapareceria mediante o mero exercício de tal direito.

2.2.2.1.2 Portabilidade para si mesmo

Além desta portabilidade para terceiros, conforme dito, a portabilidade também pode ser requerida para si mesmo. A este respeito, é justo e necessário se perguntar qual seria a diferença entre uma "portabilidade para si mesmo" e o simples direito de acesso.

Neste ponto, há uma controversa questão que merece análise: enquanto o direito de acesso daria acesso a diversas informações, inclusive aquelas não obtidas diretamente do titular de dados por força do artigo 14 do GDPR, a limitação do artigo 20 do regulamento europeu é cristalina: o

9 "Thus, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour". **Fonte:** ARTICLE 29 WORKING PARTY. **Guidelines on Portability…** p. 10.
10 EDWARDS, Lilian. Data protection: enter the general data protection regulation. **Hart Publishing**, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182454. Acesso em 21 de jun. 2019. p. 45, Nota de rodapé n° 173; TARKOMA, Janne. *Op. Cit.* p. 63, nota de rodapé n° 527

direito de portabilidade, seja com transferência para terceiros ou para si mesmo, somente inclui informações dadas pelo próprio titular.

Ao enfrentar esta questão, o órgão regulamentador de privacidade inglês (ICO) sugere que o controlador dos dados adote uma postura proativa de interpretação da intenção do titular: caso fique claro que ele quer ter acesso a dados inferidos, estas informações deveriam ser incluídas no relatório de resposta ao pedido, mesmo que o titular tenha, sem o devido cuidado ou a devida informação, requisitado o "direito à portabilidade", quando queria ter pedido o "direito de acesso" (INFORMATION…, [201?]). Sobre esta dicotomia de direitos, o EDPB entende que há uma complementação entre um e outro (ARTICLE, 2017, p. 5).

2.2.2.2 A perspectiva brasileira: o que está sendo desenhado

O tratamento do direito à portabilidade é diferente no diploma pátrio. Segundo a LGPD, o titular tem direito de requisitar a portabilidade para outro fornecedor de produto ou serviço, observado o segredo comercial e industrial ("segredo de negócio"), de acordo com a regulamentação da ANPD.

A mais nítida diferença, a ser notada na prática, é a ausência, ao menos literal, de uma "portabilidade para si mesmo". Este tipo de portabilidade, contudo, é enxergado pela doutrina brasileira. Para Frazão (2018), aplicar-se-ia, na interpretação da LGPD, uma interpretação extensiva, no sentido de que, se o titular dos dados pessoais pode requisitar o direito de portabilidade para terceiros, também poderia requisitar uma portabilidade para si. Monteiro (2018) também parece entender da maneira, quando menciona, a respeito deste, que "*[it] allows the data subject not only to request an entire copy of their data, but also to have them provided in an interoperable format*".

Maldonado (2019) vai além e verifica a existência explícita do direito de portabilidade para si mesmo no artigo 19, parágrafo 3º, quando este menciona o direito de o titular solicitar a cópia integral de seus dados pessoais (MALDONADO, 2019).

Duas observações cabem a respeito deste ponto do artigo 19: primeiramente, cabe observar que o mesmo parágrafo diz que deve ser observado o segredo de negócio, o que pode indicar, talvez, que a cópia não seja – literalmente – integral, embora tenha-se indicado que a ANPD regulamentará o parâmetro desta limitação. Além disso, cumpre destacar que o artigo 19 diz

respeito ao direito de acesso a dados pessoais, e não ao direito de portabilidade, havendo assim, na lei brasileira, a mesma dualidade entre os direitos de acesso e portabilidade que encontramos na União Europeia.

Ao observarmos, especificamente, o direito de portabilidade, questiona-se o conteúdo dos dados que devem ser abarcados por este. Enquanto no GDPR, como visto, há uma limitação explícita para os dados apenas fornecidos pelo titular (havendo ainda uma diferenciação entre dados observados e inferidos), a LGPD não faz a mesma ressalva: é garantida a portabilidade dos dados, observado o segredo de negócio (BIONI; GOMES; MONTEIRO, 2018), ressalvando ainda que haverá regulamentação da ANPD para estes casos – possivelmente para tratar de questões de interoperabilidade, um dos grandes desafios do direito a portabilidade.

Como já estudado na seção anterior, no que tange o *Big Data*, sua proteção como segredo de negócio, apesar de atingir todo o conjunto de dados pessoais ali agregados, também poderá ser individualmente aplicado a dados inferidos. Desta forma, um vácuo normativo a respeito de que tipo de dados poderia ser transferido com o direito a portabilidade, fatalmente, poderia criar uma situação de disparate, em que o segredo de negócio fica subjugado ao direito da portabilidade, quando não é este o comando legal, mas sim um balanço entre os direitos.

Resta ao Brasil, deste modo, a regulamentação por parte da ANPD, que, por força de determinação legal, não poderá se furtar de emitir instrução a respeito do tema. Trata-se, em analogia ao direito constitucional, de uma norma de eficácia contida, em que há regulação sobre a matéria, mas aberta para regulamentação de lei infraconstitucional – neste caso, regulamentação pelo órgão regulador (MORAIS, 2011). É possível, inclusive, que a ANPD entenda por bem restringir o direito à portabilidade aos dados passados pelo próprio titular, em uma inspiração na legislação europeia.

Outra questão que deve ser submetida ao crivo da Autoridade é, justamente, uma melhor modelação frente as diferenças entre o direito à portabilidade e o direito ao acesso. Como vimos, os órgãos supervisores europeus têm enfrentado questionamentos a respeito disso, especialmente porque, para o caso de portabilidade para si mesmo, é claro e explícito que os titulares de dados poderão reter e reutilizar como bem entenderem seus próprios dados (ARTICLE, 2017).

Não há, textualmente, na LGPD, uma limitação ao direito de que informações seriam passíveis de acesso – ficando esta limitação registrada no princípio da transparência. Fica o questionamento de como seria a reutilização de dados inferidos de posse do titular de dados

pessoais que requisitou direito de acesso com base na LGPD e, posteriormente, reutilizou-os encaminhando para o concorrente. Esta seria considerada uma prática anticoncorrencial, levando em conta que os dados inferidos podem potencialmente ser considerados segredos de negócio *per si*?

CONSIDERAÇÕES FINAIS

Após esta análise, é possível averiguar possível conflito normativo entre o acordo TRIPS e a Lei Geral de Proteção de Dados, na forma do exercício do direito de portabilidade de dados pessoais. Constata-se que, caso algum conjunto de dados pessoais (tal como um *Big Data*) venha a reunir os três requisitos de segredos de negócio, assim poderiam ser considerados – especialmente no que tange dados inferidos.

Isto posto, é inegável que há um conflito entre a manutenção do segredo de negócio e o exercício do direito de portabilidade – questão que até mesmo na União Europeia, bloco econômico com longa experiência de proteção jurídica a dados pessoais, enfrenta determinadas questões delicadas (como o balanceamento entre a portabilidade e o acesso a dados pessoais). Esta situação se agrava no Brasil pela falta de um detalhamento maior sobre o direito a portabilidade na LGPD, sendo uma disposição tímida que carece de maiores esclarecimentos.

A princípio, poderia se indagar se a solução para o conflito existente estes direitos seria tão simplesmente a edição de uma norma que auxilie na interpretação para os conflitos que surgirão, o que deverá surgir por um ato normativo da ANPD. No entanto, fato é que nenhuma norma será capaz de resolver em definitivo o conflito, de modo que, certamente, será necessário utilizar-se da ferramenta da ponderação, conforme nos ensina Alexy (2006), em cada caso concreto. A ausência de casos concretos no Brasil para medir esta ponderação, no entanto, se sobressai no atual momento, de modo que não é algo trivial que possa ser feito na forma de uma pesquisa. A entrada em vigor da LGPD, em agosto de 2020, colocará os testes em prática, e a atuação da ANPD é de fundamental importância para uma interpretação clara e inequívoca deste direito.

Por ora, a única afirmação concreta possível a respeito deste conflito normativo entre LGPD e acordo TRIPS no Brasil é justamente a mesma a qual chegou Malgieri (2016), ao analisar este mesmo conflito dentro da União Europeia (no âmbito do GDPR contra a diretiva de segredo de negócio): há um status de não prevalência entre estes estatutos, mas não em questão de comparação

de leis, mas sim dos direitos garantidos aos titulares em cada lei, sendo que, no que tange ao direito da personalidade, deve ser estudada uma forma de transmissão baseada no contexto, sem os ``*outputs* econômicos`` dos dados. Com isto, concordamos, haja vista que, em um embate entre a livre iniciativa e a autodeterminação informativa, é preciso verificar no caso concreto de que maneira a portabilidade deverá ser aplicada.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2006. Disponível em: http://noosfero.ucsal.br/articles/0010/3657/alexy-robert-teoria-dos-direitos-fundamentais.pdf. Acesso em: 02 de jun. 2019.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on the right to data portability.** Adopted on 13 December 2016, as last revised and adopted on 5 April 2017. Disponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099. Acesso: 05 jul. 2019.

ASCENSÃO, José de Oliveira. **Direito autoral**. 2. ed. ref. e ampl. Rio de Janeiro: Renovar, 1997.

BANTERLE, Francesco. The interface between data protection and IP law: the case of trade secrets and database sui generis right in marketing operations, and the ownership of raw data in *Big Data* analysis. *In*: Bakhoum, M. *et. al.* (orgs). **Personal data in competition, consumer protection and intellectual property law towards a holistic approach?** New York: Springer, 2016.

BARBOSA, Denis Borges. **Do Segredo Industrial**. [*s.l.: s.n.*], 2002.

BIONI, Bruno R. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. **JOTA**, 02 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso: 02 jun. 2019.

_____. Privacidade e proteção de dados pessoais em 2019. **JOTA**, 28 de jan. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2019-28012019. Acesso: 02 de jun. 2019.

_____. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; GOMES, Maria Celina Oliveira; MONTEIRO, Renato Leite. GDPR matchup: Brazil`s General Data Protection Law. **IAPP**. 4 out. 2018. Disponível em:

https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Acesso: 21 de jun. 2019.

BRASIL. Congresso Nacional. Senado Federal. **Proposta de Emenda à Constituição n° 17 de 2019**. Acrescenta o inciso XII-A, ao art. 5º e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1559251870862&disposition=inline. Acesso: 2 jun. 2019.

BRAUNEIS, Robert; GOODMAN, Ellen. Algorithmic Transparency for the Smart City. **20 Yale Journal of Law and Technology**. n. 103, 2018. Disponível em: https://www.yjolt.org/sites/default/files/20_yale_j._l._tech._103.pdf . Acesso: 05 jul. 2019.

BVerfGE 65, 1 – Volkszahlung Urteil des Ersten Senats vom 15. Dezember 1983 auf die ¨ mundliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 ¨ in den Verfahren uber die Verfassungsbeschwerden. Decisão traduzida disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso: 04 jul. 2019.

CHESBROUGH, Henry. **Open Innovation**: the new imperative for creating and profiting from technology. Cambridge: Harvard Business School Press, 2003.

CHESBROUGH, Henry; CROWTHER, Adrienne Kardon. Beyond high-tech: early adopters of open innovation in other industries. **R&D Management**, v. 36, n. 3, 2006. Disponível em: http://web.simmons.edu/~weigle/INNOVATION/Chesbrough%20and%20Kardon.pdf. Acesso: 01 set. 2017.

CHESBROUGH, Henry; VANHAVERBEKE, Wim; WEST, Joel. **Open innovation**: researching a new paradigm. Oxford: Oxford University Press. 2006.

COMISSION NATIONALE DE L`INFORMATIQUE ET DES LIBERTÉS. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC**, 21 jan. 2019. Disponível em: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Acesso: 02 jun. 2019.

DINIZ, Maria Helena. **Conflito de Normas**. 2. ed. rev. e amp. São Paulo: Saraiva, 1998.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova lei geral de proteção de dados brasileira *In*: BELLI, Luca; CAVALLI, Olga (org.).**Governança e regulações da Internet na América Latina**: análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on internet governance. Rio de Janeiro: FGV, 2019.

DONEDA, Danilo. O que está em jogo com a nova Autoridade Nacional de Proteção de Dados. **JOTA**, 13 ago. 2018. Disponível em <https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018>. Acesso: 02 jun. 2019

DREYFUSS, Rochelle C.; STRANDBURG, Katherine J. (eds). **Trade secrecy, innovation and the requirement of reasonable secrecy precautions the law and theory of trade secrecy.** Camberley: Edward Elgar Publishing Limited, 2011.

EDWARDS, Lilian. **Data protection: enter the general data protection regulation**. Oxford: Hart Publishing, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182454. Acesso: 21 jun. 2019.

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 7/2015: meeting the challenges of *Big Data* A call for transparency, user control, data protection by design and accountability**. União Europeia: EDPS, 2015 Disponível em: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf . Acesso: 02 jun. 2019.

EUROPEAN UNION. **Regulations, Directives and other acts.** Disponível em: https://europa.eu/european-union/eu-law/legal-acts_en. Acesso: 02 jun. 2019.

FEKETE, Elizabeth Kaznar. **O Regime jurídico do segredo de indústria e comércio no direito brasileiro**. Rio de Janeiro: Forenze, 2003.

_____. Segredo de Empresa. *In*: CAMPILONGO, Celso F.; GONZAGA, Alvaro de A.; FREIRE, André L. (coords.). **Enciclopédia Jurídica da PUCSP**. Tomo Direito Comercial, edição 1, julho de 2018. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa. Acesso: 02 de jun. 2019.

FRAZÃO, Ana. Nova LGPD: ainda sobre o direito à portabilidade. **JOTA**, 14 nov. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-o-direito-a-portabilidade-14112018. Acesso: 02 jun. 2019.

GANDOMI, Amir; HAIDER, Murtaza. Beyond the hype: *Big Data* concepts, methods, and analytics. **International Journal of Information Management**. v.35, n. 2, abr. 2015, p. 137-144. Disponível em: https://reader.elsevier.com/reader/sd/pii/S0268401214001066?token=2EB61EB53DC3534325D6727084E592A570C737FD67878F73AA19DE22600C652947F1D50FF2648AAB1302E62B91FB0602. Acesso: 25 jun. 2019.

GERVAIS, Daniel. Exploring the interfaces between *Big Data* and intellectual property law. **JIPTEC**, 2019. Disponível em: https://www.jipitec.eu/issues/jipitec-10-1-2019/4875/JIPITEC_10_1_2019_3_Gervais_Big_Data_IP. Acesso: 03 de jul. 2019.

GRAEF, Inge; PURTOVA, Nadezhda; HUSOVEC, Martin. Data portability and data control: lessons for an emerging concept in EU law. **German Law Journal,** v. 19, n. 16., 2018. Disponível em: https://www.researchgate.net/publication/322236453_Data_Portability_and_Data_Control_Lessons_for_an_Emerging_Concept_in_EU_Law. Acesso: 22 jun. 2019.

IINFORMATION COMISSIONERS OFFICE. **Right to data portability**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability. Acesso: 03 jul. 2019.

MALDONADO, Viviane Nóbrega. Dos direitos do titular. *In*: NOBREGA, Viviane Maldonado; BLUM, Renato Ópice (coord.). **Lgpd**: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil. 2019.

MALGIERI, Gianclaudio *et. al*. The right to data portability in the GDPR: towards user-centric interoperability of digital services. **Computer Law and Security Review**. 2018, p. 193-203.

MALGIERI, Luciano. Trade secrets vs personal data: a possible solution for balancing rights**. International Data Privacy Law**, v. 6, n. 2, maio 2016.

MANYIKA, James, *et al*. *Big Data*: the next frontier for innovation, competition, and productivity **McKinsey Global Institute**. Jun. 2011. Disponível em: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx. Acesso: 21 maio. 2019

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 6. ed ver., atual. e ampl. São Paulo: RT, 2011.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. ***Big Data*****:** a revolution that will transform how we live, work and think. New York: HMH books. 2013.

MAZZUCATO, Mariana. **O estado empreendedor**: desmascarando o mito do setor público vs setor privado. São Paulo: Portfolio; Penguim, 2014.

MITROU, Lilian. **Data protection, artificial intelligence and cognitive services:** is the general data protection regulation (GDPR) "artificial intelligence-proof"? *[s.l.: s.n.]*, abr. 2019. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2PdYu. Acesso: 02 jun. 2019.

MONTEIRO, Renato Leite. The new brazilian general data protection law: a detailed analysis. **IAPP**, 14 ago. 2018. Disponível em: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/. Acesso: 21 jun. 2019.

MORAIS, Alexandre de. **Direito Constitucional**. 27. ed. São Paulo: Atlas. 2011.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Protecting Privacy in a Data-driven Economy**: taking stocks and current thinking. [*s. n.: s. l.*], 2014. Disponível em: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en. Acesso: 02 jul. 2019.

_____. **The OECD Privacy Framework**. [*s. n.: s. l.*], 2013. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso: 02 jun. 2019.

PASQUALE, Frank. **The Black box Society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PORTILHO, Raphaela Magnino Rosa. **Open Innovation e os direitos da propriedade intelectual:** interseção ou dicotomia? a atuação dos instrumentos contratuais na promoção da inovação aberta. Rio de Janeiro: Gramma, 2016.

RADOŃ, Barbara Anna. **Trade Secrets Protection for '*Big Data*'**: personal data as trade secrets in the European Union. MIPLC Master Thesis Series (2015/16). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3012525. Acesso: 2 jun. 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar. 2008.

RUSSON, Philip. ***Big Data*** **Analytics.** TDWI: Renton, 2011.

SANDEEN, Sharon K. Lost in the cloud: information flows and the implications of cloud computing for trade secret protection. **Virginia Journal of Law and Technology**, v. 19, 2014.

SOLOVE, Daniel J. **Nothing to hide**: the false trade off between privacy and security. London: Yale University Press, 2011.

_____. **The digital person**: technology and privacy in the information age. New York: New York University Press, 2004.

SUN, Zhaohao. *Big Data* with ten big characteristics. **ICBDR 2018 Proceedings of the 2nd International Conference of *Big Data***, p. 56-61, Weihai, China, Octocber, 27-29, 2018. Disponível em:https://dl.acm.org/purchase.cfm?id=3291822. Acesso: 25 jun. 2019.

TARKOMA, Janne. ***Big Data*** **and data protection in the context of EU competition law.** Helsinke: Department of Accounting and Commercial Law, 2018. Disponível em: https://pdfs.semanticscholar.org/9883/e58814ff24f55fcd6ce37924384ce856e0d9.pdf. Acesso: 03 jul. 2019.

SUPREME COURT OF KANSAS**. Mann v. Tatge Chem. Co.** Disponível em: https://law.justia.com/cases/kansas/supreme-court/1968/45-031-0.html. Acesso: 03 jul. 2019.

UNITED STATES DISTRICT COURT OF VIRGINIA. **Beacon Wireless Solutions, Inc. et al v. Garmin International, Inc. et al, No. 5:2011cv00025 - Document 38 (W.D. Va. 2011)**. Disponível em: https://law.justia.com/cases/federal/district-courts/virginia/vawdce/5:2011cv00025/80396/38/. Acesso: 1 jun. 2019.

VAINZOF, Rony. Disposições preliminares *In*: MALDONADO, Viviane Nobrega; BLUM, Opice Renato. **LGPD**: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil. 2019.

VANBERG, Anysem Diker; ÜNVER, Mehmet Bilal. The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? **European Journal of Law and Technology**, v. 8, n. 1, 2017. Disponível em: http://ejlt.org/article/view/546/726. Acesso: 03 jul. 2019.

WACHTER, Sandra, MITTELSTADT; Brent, FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation**.** **Oxford Academic: International Data Privacy Law**, v. 7, n. 2, May 2017, p. 76–99.

WARREN S D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso: 04 jul. 2019.