Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet[1]

How to Qualify Personal Data? A Theoretical and Legal Assessment in the European Union

Submetido(*submitted*): 15/11/2017
Parecer(*revised*): 19/12/2017
Aceito(*accepted*): 13/03/2018

Judith Rochfeld[2]

Resumo

Propósito – O presente artigo tem por objetivo debater o conceito de dados pessoais, a partir da legislação europeia, perpassando por temas relativos à proteção e à comercialização.

Metodologia – Trata-se de pesquisa teórica e jurídica, na qual, a partir do debate do valor dos dados pessoais produzidos pelos usuários na internet, discutem-se suas possíveis características jurídicas. Isso ocorre por meio da análise do fenômeno da monetização dos dados pessoais em contraste com as visões decorrentes das teorias realistas e personalistas. No plano da análise documental, é explorada a legislação da União Europeia (Carta Europeia de Direitos Fundamentais, Regulamento Geral sobre Proteção de Dados – Regulamento (UE) 2016/679, de 27 de abril de 2016 – e a legislação francesa. São analisados, ainda, casos judiciais concretos.

Resultados – É analisada e testada uma categorização das teorias jurídicas acerca do conceito de dados pessoais: teorias realistas; e teorias personalistas. As teorias realistas qualificam os dados pessoais como bens ou produtos, que podem ser de propriedade dos usuários, dos operadores ou do coletivo. Já as teorias personalistas cuidam da proteção dos dados e das pessoas que os produzem, bem como de sua privacidade, uma vez que tais dados carregam traços de sua identidade. O artigo testa e concluir positivamente pelo uso dessa categorização teórica.

Implicações práticas – O trabalho pretende fornecer uma contribuição para refletir sobre os limites e as possibilidades de tratamento dos dados pessoais na era digital. Revela-se que esse tratamento pode ter uma característica mais econômica e patrimonialista, ou

[1]Texto derivado do seminário internacional "A efetividade do direito em face do poder dos gigantes da Internet – Brasil e França", realizado na Universidade de Brasília no período de 13 até 15 de abril de 2016. Agradece-se ao fomento da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), da Fundação de Amparo à Pesquisa do Distrito Federal (FAPDF), da Embaixada da França no Brasil e das universidades brasileiras e francesas envolvidas. Texto traduzido por Marsel de Souza. Revisão técnica de Alexandre Veronese. Diagramação e apoio de Murilo Borsio Bataglia.

[2]Professora Titular (*Professeur Agregé*) de Direito Privado na *École de Droit de la Sorbonne, Université Panthéon-Sorbonne* (*Paris 1*), na qual dirige o Master 2 de Direito do Comércio Eletrônico e da Economia Digital (*Droit du commerce électronique et de l'économie numérique*). Pesquisa na área de direito civil: contratos, obrigações, consumidor e a renovação da propriedade e dos bens comuns, além de direito digital. É membro do projeto de pesquisa ANR PROPICE – *Agence Nationale de Recherche* – "Propriedade Intelectual, Bens Comuns e Exclusividade" (*Propriété intellectuelle, communs et exclusivité* e do projeto de pesquisa *EnCommun*. É autora de diversos livros, dentre os quais se destacam: "*Les grandes notions du droit privé*" (PUF), prêmio do livro jurídico de 2012; e o "*Dictionnaire des biens commun*" (PUF, 2017), em conjunto com Marie Cornu et Fabienne Orsi. Email: judith.rochfeld@univ-paris1.fr.

proteger a identidade do indivíduo contida nos dados produzidos. O propósito é fortalecer o debate sobre o poder de consentimento ao uso de dados pessoais, tanto em prol do empoderamento técnico e jurídico das pessoas, quanto sobre a possibilidade de controle sobre seus dados individuais e coletivos.
Originalidade – A originalidade se traduz no fato do artigo evidenciar uma pesquisa sobre um tema crucial do direito, com forte implicação para todos os países. Não existe artigo publicado na língua portuguesa sobre essa temática, com o presente enfoque. Tal pesquisa foi realizada a partir da realidade europeia, listando os principais modos de possíveis de uso dos dados pessoais. Porém, ela evidencia um quadro teórico que é útil para pensar sobre a realidade brasileira e de outros países, também.

Palavras-chave: dados pessoais, privacidade, comércio de dados, teorias realistas e personalistas, União Europeia, Estados Unidos.

Abstract

Purpose – *This article aims to discuss the concept of personal data, based on European law, raising it up from themes related to its protection and commercialization.*
Methodology – *It is a legal and theoretical research, whose starting point is the debate on the value of personal data produced by users on the Internet. From this point forward, the article draws the theoretical features of the concept of personal data. The research draws its force from both the realistic and personality theories and the exam of the European Union Law (Charter of Fundamental Rights, EU Regulation 2016/679 of 27 April 2016). The paper also analyses the French law and judicial cases.*
Findings – *The paper analyses and tests two sets of theoretical frameworks: realistic and personality theories. The realistic theories qualify personal data as goods or products, which may be owned by users, by enterprises, or by the society as a whole. The personality theories, however, creates the concept of personal data from the individual protection and from the people who produces the data. The concept of privacy is deeply rooted in the latter theories, since they conclude that the data carry, in itself, some elements of its owner identity. The paper tests and concludes that those two sets of theoretical frameworks are useful to address the problem.*
Practical implications – *The article raises awareness about the limits and possibilities of data processing in the digital age. The legal framework to the processing tasks may focus on the economic and patrimonial features or it must try to protect the personal identity on the process? The practical implication is to strengthen the debate over the consent for the use of personal data, in order to bring on both a technical and legal empowerment of the people and the control over their own individual and collective data.*
Originality/value – *The originality comes from the innovation of that debate over a relevant aspect of the digital society. There is no equivalent article published in Portuguese. The original research focus initially the European reality producing a list of the main possible uses of personal data. Notwithstanding, the research is useful to understand different and abroad countries by comparison.*

Keywords: personal data, privacy, trade of data, realist and personality theories, European Union.

Os gigantes da Internet têm o direito de se apropriar dos dados pessoais dos usuários de seus serviços?

No contexto atual, a questão do título reveste-se de uma grande importância em razão do valor que os dados pessoais dos usuários representam e pelas críticas que têm sido dirigidas às empresas globais, denominadas de gigantes da Internet (Google, Amazon, Facebook e Apple)[3]. E, também, pelo fato de que os internautas e usuários de equipamentos eletrônicos conectados em rede estão cientes deste valor e, ainda, dos riscos inerentes aos vários processamentos destes dados. Vale observar que, atualmente, mais dados pessoais são coletados a cada semana do que ocorria durante o último milênio inteiro. E, ainda, deve-se ter em conta que cada dispositivo conectado tem o potencial de gerar bilhões de dados coletáveis. Ainda, essa possibilidade de coleta aumenta exponencialmente com o aumento da tecnologia. Embora seja impossível verificar os números, que variam consideravelmente, estima-se que o valor dos dados pessoais dos cidadãos poderia representar um trilhão de euros em 2020, considerando apenas os dados da União Europeia (ROSE, REHSE, RÖBER, 2012).[4]

Mas, como é possível transformar dados pessoais em valor? Eis um exemplo que permite uma imersão na economia subterrânea da segmentação e da predição, a partir do processamento de dados pessoais, para direcionar a visualização de informações dirigidas por meio de interfaces escondidas dos nossos computadores. As informações sobre as preferências e as preocupações do usuário são armazenadas no disco rígido do computador através dos *cookies* de conexão ou de navegação. Eles são pequenas sequências de códigos, armazenados à medida que as visitas são feitas pelos internautas em sítios eletrônicos variados da Internet. Posteriormente, essas informações são ativadas quando o usuário navega: os *cookies* fornecem detalhes dessas visitas aos parceiros de agências de publicidade especializadas, responsáveis pela gestão desses dados coletados. As agências celebram contratos com os sítios eletrônicos para essa finalidade. Em seguida, as agências analisam e adaptam de forma extremamente rápida (em centésimos de segundo) a publicidade destinada especialmente à pessoa visada[5]. Assim, um comerciante ou prestador de serviço (ou, mais precisamente, a agência que administra sua conta de publicidade) torna-se capaz de fornecer (ou deveria sê-lo), em um tempo muito curto, uma lista específica de produtos e de serviços

[3]O termo "gigantes da Internet" ("Géants de l'Internet") tem sido usado de forma corrente pelos veículos de imprensa da União Europeia. Todavia, possui a expressão possui uso acadêmico. Um uso antigo: WEISS, CAPOZZI, PRUZAK, 2004. Porém, a literatura jurídica contemporânea tem usado o termo para indicar que essas empresas globais possuem características peculiares (KIM & TELMAN, 2015).

[4]O jornal francês Le Monde informou, em um artigo de junho de 2013, que fontes dos Estados Unidos da América estimavam o valor dos dados pessoais europeus em 315 bilhões de dólares americanos, para o ano de 2012 (LE MONDE, 2013).

[5]Sobre as diferentes técnicas da propaganda segmentada (FRANÇA, 2014b: 60 e seg).

relacionados com as visitas anteriores e os interesses dos internautas, de forma direcionada. Na prática, como evidenciam os números anteriormente mencionados, os dados pessoais são assim monetizados, cedidos, revendidos, transferidos e terceirizados dentro e fora da União Europeia, enquanto novos atores – *dataminers, databrokers*, analistas, especialistas em algoritmos, etc. – tornam-se centrais na economia digital.

No entanto, essa evolução envolve vários tipos de interesses.

Em primeiro lugar, haja vista a possibilidade de prever nossos comportamentos e influenciá-los (através da publicidade ou da seleção de informações particularmente relevantes com base em análises preditivas, conduzidas a partir de perfis sociais aos quais somos ligados pelos dados), surgem, obviamente, questões de liberdade individual e de livre arbítrio. Esse processo é denominado *consumer profiling* (perfilhamento do consumidor) pela literatura técnica (RALLET, ROCHELANDET, ZOLYNSKI, 2015). Desse modo, quando usuário faz uma pesquisa com um conhecido motor de pesquisa da Internet, os resultados que ele obterá não serão os mesmos que aqueles oferecidos para o seu vizinho, porque dependem justamente de pesquisas anteriores, palavras-chave utilizadas, o perfil do internauta definido a partir de *cookies*, etc.

Em segundo lugar, na esteira do ponto precedente, deve-se considerar a questão de luta contra a discriminação de usuários por empresas, com base nos seus perfis sociais. Com efeito, esse potencial de previsão suscita um grande interesse por parte das seguradoras, dos empregadores, dos bancos, dentre outras empresas. Daí, surge uma necessidade democrática de regular os usos que podem se fazer dos dados pessoais.

Em terceiro lugar, houve uma grande conscientização, na Europa, sobre as questões de privacidade e de reputação, que ocuparam um lugar de destaque no cenário jurídico após a importante decisão do Tribunal de Justiça da União Europeia, em relação à Google Spain, em 13 de maio de 2014, sobre o "direito ao esquecimento" (UNIÃO EUROPEIA, 2014b). A decisão envolveu o senhor Costeja Gonzalves, que ficou insatisfeito ao constatar que os resultados de pesquisa feita na Internet por meio do Google (obtidos a partir da indicação do seu nome) incluíam informações a respeito da apreensão de seus bens ocorrida havia doze anos, em razão de falta de pagamento de suas dívidas à seguridade social. O senhor Costeja Gonzalves conseguiu que o Google retirasse os resultados do mecanismo de busca, com base nas disposições do artigo 8º da Carta de Direitos Fundamentais da União Europeia, de 2000[6], que consagra o direito ao

[6] Artigo 8º, (1): "Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito" (UNIÃO EUROPEIA, 2000a).

respeito dos dados pessoais[7]. Tendo em mente os três principais debates acima, o artigo tratará, na próxima seção de uma emergente questão importante: já existem internautas, hoje, a exigir participação nos lucros que seus dados permitem gerar.

Nesse contexto, para enfrentar todas estas questões no âmbito da tradição do direito civil, que tende a depender do regime aplicável à qualificação inicial, pode ser útil determinar a necessidade de considerar os dados pessoais como bens – e, nesse caso, quem seriam os seus proprietários. Outra possibilidade seria designá-los com qualificações que os ligam ainda mais à pessoa da qual são provenientes. Alguns dos principais textos europeus em vigor – isto é, a Lei de 6 de janeiro de 1978, chamada "Proteção e Liberdade", na França (FRANÇA, 1978)[8], e a Diretiva 95/46/CE, de 24 de outubro de 1995, da União Europeia (UNIÃO EUROPEIA, 1995), que será substituída no dia 25 de maio de 2018 pelo Regulamento Geral sobre Proteção de Dados, aprovado em 27 de abril de 2016 – não mencionam nada sobre o assunto. O novo Regulamento, no seu artigo 4º (1), define os dados pessoais como "(...) informação relativa a uma pessoa singular identificada ou identificável" (UNIÃO EUROPEIA, 2016b), sendo especificado que:

> "(...) é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (UNIAO EUROPEIA, 2016b).

Todavia, essa definição não traz respostas definitivas sobre o assunto. Além disso, se considerarmos o conteúdo dos textos mencionados para tentar encontrar pistas, descobriremos que eles representam padrões de circulação de dados – considerados mais como bens – e definem ao mesmo tempo um sistema de proteção da pessoa. Assim, estamos diante da constatação de que os textos atualmente em vigor não trazem uma resposta definitiva e expressiva à seguinte pergunta: o que é qualificação dos dados? Eles seriam, em uma visão realista, bens que poderiam ser objeto de uma apropriação e de um direito de propriedade e, neste caso, isso ocorria em que condições? Ou, de outro modo, ele poderiam pertencer, em uma visão personalista, ao regime jurídico das pessoas?

[7]Esta sentença é posterior a uma outra decisão importante, tomada com base no Artigo 8º como texto de aplicação efetiva, desta vez contra o poder público, que foi o caso Digital Rights Ireland Ltda contra Kärntner Landesregierung e outros (UNIÃO EUROPEIA, 2014a).

[8]Este texto foi bastante pioneiro na Europa, mas regia, no momento de sua adoção, apenas a relação dos indivíduos com registros mantidos pelo Estado, que eram muito poucos à época (DEBET *et alli*, 2015; AIGRAIN, 2014).

A tese realista: é possível falar de "propriedade" dos dados pessoais?

Na visão realista, o dado pessoal seria um bem e um elemento de valor para o qual a lei asseguraria um direito de propriedade (BELLANGER, 2014a[9]; BABINET, 2014), ou ao menos um modo de apropriação individualizado por uma pessoa. Todavia, a sua apropriação não significa necessariamente que toda coleta e tratamento de dados pessoais, mesmo cedidos remunerada ou gratuitamente seriam permitidos, pois a lei pode prever limitações à criação e à circulação de quaisquer bens que tenham, ou não, valor. Externamente à discussão sobre dados pessoais, a qualificação de bens "não comerciais" aplica-se, por exemplo, a elementos perigosos ou com ligação especial à pessoa responsável (a exploração ou tráfego legal são proibidos para armas ou para determinados drogas, por exemplo)[10]. Mas, em princípio e sob a ressalva de uma supervisão e limitações específicas (o que seria constatado pela existência de um regime especial previsto pela legislação em vigor), a coleta, a circulação e o comércio de dados pessoais seriam autorizados pelas teorias realistas.

As teorias realistas em abstrato

Todavia, tal circulação econômica ocorreria em benefício de quem? Ou seja, quem seria o seu "feliz proprietário"? São aqueles que estão na origem dos dados que devem auferir seu valor, sabendo que nós todos disseminamos nossos dados, ou aqueles que os armazenam, processam e lhes conferem justamente esse valor? Quem se tornaria proprietário dos dados e se beneficiaria da riqueza que eles representam? A questão é espinhosa porque é preciso perceber que, se um determinado dado ou conjunto de dados relativos a um único usuário pode ter um valor – para alimentar uma publicidade segmentada que lhe seja específica, por exemplo –, estaríamos diante de um ecossistema complexo e caro, criado por iniciativa dos agentes econômicos responsáveis pelo processamento dos dados. Em especial, os dados adquirem muito mais valor quando são processados em conjunto: os especialistas evocam o "gráfico", os cruzamentos, a "rede" (BELLANGER, 2014b)[11] de dados que lhes permitem conectar e construir

[9]Com a ressalva de que Pierre Bellanger mudou de opinião, posteriormente.

[10]No entanto, essa qualificação foi retirada do texto geral do artigo 1.162 do Código Civil francês, após a reforma do Direito dos Contratos pela Ordenança n. 131/2016, de 10 de fevereiro de 2016. O texto atual é o seguinte: "*Le contrat ne peut déroger à l'ordre public ni par ses stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties*". A noção, contudo, permaneceu em outros textos referentes a contratos especiais, seja para venda, seja para empréstimo.

[11]A contribuição de Pierre Bellanger que trata dos algoritmos de correlação, ou seja: "(...) programas de computador que, com base em probabilidades, permitem deduzir informações através do processamento preditivo de uma massa de dados sem relação direta com a informação inferida", o que faz com que "(...) cada dado pessoal traga indiretamente informações sobre terceiros", bem como 'o efeito da rede', isto é, o fato de que o valor de um dado seja "(...) proporcional ao quadrado do número de dados aos quais está

algoritmos eficientes que resultam em várias formas de indicações e previsões. O *Big Data* e o *Big Analysis*, tendências em destaque na economia digital de hoje, chamam especificamente a atenção para o processamento e o reprocessamento de grandes quantidades de dados de vários usuários. A expansão desses sistemas de processamento maciço dá azo à localização, na verdade, de quatro posições diferentes nesse sentido nas teorias realistas.

A primeira sustenta a defesa da propriedade de cada internauta com relação a seus dados: cada um seria proprietário de seus dados e poderia reivindicar seu uso, sua destinação e seu valor junto a um operador. As vantagens desta posição são inegáveis: ela tem o mérito de permitir a proteção de pessoas e encontrar uma redistribuição equitativa do valor (BELLANGER, 2014a). Porém, representa também desvantagens inegáveis: por um lado, oculta a valorização de dados através de sua vinculação coletiva; por outro lado, isso seria apenas parcialmente eficaz para a proteção pessoal. O Conselho Nacional Digital da França (*Conseil National du Numérique*), no seu parecer de maio de 2014, resumiu muito bem as principais falhas desta direção: "(...) ele transfere a responsabilidade de gestão e proteção de dados para o indivíduo" e "(...) reforça o individualismo e nega o equilíbrio de poder entre consumidores e empresas; só poderia gerar uma pequena receita para os usuários e criar um mercado de proteção de dados digitais". Por fim, continua o relatório: "(...) ela levaria à exacerbação das desigualdades entre cidadãos capazes de gerenciar, proteger e monetizar seus dados e cidadãos que, por falta de cultura literária, tempo, dinheiro ou outra coisa, deixariam estas funções para o mercado" (FRANÇA, 2014a: 37; PEUGEOT, 2014). O Conselho de Estado da França posicionou-se da mesma forma no seu relatório de 2014, definindo até o valor do benefício individual de cada um "(...) na ordem de alguns centavos ou algumas dezenas de centavos" (FRANÇA, 2014b: 265).

Uma segunda resposta leva em consideração a contribuição dos operadores (BELLANGER, 2014a): os dados seriam *res nullius* e não pertenceriam a ninguém enquanto não fossem capturados. Portanto, os atores da economia digital, como os primeiros ocupantes, se apropriariam dos dados e poderiam usá-los e valorizá-los à vontade (BELLANGER, 2014a)[12]. O Presidente Barack Obama, quando pediu à União Europeia que respeitasse a "propriedade" dos principais operadores no Vale do Silício, tais como os Gigantes da Internet, demonstrou que apoia essa tese (OBAMA & SWISHER, 2015). Pode-se citar também o direito francês, no artigo 571 do Código Civil, que determina que, se a mão-de-obra – a indústria – for mais importante que a matéria-prima na criação de valor, o proprietário será o responsável pela sua implementação, sob pena do

ligado", cada dado completando seu significado em um contexto e com dados adicionais (BELLANGER, 2014b).

[12]Lembrando que o autor mudou de posição posteriormente.

pagamento do valor da matéria bruta[13]. Obviamente, a vantagem certa desta posição reside no fato de reconhecer o consequente trabalho feito pelos operadores. As desvantagens não são menos visíveis: favorecer (demais) os operadores, ignorar perigosamente a ligação com a pessoa e, sobretudo, abandonar qualquer proteção desta contra os riscos mencionados.

Para tentar conciliar essas duas visões – propriedade dos internautas e a dos operadores –, uma terceira posição reintegra, por sua vez, o papel da pessoa e mantém ao mesmo tempo a ideia de propriedade: os dados seriam bens revestidos de uma textura muito especial, por causa da conexão que mantêm com a pessoa que os originou; em paralelo com a propriedade intelectual, eles seriam uma criação do internauta. Assim, e em vista dos benefícios, o internauta seria o proprietário dos dados e, como qualquer autor, deveria ser consultado sobre os usos dessas "obras" e ser remunerados por elas. Alguns até sustentam a ideia de que tal compensação pode, de acordo com o mesmo paralelo, ser recolhida pelas empresas de cobrança e distribuição dos valores amealhados (CHEMLA, 2013). A título de objeção a essa percepção, no entanto, pode-se duvidar que os dados sejam uma "criação" do usuário original, da qual os operadores não participariam (são eles que lhe dão seu valor).

Ademais, no âmbito dessas visões que consideram os dados como "bens", não se deve ignorar uma quarta posição que os considera como propriedade comum. Esta qualificação – como propriedade comum ou bem comum –, que, aliás, confere vantagens a essa posição, significa que os dados podem ter um destino coletivo e que seu uso deve ser o mais aberto possível, principalmente para favorecer a inovação e impedir sua concentração nas mãos das empresas gigantes do ramo. Além disso, essa posição demanda a definição de um regime que exige a necessidade de uma governança coletiva baseada em interesses gerais definidos coletivamente. Assim, os dados serão extraídos do domínio único dos grandes operadores privados e dos grandes confinamentos de monopólio, bem como em oposição a uma gestão pautada unicamente pelos interesses comerciais, para uso em favor da inovação ou de finalidades de interesse geral e/ou coletivo (PEUGEOT, 2014; ARGENTON & PRÜFER, 2012; FRANÇA, 2014a). Apesar das desvantagens dessa posição e do fato de que a tese dos bens comuns traz consigo ambições de proteção individual e coletiva, com as quais concordamos, pode-se notar que essa direção é mais aplicável a dados públicos, não para os

[13] Art. 571, Código Civil francês: "No entanto, se a mão de obra era tão importante que ultrapassava muito o valor da matéria empregada, a indústria seria então a parte principal, e o trabalhador teria o direito de reter a coisa trabalhada, reembolsando ao proprietário o preço da matéria estimado na data do reembolso". No original: "*Si, cependant, la main-d'oeuvre était tellement importante qu'elle surpassât de beaucoup la valeur de la matière employée, l'industrie serait alors réputée la partie principale, et l'ouvrier aurait le droit de retenir la chose travaillée, en remboursant au propriétaire le prix de la matière, estimée à la date du remboursement*".

dados pessoais. Afinal, essa orientação poderia justificar a imposição às pessoas de usos de seus dados que elas não teriam necessariamente aceitado, em nome de interesses coletivos maiores. Assim, tal ideia pode também incorrer na negação do forte laço existente entre os dados e as pessoas.

Finalmente, o que pensar dessas visões "realistas"? Confessamos que não aderimos a elas. Do ponto de vista filosófico, em primeiro lugar, utilizar os termos "bem", "propriedade" e "valor" significa dar pouca importância à textura dos dados, notadamente pelo fato de que eles podem revelar uma parte da identidade e da personalidade de cada um. Em segundo lugar, do ponto de vista estratégico, isto é, quanto a uma proteção eficiente contra os riscos mencionados – manipulação de comportamentos, discriminações e revelações não desejadas da vida privada –, é preciso enfatizar o fato de que, ao defender os dados, não estamos defendendo apenas um bem ou um valor econômico. Com efeito, trata-se de proteger a privacidade das pessoas por meio da transparência no processamento de seus dados (digitais e não digitais) e sua privacidade (ao menos quando os dados pessoais dizem respeito à vida privada, o que não é sempre o caso). Mesmo a segunda posição, que restabelece a ligação com a pessoa – embora tenhamos questionado a ideia de que os dados são "criações" do internauta –, não reintroduziu a consideração da possível violação de privacidade e dos outros riscos mencionados.

Teorias realistas no direito positivo

No entanto, deve-se notar que a prática (em que os dados são trocados em mercados, como mencionamos previamente) e os direitos positivos, tanto na Europa, como nos Estados Unidos, defendem, em parte, uma concepção de dados como valores. Certamente, os textos europeus têm avançado sobre uma corda bamba, em um equilíbrio instável, em busca de um acordo, uma vez que não fazem menção à questão crucial daquilo que eles pretendem proteger de forma prioritária: o fluxo de dados para garantir a perenidade dos modelos econômicos ou a proteção das pessoas?[14] Os próprios títulos dos textos jurídicos são vagos. A Diretiva 95/46/CE (UNIÃO EUROPEIA, 1995) e o Regulamento Geral de sobre Proteção de Dados (EU) 2016/679 (UNIÃO EUROPEIA, 2016) mostram dois objetivos relacionados com, respectivamente, "a proteção das pessoas físicas

[14]Todavia, a apresentação dos fundamentos dos textos europeus, em especial o Regulamento (EU) 2016/679, dá um lugar de destaque às razões econômicas, isto é, de construção de um mercado interno resultando em fluxo de dados, como pode ser visto no "considerando" (5), que cito: "A integração econômica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro" (UNIÃO EUROPEIA, 2016).

(singulares) no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados". Menos ambíguo é, de fato, o título da Diretiva 2002/58/CE, que menciona o "tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas", conhecida como "Diretiva relativa à privacidade e às comunicações eletrônicas".

No entanto, sobretudo sob a pressão dos grandes atores americanos, as teorias realistas tornaram-se poderosas. E assim se fizeram, com o consentimento da maioria dos cidadãos, deve-se notar, atraídos pela contrapartida proposta, na maioria das vezes de forma oculta: "deixem-nos tratar seus dados (abrindo mão de seu valor) e vocês terão acesso a serviços extraordinários (o que é verdade); na verdade, essa 'falsa' gratuidade esconde uma troca" (FARCHY, MÉADEL, SIRE, 2015)[15].

Quais são precisamente as conquistas nesse sentido? Vamos abordar apenas alguns dispositivos emblemáticos dos textos existentes para tentar identificar as garantias dadas a essa orientação.

A este respeito, encontramos em primeiro lugar, no Regulamento (UE) 2016/679, um esforço de fluidificação dos tratamentos de dados por meio de uma mudança radical do sistema em comparação com o sistema atualmente em vigor: não haverá mais a necessidade de notificação *a priori* do processamento de dados para a autoridade nacional de supervisão, nem do cumprimento de formalidades preliminares. Haverá apenas um controle *a posteriori* e um sistema de "conformidade" sob a responsabilidade do autor do tratamento dos dados[16].

Quanto ao fluxo de dados, em segundo lugar, é preciso destacar a questão crucial das transferências para países terceiros da União Europeia (a circulação é livre dentro da União). Trata-se, em particular, das transferências feitas para países com baixo custo de tratamento ou para os Estados Unidos da América. A questão é ainda mais crucial, hoje, e o acordo, ainda mais difícil de ser atingido, em razão da generalização da prática de guarda e tratamento em "nuvem" (*cloud computing*, ou seja, com o armazenamento de conteúdo digital fora de nossos computadores) e dos fluxos maciços de dados enviados para os Estados Unidos

[15]Para conferir uma denúncia dessa ocultação de objetivo (FRANÇA, 2014c).

[16]Confira trecho do "considerando" 89, do Regulamento 2016/679: "A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento" (UNIÃO EUROPEIA, 2016b).

para tratamento – que, em seguida, são transferidos para agências terceirizadas dessas empresas americanas, sempre fora da União Europeia.

No contexto do direito atual, retomado em grande parte pelo Regulamento (UE) 2016/679, as transferências para fora da União Europeia são, em princípio, proibidas. No entanto, existem exceções justificadas pela existência, no país terceiro destinatário dos dados, de um "nível de proteção adequado". A avaliação deste nível é realizada pela Comissão Europeia por meio de uma decisão tomada por uma autoridade de controle e direitos efetivos em benefício das pessoas[17]. Fora dessas hipóteses de um nível de proteção atestado, no entanto, a transferência pode também ocorrer se houver uma legitimação maior: seja pelo consentimento da pessoa interessada, seja pelo fato de ser necessária em razão de interesses superiores, nos termos do artigo 49 do Regulamento (UE) 2016/679, que detalha essas hipóteses.

Por fim, a transferência pode se sujeitar a um regime de autorização, regido por "regras empresariais vinculantes" (*Binding Corporate Rules*), que são uma espécie de código de conduta interna de empresas ou de grupos de empresas que visam garantir um nível de proteção adequado em todas as entidades, independentemente da sua localização, e que são submetidas à aprovação da autoridade nacional de controle, designada como *chef de file*, após verificação de condições estritas[18]. Pode-se também usar um acordo de transferência com cláusulas contratuais típicas, aprovadas pela Comissão Europeia, por uma autoridade nacional de controle, ou por meio de um contrato padronizado e supervisionado pela autoridade de controle[19].

Ora, uma das principais questões que surgiram das discussões sobre a adoção do Regulamento (UE) 2016/679 – e ainda continuam no âmbito do debate sobre o Tratado Transatlântico de Livre Comércio entre os Estados Unidos e a União Europeia – concerne precisamente ao destino destas transferências para fora da União. Com efeito, a Comissão Europeia excluiu os Estados Unidos da América do grupo de países que apresentam um "nível de proteção adequada", devido à ausência de uma lei federal geral que seja facilmente legível e exija uma proteção uniforme para todos os setores e os Estados daquela nação (MAXWELL, 2013).

No entanto, o acordo conhecido como *Safe Harbor*, assinado em 2000 entre a Comissão Europeia e os Estados Unidos da América, prevê que a União

[17]Confira o "considerando" 103 e o artigo 45º do Regulamento (UE) 2016/679. Tais disposições tratam do respeito ao Estado de Direito, garantias de acesso à justiça e do cumprimento de regras e de normas internacionais na área de direitos humanos, bem como uma legislação geral e setorial. Além disso, a verificação pela Comissão Europeia deve ser periódica, conforme o "considerando" 107.

[18]Confira o artigo 47 do Regulamento (UE) 2016/679 (UNIÃO EUROPEIA, 2016b).

[19]Veja o artigo 46 do Regulamento (UE) 2016/679 (UNIÃO EUROPEIA, 2016b) para essas outras possibilidades.

Europeia deva reconhecer os procedimentos norte-americanos para assegurar um nível de proteção adequado: cada ator adere ao acordo, faz uma auto-certificação junto ao Departamento de Comércio dos Estados Unidos da América e se compromete a respeitar e a aplicar os princípios fundamentais estabelecidos pela Diretiva 95/46/CE acerca dos dados pessoais transferidos por empresas localizadas no território europeu (cerca de 1.000 empresas participam do sistema, inclusive o Google e o Facebook) (UNIÃO EUROPEIA, 2000b).

Porém, tal procedimento tem recebido críticas de alguns países europeus e da própria Comissão Europeia: as regras seriam pouco vinculantes; e a auto-certificação e as obrigações seriam insuficientes (UNIÃO EUROPEIA, 2013). Assim, já haviam pedidos de intensificação dos controles e em prol de um alinhamento das obrigações endossadas com as definidas pela União Europeia (FRANÇA, 2014b: 24), mesmo antes que o Tribunal de Justiça da União Europeia questionasse totalmente o dispositivo em 6 de outubro de 2016. Com base nas revelações feitas por Edward Snowden, referentes às lacunas no tratamento de dados de cidadãos europeus pelos serviços de segurança dos Estados Unidos da América, o Tribunal de Justiça questionou a decisão de *Safe Harbor* e, com ela, as transferências de dados da União Europeia para os Estados Unidos (UNIÃO EUROPEIA, 2015). O Tribunal de Justiça mostrou, através dessa decisão, que as transferências de tais dados não devem ocorrer a um custo alto demais para os cidadãos europeus em termos de respeito à sua liberdade individual, razão pela qual demandou uma nova discussão das condições desse tráfego de dados[20].

Em terceiro lugar, a escolha de uma única opção, ou seja, a concessão de competência de controle para uma única autoridade nacional, chamada *chef de file*, que concentraria todos os pedidos contra um operador, desde que este tenha seu "estabelecimento principal" no território de um Estado-membro[21], pode parecer favorável aos responsáveis pelo processamento dos dados e à sua atividade. Com efeito, tal fato lhes daria flexibilidade para se posicionarem em um ambiente que considerem mais favorável aos seus interesses (o que representa um risco de *forum shopping*), ao menos no período em que as interpretações de um Regulamento sobre Proteção de Dados uniforme na União não estejam ainda estabilizadas. Como consequência, os níveis de proteção permanecerão divergentes nos diferentes Estados. De modo geral, seria de grande interesse aos operadores evitar se estabelecer, não apenas por razões fiscais – o que eles já

[20]Atualmente, essa circulação de dados ocorre com base em um novo acordo-quadro intitulado *Privacy Shield* ou Escudo de proteção da privacidade, publicado pela Comissão Europeia no dia 2 de fevereiro de 2016. Sobre este acordo-quadro (UNIÃO EUROPEIA, 2013).

[21]Confira o "considerando" 124 e o artigo 56 do Regulamento (UE) 2016/679. Note, entretanto, as nuances introduzidas e a recuperação necessária, sobretudo em caso de lotação de cidadãos europeus em outro país membro.

fazem, aliás – na França, na Alemanha ou na Espanha (onde as autoridades de supervisão são consideradas mais severas) e continuar a privilegiar a Irlanda, por exemplo[22]. Assim, a circulação de dados é sujeita a garantias asseguradas, que precisam ser equilibradas com a proteção da identidade digital, como indica uma leitura sistemática do texto do novo Regulamento.

A tese personalista: é possível proteger as pessoas por meio de seus dados pessoais?

Antes de tudo, vale lembrar que, do ponto de vista filosófico, usar termos como "bem", "propriedade" e "valor" significa dar pouca importância à textura dos dados e ao componente de identidade e personalidade de cada pessoa – por um lado – e ignorar – por outro lado – os riscos envolvidos, principalmente aqueles de manipulação de comportamentos possivelmente induzidos pelos vários tipos de tratamento de dados. Não defendemos apenas um bem ou um valor econômico ao proteger esses dados; mas também a proteção das pessoas na sua privacidade e na sua liberdade de agir, bem como seus componentes de identidade. No entanto, é preciso articular precisamente essa tese personalista e definir as suas implicações.

As várias teses personalistas

A concepção que considera os dados como pertencentes ao internauta dá mais ênfase à ligação entre os dados e as pessoas. E defende, também, a ideia de sustentar um regime em prol da proteção do indivíduo. Assim, os dados pessoais são elementos de personalidade de cada um; emanam dos indivíduos e revelam sua identidade e seus comportamentos, tal como tem elaborado o Tribunal Constitucional alemão desde 1983 (ALEMANHA, 1983). Trata-se, nesse caso, de defender o reconhecimento de um direito fundamental para a autodeterminação informativa, de forma que todos devam ter o controle inicial de todos os tratamentos relacionados aos seus dados e todos os tipos de coleta (POULLET & ROUVROY, 2009). Além disso, também, todos devem ser capazes de manter o controle sobre os seus usos, isto é, de poder administrá-los, ou seja, decidir sobre cópias, modificações, transferências e sobre os apagamentos, nos termos das soluções mencionadas por Pierre Bellanger (2014a; 2014b). Isso significa uma ação continuada durante todos os tratamentos – e, portanto –, aceitar as mudanças nas finalidades, por exemplo, uma questão importante no contexto do *Big Data*,

[22]Será preciso também acompanhar o destino dado à possibilidade, reconhecida no artigo 56 (2) do Regulamento (UE) 2016/679, de que: "(...) cada autoridade de controlo é competente para tratar reclamações que lhe sejam apresentadas ou a eventuais violações do presente regulamento se a matéria em apreço estiver relacionada apenas com um estabelecimento no seu Estado-Membro ou se afetar substancialmente titulares de dados apenas no seu Estado-Membro".

mas ainda de difícil implementação. Essa tese é também apoiada pelo Conselho de Estado, a mais relevante corte administrativa francesa, no seu relatório de 2014 (FRANÇA, 2014b: 267). Por fim, a mesma tese serve de base para alguns experimentos realizados no Reino Unido e na França visando a dar aos usuários o controle sobre seus dados junto aos operadores. A título ilustrativo, os dois projetos *Mydatas*[23] e *My Info*[24], criados em parceria com empresas detentoras de dados, oferecem dispositivos técnicos que permitem aos usuários não somente ficar a par dos tratamentos de seus dados, mas também lhes dá o poder de administrar os seus usos. A abordagem tem o mérito de ser ofensiva e positiva, uma vez que, ao devolver aos próprios interessados o controle sobre seus dados, abre novos campos de utilização, tanto na seara individual (submetê-los aos seus próprios tratamento e estabelecer correlações, por exemplo) quanto na coletiva (como decidir que eles servem para um estudo de saúde pública). Assim, não se trata apenas de uma abordagem defensiva[25] com o único propósito de proteção contra-ataques.

No entanto, existe a preocupação de que as implicações de uma visão personalista sejam muito drásticas e impeçam o funcionamento da economia digital atual. Com efeito, de acordo com os princípios legais franceses, a pessoa e o seu corpo são indisponíveis e não podem ser objeto de herança, nem de comércio legal (nem um valor, nem uma atribuição). Todavia, este obstáculo de princípio não deve impedir a evolução do conceito, pois o direitos pessoais já passaram e – ainda passam – por continuadas evoluções. E, ainda, os juristas sempre foram imersos em práticas de mercantilização e em debates relativos à qualificação dos elementos de personalidade (o nome de uma pessoa, sua voz, sua imagem, etc.) – por um lado – e de elementos e de produtos do corpo humano (órgãos, sangue, recursos biológicos de todos os tipos, etc.) – por outro lado. Como resultado, hoje é comum observarmos a "coisificação" da pessoa, mesmo que as respostas dadas pelo direito positivo permaneçam variáveis e não homogêneas com base nos elementos considerados. Como exemplos de tais elementos, citam-se aqueles constitutivos de personalidade (ou, pelo menos alguns deles, tais como a privacidade, o nome pessoal e a foto ou imagem) que passaram por um processo de patrimonialização, de modo que um indivíduo pode agora, mediante um contrato, conceder a terceiros o direito de usar seus dados, como reconheceu um julgado da Corte de Cassação francesa (FRANÇA, 2008).

[23]Projeto lançado pelo governo de David Cameron em 2011, determinando que as empresas compartilhem com seus clientes todas as informações pessoais de que dispõem sobre eles.
[24]Projeto conduzido pela FING – Fondation Internet Nouvelle Génération ("Fundação Internet Nova Geração". Veja o site: http://mesinfos.fing.org.
[25]Na mesma linha é o relatório do Conselho de Estado (FRANÇA, 2014b: 268).

Os elementos e os produtos do corpo humano são afetados por uma patrimonialização gradual, uma vez que, quanto mais processados e quanto mais diluída sua relação com a pessoa, mais fácil fica a sua circulação. Por exemplo, embora o sangue seja doado apenas depois de coletado, os medicamentos compostos por produtos sanguíneos, oriundos da sua transformação, podem ser transferidos a título oneroso entre profissionais, nos termos do Código de Saúde Pública francês (*Code de la santé publique*).

Esses movimentos de patrimonialização gradual nos parecem aplicáveis aos dados, no âmbito de uma abordagem personalista: quanto mais ligações tiverem os dados com a pessoa e mais ajudarem a revelar a sua identidade, mais deverão ser tratados na órbita da proteção jurídica da pessoa singular. Trata-se aqui da coleta inicial e dos usos que mantêm uma forte ligação com os usuários que estão na sua origem. Inversamente, quanto mais eles forem transformados e a ligação com a pessoa for sendo apagada, menos deverão ser tratados como um elemento de sua personalidade; trata-se aqui dos processamentos com anonimato irreversível, por exemplo, no qual o uso de dados ocorre sob a forma de estatísticas, desde que a irreversibilidade possa realmente existir, o que ninguém contesta[26]. Consequentemente, em termos de regime, a pessoa pode aceitar alguns episódios de patrimonialização de seus dados (desde que os termos de troca sejam claros, o que não é sempre o caso atualmente, isto é, de se permitir que o interessado saiba que, para se beneficiar de um serviço, deverá entregar seus dados em troca[27]), em condições mais ou menos exigentes.

Finalmente, deve-se integrar uma dimensão coletiva à abordagem personalista, sobretudo do ponto de vista substancial. Os dados de um indivíduo não carregam seus valores sozinhos, como vimos antes, mas figuram em várias redes com outros dados e estão sujeitos a tratamentos de acordo com fluxos incessantes. O consentimento de alguns afeta, assim, o tratamento dos dados de outros. É necessário também integrar essa dimensão coletiva do ponto de vista da eficácia: a exemplo de outras áreas de consumo de massa, é necessário que o grupo de pessoas possa contrariar o desequilíbrio de forças que opõe os usuários da Internet ou de objetos conectados – de um lado – e os responsáveis pelos tratamentos – de outro. Para muitos, alguns responsáveis pelos tratamentos conseguiram se tornar indispensáveis ao adquirir uma posição de monopólio ou de evidente domínio econômico. Porém, sabendo que essa necessidade foi adquirida, como seria possível integrar esta dimensão coletiva no futuro? Alguns

[26]Na mesma linha, o mencionado relatório do Conselho de Estado francês (FRANÇA, 2014b).
[27]Confira a mencionada recomendação da Comissão de Cláusulas Abusivas (FRANÇA, 2014c). Os textos relativos aos dados pessoais determinam a obrigação de lealdade de tratamento e a transparência, de modo que o responsável pela operação deve fornecer explicações sobre os tratamentos, as suas finalidades e a sua duração. No entanto, a lealdade e transparência em questão se aplicam especificamente às trocas feitas.

defendem sua organização através da criação de uma autoridade pública sobre o assunto, como Pierre Bellanger que postula a ideia da fixação de uma "agência de dados" com competência para garantir o exercício dos direitos individuais, bem como para se pronunciar sobre a legitimidade de usos de finalidade coletiva e, até mesmo, para fazer obrigar a aceitação de usos compartilhados de dados (BELLANGER, 2014a; BELLANGER, 2014b). Em razão do receio de "conluio" existente entre o mundo público e o mundo privado, que, aliás, sempre pode existir em matéria de espionagem, vê-se que haveria propensão à proposição de técnicas de representação coletiva em prol da proteção individual.

Não obstante a posição anterior, estamos de acordo com Antonio Casilli (2013) em apoiar um novo modelo de "*privacy* como negociação": é preciso poder negociar coletivamente com as principais operadoras os usos permitidos de dados. No mesmo sentido se manifesta Valérie Peugeot (2014). A mesma ideia ecoa do outro lado do Atlântico, onde Melanie Swan exorta os usuários norte-americanos a se tornarem sujeitos ativos: "Quando deixamos uma empresa apoderar-se dos nossos dados pessoais", diz ela, "(...) realizamos uma transação, entregamos uma matéria prima que tem valor; mas não temos nenhum poder de negociação, pois aceitamos as condições impostas pela indústria". E ela traça o mesmo caminho proposto por Antonio Casilli, que cito:

> "Acho que os internautas vão se unir e se organizar para defender seus interesses como fornecedores de dados. Para isso, eles buscarão inspiração nas associações de defesa de consumidores, ou até mesmo dos sindicatos. Somente uma resposta coletiva e solidária poderá restaurar o equilíbrio" (CASILLI, 2013).

Além disso, devemos promover ações coletivas. Não surpreendentemente, em nível individual, poucos internautas manifestaram interesse em ajuizar processos judiciais para defender esse material que eles geram (com exceção de Maximilian Schrems, estudante austríaco, advogado, que ajuizou vários processos contra o Facebook, dentre os quais alguns processos coletivos, e que está na origem de um famoso acórdão do Tribunal de Justiça da União Europeia, que determinou o bloqueio das transferências para os Estados Unidos) (UNIÃO EUROPEIA, 2015). O desincentivo decorre do fato de que os interesses em jogo nestas disputas judiciais são muito baixos para justificar os custos de um processo. Vale observar também que muitos órgãos de supervisão ganharam suas causas com recursos gratuitos e eficazes, a exemplo da *Commision Nacionale de l'Informatqiue et des Libertés* (Comissão Nacional de Informação e de Liberdades da França). É óbvio que o terreno é mais propício para os processos judiciais e administrativos coletivos; e menos atrativo para ações individuais.

Finalmente, para estabelecer uma política de proteção das pessoas através da proteção de seus dados, é necessário seguir três direções, todas capazes de

alimentar justamente a "autonomia da informação": o fortalecimento do poder de consentimento (e das informações subjacentes) com relação aos usos dos dados; o "empoderamento" técnico e jurídico das pessoas, isto é, o aumento do controle que elas têm sobre seus dados; e o desenvolvimento da representação e da ação coletiva, conforme já indicado em outra obra por Valérie-Laure Benabou e Judith Rochfeld (2015).

Manifestações positivas em apoio à tese personalista

No direito positivo europeu, mesmo que todos esses objetivos não sejam alcançados, existem muitos textos que apoiam essas tendências. Em relação à primeira direção, o Regulamento (UE) 2016/679 coloca em questão, em primeiro lugar, os grandes princípios da matéria: os dados devem ser tratados de forma legal, leal e transparente (com requisitos específicos de clareza e acessibilidade no que diz respeito à transparência[28]). Devem, ainda, ser tratados para determinadas finalidades, explícitas e legítimas, sem que venham a ser tratados posteriormente de modo incompatível com essas finalidades; devem ser respeitados os princípios da adequação e da minimização dos danos (o mínimo é tratado para servir à finalidade considerada durante o período apropriado), bem como sua exatidão, nos termos do art. 5º do Regulamento (UE) 2016/679 (UNIÃO EUROPEIA, 2016b). Além disso, as modalidades de informação das pessoas interessadas são especificadas nos mínimos detalhes, bem como as qualidades do seu consentimento – claro e demonstrável –, como indica o artigo 7º (1) do Regulamento:

> "(...) quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais (...)" (UNIÃO EUROPEIA, 2016b)[29].

[28]Conforme os detalhes do "considerando" 39 do Regulamento (UE) 2016/679 os detalhes constantes do constr. 39, Regulamento supracitado, segundo o qual "(...) o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples (...)". Ainda, o "considerando" 58 que faz alusão aos programas visuais, da seguinte forma: "(...) o princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado (...)". Aliás, essa menção do Regulamento é consentânea com as propostas de *Privacy Icons*, defendidas pelo *Conseil National du Numérique* (Conselho Nacional da Informação Digital francês) no parecer antes citado (FRANÇA, 2014a). Por fim, confira-se o "considerando" 166 do Regulamento sobre a implementação pela Comissão Europeia de "ícones normalizados" através de atos delegados (UNIÃO EUROPEIA, 2016b).

[29]No mesmo sentido está o "considerando 26" do Regulamento (UE) 2016/679, bem como o "considerando" 42 sobre a prova que deve constituir o responsável pelo tratamento para obtenção do consentimento e o "considerando" 43, acerca da situação de dependência da pessoa singular que a impede de consentir livremente (UNIÃO EUROPEIA, 2016b).

Finalmente, para citar apenas algumas ilustrações, os textos jurídicos em questão oferecem uma variedade de opções em função das várias finalidades possíveis do tratamento de dados e da eventual evolução desses objetivos. Por exemplo, em matéria de pesquisas científicas, o "considerando" 33 destaca que "(...) os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica (...)".

No entanto, e ainda sob a perspectiva personalista, é preciso lamentar o papel ambíguo deixado para o consentimento, que continua a ser uma mera fonte de legitimação do tratamento em meio a um conjunto de seis[30]: a existência de uma obrigação legal para o responsável pelo tratamento; a necessidade para o órgão de controle de salvaguardar a vida da pessoa interessada; a realização de um contrato no qual a pessoa em causa seja parte; a realização de uma missão de interesse geral; e, ainda, a problemática busca por "interesses legítimos do responsável pelo tratamento", prevista no artigo 6º, (1), "f" do Regulamento (UE) 2016/679, mesmo com a ressalva relacionada à proteção de interesse de menor (UNIÃO EUROPEIA, 2016b). Ora, não é legítimo que um operador comercial busque o seu interesse econômico por meio do tratamento de dados pessoais de seus usuários? De acordo com a interpretação dada a essa disposição – do artigo 6º – em particular o equilíbrio que ela prevê com "os interesses ou direitos e liberdades fundamentais do titular" –, a proteção poderá ser mais ou menos reforçada.

Quanto à segunda direção, relativa ao "empoderamento" de indivíduos, o Regulamento (UE) 2016/679 reforça e amplia a proteção de certos direitos, principalmente aqueles relativos à informação, ao acesso, à retificação, ao cancelamento e à objeção. Além da grande ênfase quanto a esses direitos, em caso de decisões tomadas com base na produção de perfis (*profiling*), o Regulamento (UE) 2016/679 prevê o fortalecimento do direito à comunicação de qualquer violação de dados, sobretudo no caso de modalidades concretas de exercício dos direitos dos titulares[31]. Ele também promove direitos inéditos, que asseguram maior controle da pessoa sobre seus dados, tal como o direito à portabilidade dos dados pessoais, nos termos do artigo 20º. Ainda, embora de um modo um pouco limitado, ele prevê o direito de excluir as referências digitais, nos termos do artigo 17º. Porém, esse direito somente pode ser exercido em casos de tratamento ilegal ou de retirada do consentimento, quando este representa a base do referido

[30]Apesar que o "considerando" 40 do Regulamento (UE) 2016/679 o apresenta como a principal causa de legitimação (UNIÃO EUROPEIA, 2016b).

[31]Para tanto, confira o Capítulo III do Regulamento supracitado (UE) 2016/679, no qual se destacam as "modalidades do exercício" de determinados direitos, em sintonia com o informado no "considerando" 59, aliás (UNIÃO EUROPEIA, 2016b).

tratamento ou, em caso de oposição da pessoa singular e quando os dados não são mais necessários)[32].

Para completar, deve-se enfatizar que a proteção da pessoa e seu controle crescente se desenvolveram também fora dos textos. Com efeito, tais características receberam um forte amparo do Tribunal de Justiça da União Europeia, com base no artigo 8º da Carta dos Direitos Fundamentais da União Europeia, e do seu artigo 7º (proteção da privacidade). Isso ocorreu a partir de duas decisões judiciais muito assertivas. A primeira de 8 de abril de 2014 ("Digital Rights Ireland Ltda contra Kärntner Landesregierung e outros") (UNIÃO EUROPEIA, 2014a) e a segunda, de 13 de maio de 2014 ("Google Spain e Google contra a Agência Espanhola de Proteção de Dados e outros") (UNIÃO EUROPEIA, 2014b). Com ambas, o Tribunal de Justiça determinou que um governo nacional – na primeira –, de um lado, e um operador privado – na segunda –, de outro, respeitem a proteção aos dados pessoais e à privacidade. Na primeira decisão, o Tribunal de Justiça da União Europeia invalidou uma Diretiva de 2006, adotada em meio à luta contra o terrorismo, que organizava a conservação dos dados pessoais para servir às políticas de segurança. Ele considerou que a conservação dos dados, na forma prevista era desproporcional e sinônimo de ingerência injustificada e excessiva. No segundo julgamento – que causou um rebuliço, pois foi visto como o reconhecimento do "direito ao esquecimento digital" –, o Tribunal de Justiça da União Europeia determinou que o Google assegurasse para cada internauta a possibilidade de remover os seus dados pessoais das listas de resultados do motor de pesquisa, uma vez que estas informações, embora exatas, poderiam parecer inadequadas.

Por sua vez, no âmbito do Conselho da Europa, o Tribunal Europeu de Direitos do Homem também não se omitiu. Apesar do artigo 8º da Convenção Europeia de Direitos do Homem, relativa à proteção da privacidade e da família, não fazer nenhuma menção aos dados de caráter pessoal – pois ele foi redigido bem antes do advento do advento desse conceito – essa jurisdição internacional incorporou a proteção destes elementos ao conceito de privacidade, como ficou notabilizado no caso "S. e Marper contra Reino Unido" (CONSELHO DA EUROPA, 2008), que concernia a questão de conservação de dados pessoais por uma duração ilimitada, no caso em relação a impressões digitais, perfis de DNA

[32]De acordo com o artigo 17º do Regulamento (UE) 2016/679, o exercício pode ocorrer, uma vez que o tratamento não seja necessário para "o exercício do direito à liberdade de expressão e informação"; "para cumprir com uma obrigação legal" ou "para realizar uma missão de interesse público ou exercício de um poder público de competência do responsável pelo tratamento"; "por razões de interesse público na área da saúde pública"; para fins de "arquivamento no interesse público, pesquisa científica ou histórica ou fins estatísticos"; ou, por fim, "para a constatação, exercício ou defesa de direitos na justiça" (UNIÃO EUROPEIA, 2016b).

e de amostras de células de pessoas que foram absolvidas ou cujos processos haviam terminado.

Por fim, no que diz respeito às representações e aos processos judiciais coletivos, observamos apenas algumas poucas premissas de evolução. Quanto à representação coletiva, em primeiro lugar, a regulamentação europeia não só incentiva o desenvolvimento de códigos de conduta para "famílias" de responsáveis pelo tratamento, mas também convida para uma discussão dos seus termos com os interessados, mas não exatamente com as associações que representam os seus interesses, nos termos dos "considerandos" 98 e 99 do Regulamento (EU) 2016/679. Quanto aos processos judiciais, em segundo lugar, se nós considerarmos apenas o caso da França, pode-se ressaltar que uma lei nacional sobre consumo, conhecida *Hamon*, de 17 de março de 2014, não permite processos judiciais, de forma geral. Ela apenas autoriza tais ações coletivas para proteção do consumidor em caso de danos materiais. No entanto, este termo resultará em ambiguidades significativas se for aplicado à violação de dados.

No âmbito europeu, ainda, podemos testemunhar um fortalecimento muito importante da aplicação de multas administrativas que as instâncias de controle poderão aplicar, nos termos do artigo 83º, parágrafos 4º, 5º e 6º do Regulamento (UE) 2016/679. Elas podem chegar até 20 milhões de euros ou 4% da % do total da receita global anual no exercício anterior. Como exemplo e em contraste, a *Commision Nacionale de l'Informatqiue et des Libertés* (Comissão Nacional de Informação e de Liberdades da França) podia apenas chegar até o valor máximo de 150.000 euros para uma primeira violação, sendo dobrado em caso de descumprimento e, logo, chegando ao limite de 300.000 euros.

Porém, por fim, cabe notar que o novo Regulamento europeu não prevê muitas oportunidades de processos judiciais coletivos, sendo apenas mencionados alguns casos no artigo 80º (UNIÃO EUROPEIA, 2016b). E, ainda assim, isso ocorre sob a alusão à possibilidade para que uma pessoa prejudicada possa delegar poderes por um mandato em prol de "um organismo, organização ou associação sem fins lucrativos", cujo objetivo estatutário seja concernente à proteção de dados pessoais, ou, ainda, outorgar tal poder para que, em determinados Estados-membros ou agências estatais possam agir em defesa de proteção de pessoas singulares, sem especificar se os resultados da ação seriam em benefício de uma comunidade de consumidores, por exemplo. Não obstante essa limitação na nova legislação europeia, cabe notar, por fim, que, por enquanto, os únicos processos coletivos ajuizados na Europa tiveram seus pedidos indeferidos. Um exemplo reside num processo judicial ajuizado em abril de 2015 perante o Tribunal Civil de Viena, no qual cada pessoa envolvida pediu uma indenização de 500 euros contra o Facebook sob a alegação de que o aplicativo faria um uso ilícito dos seus

dados e violaria a sua privacidade. O pedido da ação foi indeferido (REUTERS, 2015).

Referências Bibliográficas

ALEMANHA: Tribunal Constitucional, **Bverfge 65,1: Volksählung, 1983** (Acórdão constitucional 65,1: censo, 1983), 1983. Disponível em: http://www.servat.unibe.ch/dfr/bv065001.html. Acesso em: 07 nov. 2017.

AIGRAIN, Philippe. L'individu et la société à l'age numérique: entre capture et emancipation**O indivíduo e a sociedade na era digital**: entre captura e emancipação, palestra dada no Sindicato da Magistratura, 20-21 de set.embro de 2014, Lille, Disponível em: <http://paigrain.debatpublic.net/?p=8944>.

ARGENTON, Cédric. ; PRÜFER, Jens.., Search Engine Competition With with Network Externalities. Journal of Competition Law and Economics, v. 8, n. 1, p. 73-105. DOI: 10.1093/joclec/nhr018.Disponível em: <http://ideas.repec.org/p/dgr/kubtil/2011024.html>.

BABINET, Gilles. **L'ére numérique: um nouvel âge de l'humanité**. Paris: Le Passeur Éditeur, **A era digital:** uma nova idade da Humanidade. Le Passeur, 2014.

BELLANGER, Pierre. **La souveraineté numérique**. Paris: Stock, 2014a.

BELLANGER, Pierre. **Principes et pratiques des données personnelles em réseau**, 2014b. Disponível em: <http://pierrebellanger.skyrock.com/3231110655-Principes-et-pratiques-des-donnees-personnelles-en-reseau.html>. Acesso em: 07 out. 2017.

BENABOU, Valérie-Laure; ROCHFELD, Judith. **À qui profir le clic? Le partage la valeur à l'ère du numérique**. Paris: Odile Jacob, 2015.

CASILLI, Antonio. Contre l'hypothèse de la 'fin de l avie privée': la négociation de la 'privacy' dans les médias sociaux. Revue française des sciences de l'iformation et de la communication, n. 3, 2013. Disponível: <http://journals.openedition.org/rfsic/630>. Acesso em: 07 out. 2017.

CHEMLA, Laurent. Nous sommes tous des ayants droit ("Somos todos titulares de direito"). **Médiapart.** 23 out. 2013, Disponível em: <https://blogs.mediapart.fr/laurent-chemla/blog/231013/nous-sommes-tous-des-ayants-droit>. Acesso em: 07 out. 2017.

CONSELHO DA EUROPA: Tribunal Europeu de Direitos do Homem, **consultas 30562/04 e 30566/04**, acórdão de 4 de dezembro de 2008, S. e Marper contra Reino Unido. Disponível em: <http://actu.dalloz-etudiant.fr/fileadmin/actualites/pdfs/MAI_2013/AFFAIRE_S._ET_MARPER_c._ROYAUMEUNI.pdf>. Acesso em: 08 out. 2017.

DEBET, Anne; MASSOT; METTALINOS, Nathalie. **Informatique et libertés: la protection des données à caractere personnel em froit français et européen**. Paris:et al., **Informática e Liberdades**. Lextensio-éditions, 2015.

FARCHY, Joëlle; MÉADEL, Cécile; SIRE, Guillaume. **La gratuité, à quel prix? Circulation et échanges de biens culturels sur Internet**. Paris: Transvalor - Presses des Mines, 2015.

FONDATION INTERNET NOUVELLE GÉNÉRATION ("Fundação Internet Nova Geração") (FING), **MyInfo.** Disponível em: <Mesinfos.fing.org>. Acesso em: 07 outr. 2017.

FRANÇA. **Loi n. 1978-17**, 6 Janvier 1978, relative à l'informatique, aux fichiers et aux libertés modifiée – Loi Informatique et Libertés (Lei n. 1978-17, relativa à informática, aos arquivos e às liberdades – Lei para Informática e Liberdades, LIL). Paris: Journal Officiel de la République Française, 7 jan. 1978, p. 227-231 (Jornal Oficial da República Francesa). Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acesso em: 09 nov. 2017.

FRANÇA: Cour de Cassation (Corte de Cassação), **Arrêt n. de pourvoi 07-19494** ("acórdão de apelação"), Paris: Journal Officiel de la République Française, 11 dez. 2008 ("Jornal Oficial da República Francesa"). Disponível: https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000019922649&fastReqId=1791188556&fastPos=1. Acesso em: 7 out. 2017.

FRANÇA: Commision des Clauses Abusives. Recommandation n. 14-02 – Contrats de fourniture de services de réseaux sociaux, 7 nov. 2014. Disponível em: < http://www.clauses-abusives.fr/recommandation/contrats-de-fourniture-de-services-de-reseaux-sociaux-nouveau>. Acesso em: 7 out. 2017.

FRANÇA: Conseil National du Numérique. ("Parecer 2014-2 sobre a neutralidade das plataformas: reunir as condições de um ambiente digital aberto e sustentável"). 2014a. Disponível: https://cnnumerique.fr/files/2017-09/CNNum_Rapport_Neutralite_des_plateformes.pdf

FRANÇA: Conseil d'Etat. **Etude annuelle 2014 du Conseil d'Etat: le numérique et les droits fondamentaux** (Estudo anual 2014 do Conselho de Estado francês: o digital e os direitos fundamentais). Paris: La Documentation Française, 2014b. Disponível: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf. Acesso em: 11 dez. 2017.

KIM, Nancy S.; TELMAN, D. A. Internet giants as quasi-governmental actors and the limits of contractual consent. **Missouri Law Review**, v. 80, p. 723-770, 2015.

LE MONDE. http://www.lemonde.fr/a-la-une/article/2013/06/02/tres-cheres-donnees-personnelles_3422477_3208.html.

MAXWELL, Winston. **Accord de libre-échange transatlantique: pas sans la protection des données personnelles**, 22 abr. 2013. Edition Multimédi@. Disponível em:

http://www.editionmultimedia.fr/2013/04/22/accord-de-libre-echange-transatlantique-pas-sans-la-protection-des-donnees-personnelles. Acesso em: 8 out. 2017.

MERCIER, Silvère. Bien comuns et données personnelles: il nous faut inventer! Blog Bibliobsession, 12 mar. 2014. Disponível em: <http://www.bibliobsession.net/2014/03/12/biens-communs-et-donnees-personnelles-il-nous-faut-inventer/>. Acesso em: 07 out. 2017.

OBAMA, Barack; SWISHER, Kara. ***White House. - Red Chair - . Obama Meets Swisher***, 15 de fevereiro de 2015. Entrevista concedida a Recode. Disponível em: <https://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher>. Acesso em: 07 out. 2017.

PEUGEOT, Valérie. Données personnelles: sortir des injonctions contradictoires ("dados pessoais: abandonar as decisões contraditórias"), VECAM: Citoyenneté dans la societé numérique, Julho 13 abr. 2014. Disponível em: <https://vecam.org/Donnees-personnelles-sortir-des-injonctions-contradictoires>. Acesso em: 07 out. 2017.

POULLET, Yves; ROUVROY, Antoinette. Le droit à l'autodétermination informationelle et la valeur du dévelopment personnel: une réevaluation de l'importance de l avie privée pour la démocratie. In: BENYEKHLEF, Karim. (dir.); TRUDEL, Pierre P. (dir.)., **État de droit et virtualitéEstado de Direito e virtualidade**, . Montreal: Thémis, 2009, p. 157-222.

RALLET, Alain; ROCHELANDET, Fabrice; ZOLYNSKI, Célia. De la 'privacy by design' à la 'privacy by using'. **Réseaux**, v. 189, n. 1, p. 15-46, 2015.

ROSE, John; REHSE, Olaf; RÖBER, Björn. The value of our digital identity. BCG.perspectives, 20 nov. 2012. Disponível: https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity. Acesso em: 13 dez. 2017.

UNIÃO EUROPEIA: Parlamento Europeu e Conselho. **Directiva 95/46/CE**, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, 1995. Bruxelles: Jornal Oficial da União Europeia, de 23 nov. 1995, p. 31. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:01995L0046-20031120&from=EN. Acesso em 18 dez. 2017.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**, de 18 de dezembro de 2000a. Bruxelas: Jornal Oficial das Comunidades Europeias, 2000. Disponível: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 07 out. 2017.

UNIÃO EUROPEIA. Comissão Europeia, **Decisão da Comissão 520/2000/CE**, de 26 de julho de 2000, referente a Safe Harbor, 2000b. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2000.215.01.0004.01.POR&toc=OJ:L:2000:215:TOC>. Acesso em: 07 out. 2017.

UNIÃO EUROPEIA. Comissão Europeia, **Communication from the Commission to the European Parliament and the Council,** Rebuilding Trust in EU-US Data Flows, 27 de novembro de 2013, COM(2013) 846 final. Disponível em: <http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf>. Acesso em: 07 out. 2017.

UNIÃO EUROPEIA: Tribunal de Justiça da União Europeia, **Processo número C-293/12**, acórdão de 8 de abril de 2014. Digital Rights Ireland Ltda contra Kärntner Landesregierung e outros, 2014a. Disponível em: http://curia.europa.eu/juris/liste.jsf?num=C-293/12. Acesso em: 08 nov. 2017.

UNIÃO EUROPEIA: Tribunal de Justiça da União Europeia, **Processo número C-131/12**, acórdão de 13 de maio de 2014. Google Spain e Google contra a Agência Espanhola de Proteção de Dados (AEPD) e outros, 2014b. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pt.pdf. Acesso em: 08 nov. 2017.

UNIÃO EUROPEIA: Tribunal de Justiça da União Europeia, **Processo C-362/14**, acórdão de 6 de outubro de 2015, Maximillian Schrems contra Data Protection Commissioner, 2015. Disponível em: <http://curia.europa.eu/juris/liste.jsf?td=ALL&language=pt&jur=C,T,F&num=C-362/14#>. Acesso em: 8 nov. 2017.

UNIÃO EUROPEIA: European Data Protection Supervisor. **Opinion on the EU-U.S**. Privacy Shiel draft adequacy decision, 13 abr. 2016a, WP 238. Disponível em: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf>. Acesso em: 07 out. 2017.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,** de 27 de abril de 2016, referente à proteção de pessoas físicas contra o processamento de seus dados pessoais e livre circulação desses dados, revogando a diretiva 95/46/CE (regulamento geral sobre a proteção de dados). 2016b. Disponível em: <https://publications.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt>. Acesso em: 07 out. 2017.

WEISS, Leigh M.; CAPOZZI, Marla M.; PRUSAK, Laurence. Learning from the internet giants. **MIT Sloan Management Review**, v. 45, n. 4, p. 79-84, 2004.

REUTERS. Austrian student´s lawsuit vs. Facebook bogged down in procedure, 9 abr. 2015. Disponível: https://www.reuters.com/article/us-facebook-austria-lawsuit/austrian-students-lawsuit-vs-facebook-bogged-down-in-procedure-idUSKBN0N019420150409. Acesso em: 8 out. 2017.