A PROTEÇÃO DE DADOS PESSOAIS E SEUS DESAFIOS REGULATÓRIOS

THE PROTECTION OF PERSONAL DATA AND ITS REGULATORY CHALLENGES

Mayara Rocumback Vieira da Silva[*]

Resumo:
Na atual sociedade da informação, ferramentas poderosas de tratamento de dados pessoais foram criadas, por meio das inovações tecnológicas, dominadas por interesses mercadológicos e pela lógica de coletar volumes exponenciais de dados. Tal cenário coloca em risco a proteção de dados pessoais, observado o descompasso entre a sofisticação do processamento de dados e as técnicas e instrumentos que visam a resguardar os interesses de seus titulares. Nesse contexto, este artigo tem por objetivo discutir algumas limitações da autodeterminação informacional e quais são as possíveis alternativas ou complementações a esse modelo. Para isso, foi abordada, sinteticamente, a estrutura do mercado de dados pessoais, elencando-se alguns modos de coleta de dados e riscos decorrentes de violação à privacidade. Em seguida, discutiu-se a relação entre privacidade e proteção de dados pessoais e como essa é prevista pelo ordenamento jurídico brasileiro, em especial, pela Lei n. 13.709/2018. Foram analisados também os aspectos relacionados à chamada crise do consentimento. Por fim, foi examinado como a regulação de risco é importante para a proteção de dados pessoais, em uma dimensão coletiva. Assim, concluiu-se que o consentimento como modo de legitimar a proteção de dados pessoais está sendo usado para além de suas capacidades e que, embora a Lei n. 13.709/2018 represente um avanço no tema, é necessário pensar como ela será interpretada e implementada. Diante disso, a visão da privacidade, por meio do caráter coletivo, integrando-se normas, como a Lei n. 13.709/2018, com propostas de responsabilidade demonstrável das empresas e privacidade "by design", é essencial para a proteção de dados pessoais.

Palavras-chave: Dados pessoais. Autodeterminação informacional. Consentimento. Regulação de risco. Processamento de dados.

Abstract:

In today's information society, powerful personal data processing tools have been created through technological innovations, dominated by market interests and the logic of collecting exponential volumes of data. This scenario puts the protection of personal data at risk, due to the mismatch between the sophistication of data processing and the techniques and instruments intended to protect the interests of its owners. In this context, this article aims to discuss some limitations of informational self-determination and what are possible alternatives or complements to this model. For this purpose, the structure of the personal data market was briefly analyzed, by listing some means of collecting data and risks arising from privacy violation. Next, it was discussed the relationship between privacy and protection of personal data and how this latter is foreseen by the Brazilian legal system, in particular,

[*] Graduanda em Direito pela Universidade de São Paulo. E-mail para contato: mayara.rocumback.silva@usp.br.

by Law 13,709/2018. The aspects related to the so-called consent crisis were also analyzed. Finally, it was examined how risk regulation is important for the protection of personal data, in a collective dimension. Finally, it was concluded that consent as a way to legitimize the protection of personal data is being used beyond its capabilities and, although Law 13,709/2018 represents a progress on the topic, it is necessary to think how it will be interpreted and implemented. Considering this, the vision of privacy, through its collective character, integrating standards, such as Law 13,709/2018, with proposals of demonstrable corporate responsibility and privacy "by design" is essential for the protection of personal data.

Keywords: Personal Data. Informational self-management. Consent. Risk Regulation. Data Processing.

1. Introdução

A proteção de dados pessoais tem ganhado cada vez mais importância, no contexto de uma sociedade da informação, marcada por uma forma de organização dependente de informações, que circulam em grande volume e velocidade. Diante dos avanços tecnológicos e do surgimento de potentes ferramentas para a captação, processamento e comercialização, em massa, de dados pessoais, as ofensas à privacidade multiplicaram-se, já que há uma crescente transformação do próprio cotidiano dos indivíduos em dados. As mudanças propiciadas pelas tecnologias de informação refletiram no próprio conceito de privacidade, que há muito tempo deixou de ser "o direito de estar só" (BRANDEIS; WARREN, 1890, p. 193-194) e passou a abranger o direito de manter o controle das próprias informações (RODOTÀ, 2008, p. 92).

Nesse cenário, o ordenamento jurídico não foi capaz de assegurar a tutela jurídica da personalidade humana e dar soluções jurídicas eficientes a essas violações no mesmo ritmo em que ocorreram essas mudanças e aprimoraram-se os mecanismos de inteligência artificial e de Big Data. O modelo da autodeterminação informacional, que ganhou força, nas décadas finais do século XX, na Europa, como uma reação ao incremento de ferramentas de armazenamento e cruzamento de dados, pautou-se na ideia de que o indivíduo seria capaz de autodeterminar suas informações por meio do consentimento, ou seja, emitindo autorizações para o uso de seus dados. Contudo, atualmente, ele tem sido friccionado pelo mercado de dados pessoais e pela arquitetura da internet (BIONI, 2016, p. 17-21).

Assim, discute-se aqui os principais desafios e limitações da autodeterminação informacional, nos dias de hoje, e quais são as possíveis alternativas ou modelos teóricos complementares a ela. Esse artigo pretende abarcar essas questões, analisando, inicialmente, como se estrutura o mercado de dados pessoais, de maneira geral, indicando algumas decorrentes violações à privacidade, que podem ser agrupadas, em uma taxonomia (SOLOVE, 2006). Em seguida, abordou-se a relação entre privacidade

e proteção de dados pessoais e como essa última está presente no ordenamento jurídico brasileiro, com destaque à nova Lei n. 13.709/2018. Além disso, também foram analisados os limites do modelo teórico de autodeterminação informacional nessa proteção dos dados, principalmente, no tocante aos problemas relacionados ao consentimento como modo de legitimar o tratamento de dados. Por fim, foi aprofundado o estudo da dimensão coletiva da privacidade como forma de complementar o modelo da autodeterminação informacional na proteção de dados pessoais, em especial, por meio da regulação de risco, apontando as principais dificuldades que envolvem essas propostas.

2. O mercado de dados pessoais e as violações à privacidade

"Os dados dos clientes estão sendo transformados em armamentos de guerra com eficiência militar", afirmou o presidente executivo da Apple, Tim Cook, em uma Conferência Internacional de Proteção de Dados e Comissários de Privacidade, em Bruxelas, na Bélgica. Segundo ele, informações do dia a dia e de cunho estritamente pessoal dos indivíduos estão sendo transformadas em dados, que são montados, agrupados e vendidos, alimentando um comércio que explodiu em um complexo industrial de dados (CHEE, 2018).

Essa declaração reforça a ideia de que se vive em um contexto de "datificação" da vida, marcado pela transformação de elementos do cotidiano em dados. Tal cenário tem como pano de fundo a ideia de sociedade da informação, que remete a uma organização social, política e econômica relacionada ao uso das tecnologias em prol da produção, coleta, processamento, transmissão e armazenamento de informações (VIEIRA, 2007, p. 156), o que tem reflexos nos setores do mercado e na própria cultura, cada vez mais dominada por meios de comunicação e informação. Essa formação social é impulsionada pela internet, que pode ser caracterizada como um ambiente de vigilância, no qual o crescente número de pontos de contato entre o mundo físico e virtual faz com que os sistemas eletrônicos produzam grande fluxo de dados pessoais, fruto da observação da atividade humana e que podem ser reconstruídos, conforme a demanda (MENEZES NETO; MORAIS; BEZERRA, 2017, p. 187). Soma-se a isso o fato de que, desde a década de 1980 até os dias atuais, houve um barateamento do custo de armazenamento e processamento de dados, o que contribuiu para um aumento massivo no volume de dados gerados e disponibilizados.

A propósito, o "Big Data" pode ser definido como o crescimento, disponibilidade e o uso exponencial de informações estruturadas (objetivamente coletadas e dirigidas a bancos de dados específicos) ou não estruturadas (como as captadas pela análise de rastros digitais, que transitam pela internet), no campo da liberdade de expressão (SIMÃO FILHO; SCHWARTZ, 2016, p. 315). Desse modo, ele é um conjunto

de dados caracterizado por três "V"s: volumetria, variedade e velocidade de atualização, cuja base para o tratamento de dados é a inteligência artificial, com modelos de análise compostos por algoritmos e técnicas de *machine learning,* que tem capacidade preditiva, associada à identificação de padrões a partir de conjuntos de dados e a decorrente previsão de resultados e tendências futuros (LEAL, 2018, p. 18).

Percebe-se que os princípios do Big Data, que orientam a coleta e cruzamento do maior volume de dados possíveis, contrastam-se com os da proteção de dados pessoais, cuja premissa é limitar o quantum de dados captados e ligar essa coleta a uma finalidade específica, sendo que a difícil tarefa de como conciliar essas duas lógicas ainda permanece em aberto (BOEHME-NßBLER, 2016, p. 222-224).

Além disso, os indivíduos, por diversas vezes, desfrutam das facilidades propiciadas pelo fenômeno do Big Data e pelas inovações tecnológicas, mas não percebem os diversos riscos envolvendo a proteção de dados pessoais. Um caso que ilustra essa situação é o da "Data Dollar Store", que foi uma loja aberta por dois dias, no centro de Londres, onde só se poderia pagar por camisetas, canecas e outros bens por meio de informações, uma moeda denominada "dólar de dados", criada pela Kaspersky. Os produtos eram trocados por conversas no WhatsApp e imagens a serem exibidas nas telas das lojas por dois dias. A proposta visava a conscientizar as pessoas sobre o valor de seus dados, já que, muitas vezes, elas não refletem que, ao aceitar rapidamente um termo de uso de privacidade, em troca de serviços gratuitos, consentem com a coleta de seus dados, que serão inseridos, posteriormente, em um mercado de dados pessoais.

Esse mercado é orientado pela lógica de coletar e conectar a máxima quantidade possível de dados para gerar informações relevantes para as grandes empresas, que comercializam e compartilham bancos de dados. É possível dividi-lo entre 4 camadas, que se articulam e podem até se sobrepor entre si: *i*. coleta e armazenamento de dados; *ii*. processamento e mineração de dados; *iii*. análise e formação de amostras; *iv*. modulação (SOUZA; AVELINO; SILVEIRA, 2016, p. 223).

A captação de dados pessoais, na internet, pode acontecer de diversas formas, tais como as transações comerciais por meio das quais as empresas obtêm dados cadastrais dos consumidores, no momento da compra do produto ou realização de serviços; pesquisas de mercado e de estilo de vida; sorteios e concursos e, por fim, *cookies* e *spywares*, capazes de rastrear a navegação dos usuários, sendo que por intermédio dos *cookies* as preocupações dos usuários podem ser transformadas em sequências de códigos e salvas no disco rígido do computador (MENDES, 2014, p. 101-106).

O processamento de dados pessoais, por sua vez, é caracterizado pelo uso, armazenamento e manipulação desses dados, que envolvem meios de conectá-los e identificá-los aos seus titulares. Assim como a prática de mineração, ele está atrelado ao tratamento e à reunião dos dados coletados e armazenados para que se possa traçar,

detalhadamente, um perfil virtual dos indivíduos, o que, muitas vezes, é feito pelos data brokers, empresas que coletam dados pessoais dos consumidores e vendem para outras organizações (SOUZA; AVELINO; SILVEIRA, 2016, p. 224).

Dentre as práticas de tratamento de dados, estão: *i*. o "Data Warehousing", relativo à tomada de decisões estratégicas, a partir da transformação e armazenamento de uma base de dados, indicando se um fator será ou não determinante para uma ação de marketing, por exemplo; *ii*. o "Data Mining" ou mineração de dados, que é uma ferramenta para descobrir padrões significativos de informações a partir de um banco de dados, produzindo uma classificação de pessoas e objetos, o que corre o risco de ser discriminatório e violar o princípio fundamental da igualdade; *iii*. *profiling* ou construção de perfil, referente à construção de uma imagem abrangente e detalhada da personalidade de cada pessoa por meio de seus dados, com o intuito de prever padrões de comportamento, gostos, hábitos e preferência de consumo, o que possibilita a tomada de decisão sobre consumidores, trabalhadores e cidadãos, além de permitir que se molde a vontade de consumo de muitas pessoas, etc. (MENDES, 2014, p. 113-116).

Já os departamentos de marketing, que compõem a terceira camada do mercado de dados pessoais, são responsáveis por traçar estratégias com o auxílio de empresas especializadas em analisar e interpretar dados, organizando públicos segmentados, com o intuito de transformar internautas em clientes por meio de campanhas publicitárias. Por fim, na modulação, há a oferta de produtos e serviços a determinados públicos específicos, por exemplo, a partir das estratégias elaboradas na camada anterior (SOUZA; AVELINO; SILVEIRA, 2016, p. 224).

Ressalta-se que a comercialização de dados pessoais tem impactos até mesmo concorrenciais, como pode ser ilustrada pelo caso da condenação da Google, pela Comissão Europeia, no valor de 4,34 bilhões de reais, em julho de 2018, devido a violações de regras *antitrust* da União Europeia. Dentre as práticas ilícitas estava uma estratégia da empresa que resultou no impedimento dos motores de pesquisas rivais recolherem dados, como os relativos à pesquisa e à localização dos telemóveis, a partir de dispositivos móveis inteligentes, o que ajudou a Google a consolidar sua posição dominante, no mercado, como motor de pesquisa (COMISSÃO EUROPEIA, 2018, p. 3-5).

Em outra perspectiva, percebe-se que, para lidar com as novas modalidades de violação à privacidade, na internet, Solove propôs uma compreensão desse direito, de forma plural ampla e genérica, como um ponto de cruzamento de problemas muitos distintos entre si (LEONARDI, 2011, p. 89). Nessa linha, o autor elaborou uma taxonomia da privacidade, apresentando 4 grupos de atividades danosas a esse direito: *i*. coleta de informações; *ii*. processamento de informações; *iii*. disseminação de informações; e *iv*. invasão, que pode se dar na forma de incursão, na vida de alguém ou de incursão

indesejada, feita pelo governo, nas decisões do indivíduo, sobre sua vida (SOLOVE, 2006, p. 504-505, 549 e 555).

Analisando o instrumento da coleta de dados, muito presente no mercado de dados pessoais, Solove destaca o problema da vigilância, que é exacerbado com a revolução tecnológica, devido ao desenvolvimento de novos instrumentos de monitoramento, controle a distância e rastreamento, dentre os quais estão a videovigilância, o rastreamento via satélite de usuários de celular, além do controle da navegação e transações dos usuários no meio virtual, do envio de e-mails, visualização de vídeos e imagens e interações nas redes sociais. Esse fenômeno é prejudicial porque pode deixar os indivíduos desconfortáveis e inquietos, alterando seu comportamento (SOLOVE, 2006, p. 495).

No tocante ao processamento de dados pessoais, um de seus mecanismos mais polêmicos é a agregação, que consiste na reunião de pequenos pedaços de dados, formando um retrato do indivíduo (SOLOVE, 2006, p. 506-507). O escopo e o poder dessa ferramenta aumentaram muito, na sociedade da informação, observado o incremento da sofisticação dos instrumentos de processamento e a facilidade de combinação de dados.

Esse desenvolvimento tem um lado benéfico, pois pode ajudar o consumidor a encontrar produtos de seu interesse, por conta da publicidade direcionada, por exemplo. Contudo, ele também apresenta efeitos prejudiciais, como a perturbação das expectativas dos titulares de dados, quanto à divulgação de suas informações. Isso ocorre porque, ao fornecer pequenas informações próprias, em contextos específicos, nas suas atividades diárias, as pessoas esperam que haja limites sobre o que é sabido delas, a partir do que foi divulgado. A agregação, todavia, contraria essas expectativas, pois pode revelar novos fatos sobre alguém, que eram, a princípio, desconhecidos, o que é propulsionado pelo uso secundário desses dados, ou seja, a utilização para propósitos diferentes dos que foram consentidos pelo seu titular (SOLOVE, 2006, p. 506-507, 519-520). Dessa maneira, esse fenômeno pode aumentar o poder que um indivíduo tem sobre outro, já que "dossiês", muitas vezes, reveladores e incompletos, de informação digital sobre uma pessoa podem ser usados para julgá-la, em diversas situações, como na decisão de um fornecimento de empréstimo, por exemplo (SOLOVE, 2006, p. 507-508).

Outro problema relacionado ao processamento de dados é a insegurança, atrelada ao risco de vazamento de dados, que causa danos aos seus titulares, que podem ter suas informações divulgadas e até mesmo distorcidas (SOLOVE, 2006, p. 515-516), além da exclusão, referente à falha em fornecer avisos aos usuários sobre o registro de dados sobre eles, criando incerteza e vulnerabilidade aos indivíduos (SOLOVE, 2006, p. 521).

Embora a organização proposta por Solove auxilie na identificação dos potenciais danos à privacidade dos indivíduos, ela tem enfoque pragmático voltado à solução de problemas práticos, concebido por um sistema de Common Law e não gera um

sistema normativo, referenciado na tutela da dignidade da pessoa humana (LEONARDI, 2011, p. 88-89).

Diante disso, Erick Peixoto e Marcos Ehrhardt discordam desta taxonomia, pois tal sistematização não considera a teoria tridimensional da privacidade, pautada na ideia de que "quando se diz que um indivíduo sofreu uma violação da privacidade, na verdade, o que se está querendo dizer é que ocorrem várias violações, em vários direitos da personalidade e até em dimensões diferentes desta" (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 53). Para os autores, existem 3 dimensões da privacidade: espacial, decisional e informacional. A primeira dimensão remete ao controle de acesso a algo físico, como a proteção contra a entrada, no local onde outrem habita, por exemplo. Já a segunda se liga às decisões, ações e aos modos de vida dos indivíduos e se relaciona com a proteção de dados pessoais, na medida em que vários aspectos do modo de viver das pessoas acabam virando dados e, muitas vezes, dados sensíveis, o que traz muitas preocupações (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 51). Todavia, a proteção de dados pessoais está, principalmente, relacionada com a terceira dimensão da privacidade, a informacional, que se liga ao resguardo de dados e informações que digam respeito aos indivíduos, em relação ao mau uso e aos abusos da utilização de dados pessoais (ARTESE, 2017, p. 2).

É possível dizer que a informação pessoal e a privacidade se relacionam por uma equação simples, na qual o maior grau de privacidade se associa à menor difusão de dados pessoais e vice-versa, sendo que a proteção de dados pessoais é um desdobramento da privacidade (DONEDA, 2011, p. 94).

3. A proteção de dados pessoais e o paradigma da autodeterminação informacional

3.1. A qualificação jurídica dos dados pessoais e sua proteção no ordenamento jurídico brasileiro

A proteção de dados pessoais remete ao "conjunto de regras que visam impedir o tratamento inadequado, injusto ou antiético de dados pessoais" (ARTESE, 2017, p. 2). Esse assunto vem ganhando cada vez mais destaque, no Brasil, em especial, por conta da aprovação da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), em 14 de agosto de 2018, com período de *vacatio legis* de 24 meses, segundo a Medida Provisória n. 869/2018. Essa lei demonstra um avanço brasileiro em relação a esse tema, pois prevê um rol taxativo de hipóteses de tratamento legal de dados pessoais, dentre as quais está o consentimento do seu titular. Além disso, são previstos diversos direitos dos usuários, princípios de proteção de dados, responsabilidades dos agentes envolvidos no processamento desses dados e sanções em caso de descumprimento de normas.

Assim, é importante compreender como os dados pessoais podem ser qualificados juridicamente. Nessa linha, parece mais adequado, no campo da proteção

desses dados, adotar uma teoria personalista, que os compreende como componente da identidade e personalidade das pessoas e não só como um elemento de valor, passível de ser apropriado (isto é, de ser objeto de propriedade), bem como coletado e comercializado, ainda que sob certas limitações (ROCHEFELD, 2018, p. 66 e 73), que é o entendimento da teoria realista.

Contudo, existe uma preocupação de que os desdobramentos de uma visão personalista sejam muito drásticos para o funcionamento atual da economia (ROCHEFELD, 2018, p. 74). Diante disso, é possível aplicar a ideia de patrimonialização gradativa à proteção de dados pessoais, criando uma gradação entre os dados para determinar quando as pessoas podem aceitar a patrimonialização de seus dados e sob quais condições (mais ou menos exigentes), de modo que "quanto mais ligações tiverem os dados com a pessoa e mais ajudarem a revelar sua identidade, mais deverão ser tratados na órbita da proteção jurídica da pessoa singular". (ROCHEFELD, 2018, p. 74-75).

Adotando-se uma visão dos dados pessoais como extensão da personalidade, é possível dizer que o uso e o processamento desses dados por grandes empresas comprometem o próprio desenvolvimento da personalidade do indivíduo, prejudicado também pelo enfraquecimento das fronteiras entre público e privado no mundo virtual. Isso reduz o poder de controle dos indivíduos sobre os dados no que lhes dizem respeito, o que compromete seu direito de autodeterminação, relacionado à construção de um espaço reservado, em que a pessoa pode explorar seu íntimo, sem que tema uma reprimenda externa, além de desvencilhar-se das máscaras impostas pela sociedade (VIEIRA, 2007, p. 20).

Vale ressaltar que a proteção de dados pessoais é uma dimensão da privacidade, que é um direito de personalidade, assegurado pelo art. 5º, X da Constituição Federal, além dos arts. 11 e 21 do Código Civil, dentre outros dispositivos, como o art. 1º, III da CF/1988, que assegura o direito à dignidade da pessoa humana. Além disso, a tutela da personalidade não se trata de um único direito subjetivo ou de classificar diversos direitos da personalidade, mas de salvaguardar, em qualquer momento da atividade econômica, a pessoa humana (TEPEDINO, 2004, p. 23). Essa tutela deve ser considerada, em observância à Constituição, não como um reduto do poder do indivíduo, no âmbito do qual seria exercido a sua titularidade, mas como valor máximo do ordenamento, capaz de submeter a atividades econômicas a novos parâmetros de validade e de modelar a autonomia privada (TEPEDINO, 2004, p. 23).

Dessa forma, o art. 11 do CC/2002, em uma abordagem paternalista, previu que os direitos da personalidade são irrenunciáveis e intransmissíveis, o que permite apenas limitações voluntárias destes direitos, desde que não sejam permanentes nem gerais, observado o enunciado n. 4 aprovado na I Jornada de Direito Civil. (BRASIL, 2012). Na perspectiva da proteção de dados pessoais, deve-se refletir, então, sobre como

parametrizar os limites dessa autonomia relativa (BIONI, 2019, p. 220), o que será discutido no subcapítulo seguinte.

A proteção de dados pessoais é também assegurada por outros dispositivos constitucionais e legislativos. Nesse passo, o art. 5º, XII da CF/1988 garante o direito à confidencialidade e à segurança dos dados pessoais. Já o *habeas data,* previsto no art. 5º, LXXII da Constituição Federal representa um remédio contra usos abusivos de dados coletados de modo fraudulento e a conservação de dados falsos ou com fins diferentes daqueles autorizados pela lei, entre outras situações. Ele abrange, assim, o direito de acesso, de retificação e de complementação em relação aos dados pessoais. Contudo, o *habeas data,* juntamente com o direito dos indivíduos receberem informações de interesse particular ou coletivo, no prazo legal (art. 5º, XXXIII, CF/88) oferecem uma proteção genérica para os dados pessoais, que, devido à complexidade das técnicas de coleta e processamento de dados, mostra-se insuficiente.

Diante disso, os direitos dos usuários (como o da confirmação da existência de tratamento; acesso; correção de dados completos, inexatos ou desatualizados; anonimização e eliminação de dados desnecessários; portabilidade dos dados a outro fornecedor e revogação do consentimento, previstos no art. 18 da Lei n. 13.709/2018), em conjunto com os princípios da proteção de dados pessoais proverão ferramentas mais específicas para a tutela desses dados.

Ademais, há um eminente ponto de interconexão entre a proteção do consumidor e dos dados pessoais. Isso ocorre porque o tratamento de dados, capaz de ensejar violações à privacidade, acontece, por diversas vezes, entre empresas, prestadores de serviços de conexão e de conteúdo e outros agentes considerados fornecedores pelo art. 3º do Código de Defesa do Consumidor, e indivíduos que podem ser enquadrados como consumidores nos termos do art. 2º do CDC. Desse modo, o Marco Civil da Internet (Lei n. 12.965/2014) e a própria Lei n. 8.078/90, em especial no seu art. 43, que trata dos bancos de dados e cadastros de consumidores, podem ser consideradas leis que protegem os dados pessoais em relações de consumo, que devem ser aplicadas em conjunto com a Lei n. 13.709/2018.

Vale ressaltar que, dentre os princípios que norteiam a proteção do consumidor, está o da igualdade, de maneira que este se atrela a um ideário contrário à discriminação, ou seja, as características pessoais dos indivíduos, expressadas por seus dados, por exemplo, não podem ser usadas para lhes negar oportunidades e acesso a recursos sociais. Dessa forma, há uma relação delicada entre esse princípio e o mecanismo de tomada de decisões automatizadas, por meio de ferramentas de inteligência artificial, como a classificação de risco dos clientes para concessão de crédito. Para aprofundar esse tema, é importante compreender o que é um dado pessoal, cujo conceito relacionado

à ideia de identificabilidade e como ela é insuficiente para assegurar a proteção dos indivíduos contra a discriminação.

3.2. O conceito de dado pessoal, os dados sensíveis e o processo de anonimização

A definição de dados pessoais é um conceito-chave para a proteção, pautada no grau de identificabilidade do dado, pois, em regra, se ele não é identificável, não há dano à privacidade (SCHWARTZ; SOLOVE, 2011, p. 1.814). É possível dividir as informações em um espectro com 3 tipos, definidos em termos de padrões, por não terem limites rígidos: *i*. informações de pessoas identificadas, cuja identificação já pode ser verificada; *ii*. de pessoas identificáveis, com risco leve a moderado de identificação, no futuro; *iii*. de pessoas não identificadas, que tem risco remoto de identificação (SCHWARTZ; SOLOVE, 2011, p. 1.877-1.878). Semelhante à abordagem europeia, a Lei n. 13.709/2018 define os dados pessoais como: "informação relacionada a pessoa natural identificada ou identificável" (Art. 5º, I, da referida Lei). Ilustrando-se o conceito de dados pessoais, portanto, tem-se que ele pode se referir a identificadores únicos das pessoas, como CPF, CNH ou eletrônicos como e-mail e *cookies*, por exemplo.

Considerando que os ataques virtuais podem levar a descobertas de outros dados a partir dos que são disponibilizados em estatísticas, testes, pesquisas, dentre outras situações, são necessárias técnicas de preservação de dados pessoais. Desse modo, há três mecanismos que podem ser usados para esse fim: a criptografia (uso de algoritmo para "embaralhar matematicamente dados sensíveis", gerando substitutos ilegíveis), tokenização (geração aleatória de um valor de *token* sem formatação específica a partir de um registro original e armazenamento do mapeamento desse *token* com seu respectivo valor original em uma base de dados) e a anonimização (constituída por um "conjunto de técnicas que modificam dados originais, de tal forma que os dados anonimizados não se assemelham aos dados originais, mas ambos possuem semântica e sintaxe bastante semelhantes") (BRITO; MACHADO, 2017, p. 96-99).

Nessa linha, o processo de anonimização, que também pode ser entendido como "a retirada do vínculo da informação com a pessoa a qual se refere", dá origem ao dado anônimo (aquele que se refere a uma pessoa indeterminada), o qual tem diversas utilidades, como revelar informações sobre uma coletividade ou grupo específico sem que as pessoas a quem os dados se referem sejam nominadas (DONEDA, 2006, p. 157-158).

Para eliminar, em tese, a identificabilidade de um dado, pode-se suprimir o CPF do titular, generalizar o nome completo, fazendo constar apenas o prenome do indivíduo, generalizar a idade (indicar apenas a faixa etária das pessoas e não a idade exata), etc. (BIONI, 2015, p. 19-20). Todavia, existem cada vez mais estudos que comprovam a falibilidade do processo de anonimização, de modo que "sempre existirá a possibilidade de

uma base de dados anonimizada ser agregada a outra para a sua reidentificação", levando a um cenário antagônico à promessa semântica de dado anônimo (BIONI, 2015, p. 22-23).

Além disso, algumas informações identificáveis, contudo, devem ser tratadas como de uma pessoa identificada, visto que há um risco substancial de futura identificação do indivíduo. Essa condição é determinada a partir de um teste contextual que envolve uma avaliação dos meios que, provavelmente, serão utilizados pelas partes que têm ou terão acesso à informação, bem como das informações adicionais que poderão ser agregadas a ela (SCHWARTZ; SOLOVE, 2011, p. 1.877). De maneira similar, o critério utilizado para determinar se um dado é anônimo ou não, considerando a possibilidade de reversão é "um risco aceitável em torno da reversibilidade do processo de anonimização, a fim de que os dados anonimizados estejam fora do conceito de dados pessoais" (BIONI, 2015, p. 25-26), entendimento que é adotado pelo art. 12, *caput*, da Lei n. 13.709/2018.

É muito importante compreender que, por conta do fenômeno da agregação ou devido a ataques virtuais, as pessoas podem optar por não divulgar certas informações, como orientação ideológica ou idade, classificadas como sensíveis, mas esses dados serem previstos, a partir de um senso estatístico de outros aspectos de sua vida que ela revelou. Para entender a gravidade desse cenário, deve-se pontuar que os dados sensíveis são aqueles que informam, por exemplo, orientação sexual, religiosa, ideológica, política, dados de saúde, genéticos ou biométricos, que podem acarretar discriminações, caso se tornem públicos. Diante disso, eles gozam de uma proteção específica tanto no Regulamento Europeu de Proteção de Dados, quanto na Lei n. 13.709/2018. Assim, semelhante ao disposto, no art. 9º do Regulamento (UE) 2016/679, o art. 11 da lei brasileira de proteção de dados autoriza o tratamento de dados sensíveis, quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; para cumprimento de obrigação legal do controlador; com o fim de realização de estudos por órgão de pesquisa, entre outras hipóteses (BRASIL, 2018).

Nessa perspectiva, a complexidade da dinâmica de tratamento de dados e o processo de tomada de decisões automatizadas extrapolam a classificação dos dados, a partir de seu grau de identificabilidade, que exclui do âmbito de proteção aqueles não identificáveis ou anônimos. Isso ocorre porque é possível agregar esses últimos tipos de dados, identificando seus titulares, ou ainda, pode-se basear em dados não identificáveis para tomar decisões que afetam o desenvolvimento da personalidade dos indivíduos. Nota-se, por exemplo, que a formação de perfis comportamentais, a partir de dados anônimos para a tomada de decisões, pode introjetar nelas padrões discriminatórios (BIONI, 2019, p. 78-79). Assim, o parâmetro mais seguro para determinar se as normas de proteção devem incidir ou não sobre um dado é a relação de causa e efeito que o tratamento de dados pode exercer sobre uma pessoa (BIONI, 2019, p. 78). Dessa maneira, a análise do conceito de dado pessoal deve ser feita por meio de uma abordagem consequencialista,

ou seja, que o tratamento de dados, anônimos ou pessoais, que afetem o desenvolvimento da personalidade deve ser enquadrado no âmbito das normas de proteção de dados pessoais, o que é corroborado pelo art. 12, § 2º da Lei n. 13.709/2018, que estabelece que dados anonimizados podem ser considerados pessoais, caso sejam utilizados em perfis comportamentais e pelo art. 20 da mesma Lei, que permite o direito do titular de dados à revisão de decisões automatizadas relativas a qualquer tratamento de dados que afete seus interesses (BIONI, 2019, p. 78-82).

Parte-se, agora, para o estudo de outros importantes aspectos da proteção de dados pessoais: os princípios e o consentimento como forma de legitimar o processamento de dados.

3.3. Os princípios da proteção de dados pessoais e a crise do consentimento

Na década de 1980, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) publicou as diretrizes relativas à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, que se aplicam a nível nacional e internacional, aos setores público e privado e estão presentes em vários instrumentos de regulamentação, possuindo clareza e flexibilidade para se conformar às mudanças tecnológicas (OECD, 2003, p. 1).

As diretrizes da OCDE se coadunam com o modelo teórico da autodeterminação informacional, desenvolvido na década de 1980, pois atribui ao usuário a responsabilidade pela proteção de dados pessoais, já que o poder do indivíduo de autodeterminar/controlar suas informações pessoais seria o elemento principal da licitude do tratamento de dados pessoais (BIONI, 2016, p. 150). O consentimento, nesse momento, era visto como uma forma de empoderá-lo na medida em que ele poderia ler as políticas de privacidade e aceitar ou não o tratamento de dados, por organizações, por exemplo.

Pode-se dizer que a autodeterminação informacional tem repercussões ainda nos dias atuais, já que uma das hipóteses de legitimidade do tratamento legítimo de dados tanto na legislação europeia, quanto na brasileira, continua a ser consentimento.

Além disso, os princípios, presentes nas diretrizes, influenciaram tanto o Regulamento Geral de Proteção de Dados, que traz, em seu art. 5º, um catálogo de princípios aplicáveis ao tratamento de dados, quanto a Lei n. 13.709/2018, que apresenta, em seu art. 6º, um rol de princípios, tais como da *finalidade* (o tratamento de dados deverá atender a propósitos legítimos, específicos, explícitos e informados ao titular); o da *adequação*, (o tratamento de dados deve ser compatível com as finalidades que foram informadas ao titular, segundo o contexto desse tratamento); o da *necessidade*, que expressa a limitação do tratamento de dados ao "mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos

em relação às finalidades do tratamento de dados"; o da *qualidade dos dados*, que garante ao titular a exatidão, clareza, relevância e atualização de seus dados; o da *transparência*, que assegura aos indivíduos "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial", etc. (BRASIL, 2017).

Nesse contexto, Laura Mendes afirma que o consentimento é um instituto jurídico para "fazer valer a autonomia privada do cidadão", considerando o componente de autoconformação e liberdade do titular, na proteção de dados pessoais (MENDES, 2014, p. 57). A autora ainda afirma que o consentimento tem natureza atípica para o processamento de dados, visto que ele apresenta características negociais e, ao mesmo tempo, possui caráter personalíssimo, sendo possível aplicar as regras relativas aos negócios jurídicos e contratos ao consentimento, sempre que isso for adequado (MENDES, 2014, p. 60).

Nessa linha, Bruno Bioni ressalta que o consentimento pode se vestir de várias roupagens na proteção de dados pessoais, as quais são refletidas pela adjetivação atribuída a ele, que fornece pistas sobre como deve ser a carga participativa do cidadão, em relação ao controle de seus dados pessoais, por meio do consentimento (BIONI, 2015, p. 34-35). Essa adjetivação é resultado do revigoramento da estratégia regulatória da autodeterminação informacional da década de 1980 (BIONI, 2016, p. 167). Ela tem expressão na lei de proteção de dados brasileira, que prevê que o consentimento deverá ser "uma manifestação *livre, informada e inequívoca* pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Art. 5º, XII da Lei n. 13.709/2018), o que é semelhante ao Regulamento (UE) 2016/679, que prevê uma manifestação de vontade *livre, específica, informada e inequívoca* do titular de dados, em suas considerações iniciais.

Pode-se dizer que há uma escala progressiva de adjetivação do consentimento e a correspondente carga participativa do titular de dados pessoais, de maneira que a carga de participação máxima corresponde a consentimento expresso (manifestação clara e específica de concordância com o uso dos dados) e específico (os dados a serem tratados deverão ter o destino detalhado ao titular); já a intermediária se relaciona ao consentimento inequívoco (não há dúvida que o indivíduo, naquele contexto, concordou com o processamento de dados); a pré-intermediária, por sua vez, remete à finalidade determinada (a autorização não pode ter propósitos demasiadamente genéricos, mas deve ter direcionamento quanto a um leque de situações pertencentes a um contexto); a mínima corresponde à anuência voluntária e livre de coação física ou moral; a básica, por fim, se liga ao consentimento informado, ou seja, o indivíduo deve ter ciência da coleta e do tratamento de dados (BIONI, 2015, p. 34-37).

Entretanto, o consentimento como maneira de controle dos indivíduos sobre suas informações possui forma de implementação complexa, em um contexto de

constante inovação tecnológica, já que nem sempre a pessoa consegue dimensionar as consequências de uma disposição de seus dados (MENDES, 2014, p. 58-59). Nessa linha, Solove afirma que, apesar do modelo da autodeterminação informativa ou, nas palavras do autor, "privacy self-management" ser um componente necessário de qualquer regime regulatório, ele está sendo usado para além de suas capacidades, já que existem problemas cognitivos e estruturais que prejudicam a capacidade do cidadão autogerir sua privacidade (SOLOVE, 2013, p. 1.880).

Para Solove, esse modelo pressupõe uma pessoa racional e informada, apta para tomar decisões adequadas acerca do consentimento ou não à coleta e ao tratamento de seus dados pessoais. Contudo, estudos empíricos e sociais demonstram que a habilidade real das pessoas decidirem, de forma racional e informada, de fato, é bem diferente da visão idealizada no sistema de autogestão da privacidade, de maneira que existem obstáculos a esse mecanismo, tais como: *i*. as pessoas não leem as políticas de privacidade; *ii*. se elas leem, não as entendem; *iii*. se as pessoas lerem e entenderem tais políticas, elas ainda podem possuir conhecimento de fundo insuficiente para tomar uma decisão informada; *iv*. se as pessoas leem e entendem as políticas de privacidade e conseguem decidir, de maneira informada, uma escolha ainda será direcionada por várias dificuldades do processo de tomada de decisão (SOLOVE, 2013, p. 1.883 e 1.888). Além disso, há um dilema entre a necessidade de simplificar os avisos de privacidade, para facilitar a compreensão e o fato de que, para o consentimento ser significativo, os avisos devem explicitar os detalhes do tratamento de dados, o que os torna mais complexos (SOLOVE, 2013, p. 1.880).

Nesse cenário, é possível dizer que um quadro regulatório voltado à redoma do modelo da autodeterminação informacional mostra-se insuficiente para lidar com o atual contexto dos dados pessoais como ativos econômicos e elementos que condicionam o livre desenvolvimento da personalidade de seus titulares (BIONI, 2016, p. 167-168). Além disso, o papel central do consentimento, nesse modelo, está relacionado à visão do século XX de que os dados pessoais são autônomos, granulares, independentes, que confirma um direito autônomo e exclusivo dos cidadãos para determinar a utilização e captação de dados (BELLANGER, 2014, p. 2). Entretanto, essa perspectiva merece ressalvas, já que os dados pessoais não estão isolados, mas formam uma rede, na qual cada um dos dados permanece pessoal, mas forma uma totalidade inseparável, considerando que, por exemplo, não há valor absoluto para as empresas em um dado unitário, visto que eles ganham sentido por sua agregação inteligente aos outros (BELLANGER, 2014, p. 2).

Assim, há uma dimensão social por trás da proteção de dados pessoais de grande importância. Nesse sentido, Bruno Bioni propõe que a teoria da privacidade como integridade contextual de Hellen Nissenbaum pode ser utilizada como alternativa ao papel central dado ao consentimento, no modelo da autodeterminação informacional

(BIONI, 2019, p. 210-211). A tese de Nissenbaum atrela-se ao estudo do fenômeno social da existência de distintos contextos que possuem conjuntos diferentes de normas relativas a papéis sociais e expectativas, que forneceriam uma espécie de relativa normatividade da privacidade (NISSENBAUM, 2004, p. 136-137).

Dentre os diversos tipos de normas, estão as relativas às informações sobre as pessoas envolvidas, em determinado contexto, cujo descumprimento leva a uma violação à privacidade (NISSENBAUM, 2004, p. 138). Elas são as normas de adequação, que circunscrevem o tipo e a natureza da informação sobre vários indivíduos, que são autorizadas, esperadas ou até demandadas que sejam reveladas, dentro de certo contexto, e as de fluxo ou distribuição, exemplificadas por regras de discrição e confidencialidade esperadas quando se compartilha uma informação com um amigo, por exemplo, além das normas de transações entre clientes (o consumidor é obrigado a fornecer dados suficientes de que ele pode pagar por determinado produto/serviço) (NISSENBAUM, 2004, p. 138 e 140-142). Essas normas impõem restrições ao fluxo informacional, verificando-se sua integridade através do contexto em que eles estão inseridos, que independem do controle por meio do consentimento, feito pelo indivíduo (BIONI, 2019, p. 212).

Para verificar se um fluxo informacional é adequado ou não a certo contexto, pode-se questionar alguns elementos: *i*. quais são os propósitos do tratamento de dados, considerando o contexto deste fluxo; *ii*. como terceiros estão inseridos neste fluxo e com que condições; *iii*. quais as implicações do tratamento de dados para o titular quanto ao desenvolvimento de sua personalidade e para suas relações sociais (BIONI, 2019, p. 238). Nessa perspectiva, a teoria da integridade contextual à proteção de dados pessoais pode auxiliar na aplicação do princípio da finalidade, adequação e necessidade, previstos no art. 6º, I da Lei n. 13.709/2018, bem como na análise da compatibilidade das finalidades do tratamento de dados com aquelas consentidas pelo titular, além da legitimidade do processamento de dados por conta do legítimo interesse do controlador (BIONI, 2019, p. 238-242), que é uma das hipóteses que legitimam o tratamento de dados pessoais, dentre as quais está o consentimento.

4. Aprofundando a dimensão coletiva da privacidade

4.1. Regulação de risco e responsabilidades dos agentes de tratamento de dados

Entre a edição das diretrizes sobre proteção de dados pessoais, na década de 1980, pela OCDE e da Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC), houve um progresso geracional das leis de dados pessoais, pois essa última, ao tentar resolver o problema do controle pouco efetivo do titular sobre seus dados, não só previu direitos aos indivíduos, mas estabeleceu, simetricamente, deveres a quem processa os dados pessoais (BIONI, 2016, p. 152-153). Essa tendência se intensificou de tal forma

que é possível dizer que houve, no Regulamento Geral de Proteção de Dados da União Europeia, uma guinada teórica, marcada pela incorporação de novas lentes de análise ao debate sobre proteção de dados pessoais, representado pela regulação do risco e pela reproblematização dos arranjos normativos do Brasil, que fricciona o modelo da autodeterminação informacional (ZANATTA, 2017, p. 2).

Nesse modelo da regulação de risco, a proteção de dados pessoais é marcada pela presença de: *i*. instrumentos de tutela coletiva e participação de organizações civis em discussões preventivas com autoridades independentes de proteção de dados; *ii*. "obrigações e instrumentos de regulação *ex ante* atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais"; *iii*. disseminação de métodos de "gestão de riscos" (ZANATTA, 2017, p. 9). Com isso, compreende-se que a coleta e o tratamento de dados pessoais trazem riscos aos direitos fundamentais dos cidadãos, que devem ser identificados e mitigados por intermédio de mecanismos preventivos, além do fomento à transparência e ao diálogo entre os controladores de dados, reguladores, membros da sociedade civil, entre outros atores.

É possível identificar traços do modelo da gestão de risco, tanto no Regulamento Geral de Proteção de Dados, quanto na Lei n. 13.709/2018, como o teste de proporcionalidade necessário para que o controlador realize o tratamento de dados com base em seus legítimos interesses (art. 7º, IX e art. 10 da Lei n. 13.709/2018), cuja análise deve considerar se os direitos fundamentais dos titulares não se sobrepõem a esses interesses e uma avaliação de riscos relativa aos prejuízos que os indivíduos podem ter.

Ademais, o art. 20 da Lei n. 13.709/2018, que prevê o direito do titular de dados de solicitar revisão por uma decisão tomada unicamente com base em um tratamento automatizado de dados, tem por objetivo, justamente, gerir os riscos que envolvem esse tipo de decisão para os interesses dos indivíduos, o que pode ocorrer na definição de perfis comportamentais, de consumo e de crédito. Assim, o responsável pelo processamento de dados deve fornecer os dados pessoais ou anônimos usados na tomada de decisões e explicar os critérios e a lógica dos algoritmos que os controlam, o que será fiscalizado pela Autoridade Nacional de Proteção de Dados (MONTEIRO, 2018, p. 9-10).

Além disso, há as responsabilidades daqueles que realizam o tratamento de dados, disciplinadas pelos arts. 42 a 45 da Lei n. 13.709/2018, que trazem, como regra geral, no art. 42, *caput*, da Lei, o dever de reparação do controlador, a quem compete as decisões quanto ao processamento de dados (art. 5º, VI da Lei) e do operador, que realiza o tratamento em nome do controlador (art. 5º, VII da Lei) por dano patrimonial, moral devido à violação da lei de proteção de dados.

Assim, a Lei n. 13.709/2018 estabelece uma série de obrigações para esses agentes como o dever de "comunicar à autoridade nacional e ao titular a ocorrência de um incidente de segurança que possa acarretar risco ou dano relevante aos titulares", de

modo que essa comunicação deve ser feita, em prazo razoável, mencionando a natureza dos dados pessoais envolvidos, as informações sobre os titulares desses dados, os riscos relacionadas a esse incidente, etc. (art. 48, *caput* e § 1º da Lei n. 13.709/2018). Existem também algumas sanções para os agentes de tratamento de dados, em caso de violações à lei de proteção de dados, tais como multa simples de até 2% do faturamento das pessoas jurídicas de direito privado, grupo ou conglomerado no Brasil (art. 52, II da Lei n. 13.709/2018).

Em outra perspectiva, a responsabilidade demonstrável das empresas corresponde, grosso modo, à adoção de políticas de privacidade compatíveis com leis, princípios, etc., além do estabelecimento de mecanismos de desempenho para que sejam tomadas decisões responsáveis sobre o gerenciamento de dados. Pode-se dizer que há uma estreita ligação entre essa proposta e o modelo da regulação de risco. Isso se dá porque, dentre os elementos dessa responsabilidade, estão a transparência e os mecanismos de participação individual (que envolvem o fornecimento de informações úteis aos titulares de dados sobre as suas utilizações futuras e não óbvias, os benefícios e potenciais riscos do tratamento de dados, além dos meios para amenizá-los, de maneira que se fortalece a confiança dos clientes na organização, permitindo que os usuários exerçam seus direitos) (CENTER FOR INFORMATION POLICY LEADERSHIP AT HUNTON & WILLIAMS LLP, 2015, p. 3); a melhor avaliação de risco, no tocante aos impactos do tratamento de dados para os usuários e para a sociedade como um todo, para decidir as medidas de segurança adequadas a ele; estrutura organizacional que reflita compromisso quanto à proteção de dados, com políticas de acordo com critérios legais, principiológicos ou ligados a práticas do setor (ARTESE, 2017, p. 16), a ética e o processamento justo do dados, que envolve uma estrutura ética adequada para guiar as decisões "se" e "como" processar uma informação, etc.

Nesse contexto, Artese propõe uma interligação entre a responsabilidade demonstrável das empresas, e a taxonomia dos dados pessoais para lidar com a crise do consentimento e com o próprio modelo de autodeterminação informacional, que já foram tratados no capítulo anterior. Assim, pode-se estabelecer uma gradação decrescente entre os dados: 1) fornecidos, originados das ações de seus titulares, plenamente conscientes de sua coleta; 2) observados, que advêm do mapeamento sobre os conteúdos que o indivíduo busca, a duração da pesquisa, etc.; 3) derivados, que provêm de outros, formando um novo conjunto de dados sobre o indivíduo e 4) inferidos, resultado de um processo analítico de análise preditiva para capacidade de crédito, por exemplo (ARTESE, 2017, p. 12-13). Quanto mais perto o dado do grau 1, maior o grau de consciência e mais significativo o consentimento, já quanto mais próximo do nível 4, mais necessária é a responsabilidade demonstrável e menor o papel do consentimento, no tratamento de dados (ARTESE, 2017, p. 13-14).

Percebe-se que muitos desses elementos da responsabilidade demonstrável podem ser considerados já na própria confecção de produtos e serviços relacionados ao tratamento de dados pessoais. Nesse quadro, a privacidade "by design" é uma importante ferramenta de proteção de dados pessoais e está prevista no art. 46, § 2º da Lei n. 13.709/2018. Assim, a ideia dessa técnica é que o administrador dos dados antecipe o interesse dos indivíduos, ainda na fase de planejamento da proteção de dados, adequando seu produto ou serviço a processar a mínima quantidade de dados para satisfazer o propósito do tratamento, limitando os tipos, o volume de dados, o número de vezes que o processo ocorre, bem como o período de armazenamento dos dados, além das pessoas e entidades que podem acessar esses dados (CLARK; ALMOND; ROOM, 2017, p. 13-14). Dessa maneira, a privacidade "by design" exige que os arquitetos de sistemas de tratamento de dados valorizem os interesses dos indivíduos, estabelecendo padrões fortes de privacidade que passarão a integrar a arquitetura do sistema operacional de tratamento de dados e as práticas negociais, sem diminuir sua operacionalidade (CAVOUKIAN; DIX; EMAM, 2014, p. 19-20).

É importante dizer que existem desafios referentes tanto à lente teórica da regulação de risco, como um todo, quanto da privacidade "by design", em específico. Assim, a "risquificação" traz preocupações quanto a atribuição de mais responsabilidades aos processadores de dados, que dá a eles mais oportunidades para tomarem decisões sobre o tratamento, o que pode ocasionar um isolamento do cidadão sobre as questões jurídicas, sociais, etc. que envolvem seus dados pessoais (ZANATTA, 2017, p. 26). Há também muitos desafios relacionados à privacidade "by design" para serem enfrentados, como a falta de engajamento das organizações para implementar suas propostas, o questionamento se os consumidores estariam dispostos a pagar por serviços que antes eram gratuitos, caso as empresas alterem sua política de privacidade e lucrem menos com dados pessoais, além do escasso conhecimento sobre os benefícios tangíveis e intangíveis e os riscos relativos às práticas de privacidade das empresas (SPIEKERMANN, 2012, p. 39-40).

Pertinente mencionar aqui um tema que causa preocupação, em um contexto em que cada vez mais produtos confeccionados com tecnologia de inteligência artificial são responsáveis por decisões e condutas desses sistemas. O fato de os sistemas autônomos não terem personalidade jurídica, observado que não se pode atribuir declarações de vontade a eles, leva a reflexões sobre quem deve ser acionado em caso de danos (DÖPKE, 2018, p. 17). Embora seja uma questão de difícil solução e que dependa de análises técnicas no caso concreto, tem-se que a responsabilidade do usuário tende a ser subjetiva, porém a dos produtores é mais delicada, pois ela é enquadrável como objetiva pelas normas consumeristas, mas poderão ser considerados excludentes o conhecimento científico existente no momento da confecção para detectar um defeito e podem ser

analisados os cuidados tomados por eles por meio da elaboração de instruções da máquina antes de colocá-la no mercado (DÖPKE, 2018, p. 17-18), que pode levar em consideração as medidas de privacidade "by design" adotadas pelos produtores.

4.2. Os agentes sociais na proteção de dados pessoais

A proteção de dados pessoais tem uma notável dimensão coletiva, uma vez que a privacidade é essencial para garantir a autonomia dos cidadãos, em um ambiente democrático, pois remete a uma necessidade psicológica e antropológica dos indivíduos de refletir sobre sua autoimagem, desejos contraditórios e tomada de decisões, possibilitando a formação de cidadãos livres e autônomos (BOEHME-NEßLER, 2016, p. 225-228).

Além disso, a privacidade tem valor coletivo (codependência), pois o nível dela não depende apenas de escolhas isoladas, mas de outros agentes sociais (indivíduos e instituições), além de ser um fenômeno social coletivo (cooperação), já que deve haver uma conscientização dos impactos coletivos de decisões individuais sobre privacidade, visto que o consentimento de um titular de dados pode afetar a privacidade do outro, porque suas informações podem ser usadas para montar o perfil de um grupo social (BARUH, POPESCU, 2017, p. 590-591). Vale ressaltar também que as ações processuais coletivas têm maiores chances de êxito do que as individuais, por conta dos altos custos envolvidos na produção probatória dos processos, por exemplo (ROCHEFELD, 2018, p. 76). Nessa linha, faz-se necessário um engajamento social, coletivo em prol da proteção de dados pessoais, o que já vem acontecendo, mesmo que de maneira incipiente, no Brasil.

Nesse sentido, destaca-se a atuação do Ministério Público, em especial, o Federal e o Ministério Público do Distrito Federal e Territórios (MPDFT) na defesa dos direitos relacionados a interesses coletivos e difusos atrelados à proteção de dados pessoais. Como exemplo de atuação do MPDFT, há o caso do incidente de segurança relativo a dados de clientes da empresa Netshoes, cujos dados de CPF, nome de cliente, e-mail, data de nascimento, códigos de referência de produtos (como monitores arteriais), entre outros, de quase 2 milhões de contas foram vazados. Nesse caso, o MPDFT instaurou um Inquérito Civil Público para investigar as causas do acidente, avaliando a qualidade dos esclarecimentos que a Netshoes prestou aos clientes, o que foi considerado insuficiente, pois foi feito por e-mail genérico que não informava o rol de dados comprometidos, e declarou à Netshoes que, se não fizesse esse aviso mais detalhado, poderia ser instaurada Ação Civil Pública por danos materiais e morais aos consumidores (BRASIL, 2018, p. 1-4).

Ademais, há a atuação do Instituto Brasileiro de Defesa do Consumidor (IDEC), que, recentemente, ajuizou uma ação civil pública contra a concessionária da linha 4 do Metrô da cidade de São Paulo, por conta da instalação das "portas interativas",

em abril de 2018, cuja tecnologia permitia que uma lente com um sensor identificasse a quantidade de pessoas humanas que olhavam para a tela e permitia a captação de emoções, gênero e faixa etária das pessoas situadas em frente ao sensor. Segundo o IDEC, essas lentes eram colocadas acima de propagandas, o que as permitia identificar quais eram as emoções das pessoas ao verem esses anúncios, sem, contudo, ter o consentimento dos usuários do metrô. Os dados gerados a partir dessa análise eram vendidos para terceiros, que poderiam utilizá-los em suas estratégias de marketing. Tal prática viola uma série de dispositivos, como a proteção contra práticas abusivas ao consumidor (art. 6º, IV, CDC), o dever de informar de forma clara os consumidores sobre produtos e serviços (art. 6º e 31 do CDC) e o próprio art. 10 da Lei n. 13.709/2018.

Por fim, é importante discutir sobre a Autoridade Nacional de Proteção de Dados (ANPD), cuja atuação e existência é essencial para a aplicação, supervisão, interpretação, educação, cumprimento e aplicação de sanções de uma lei de proteção de dados, além do fato de que a ANPD tende a ter maior experiência dos que os tribunais para "interpretar a lei de privacidade com a nuance e a flexibilidade adequada às circunstâncias", servindo de ouvidoria para acolher reclamações dos titulares de dados (CENTER FOR INFORMATION POLICY LEADERSHIP AT HUNTON & WILLIAMS LLP, 2017, p. 15-16). Além disso, espera-se que a Autoridade atue como instância regulatória, emitindo opiniões técnicas específicas para a proteção de dados e realizando o controle homogêneo do cumprimento de normas da LGPD, independente de pressões políticas ou ideológicas (DOUEK; ADAMI; LANGENEGGER; LEMOS; FRANCO, 2018).

Originariamente, ela estava prevista no projeto 53/2018 que deu origem à Lei n. 13.709/2018. Contudo, sua instituição sofreu veto presidencial, sob o argumento de vício de iniciativa pelo Legislativo, quanto à criação dessa autoridade nacional, o que tornaria os artigos da lei relativos à sua criação e estruturação inconstitucionais. Todavia, houve explícito compromisso do governo em restabelecê-la, o que foi feito, pela Medida Provisória n. 869/2018.

Essa medida prevê que a Autoridade Nacional de Proteção de Dados (ANPD) será um órgão da Administração Pública Federal, integrante da Presidência da República com autonomia técnica, diferente do que havia estabelecido o PL n. 53/2018, pois nele a ANPD comporia a administração pública federal indireta, submetida a regime autárquico especial e vinculado ao Ministério da Justiça, gozando de independência administrativa, ausência de subordinação hierárquica, mandato fixo, estabilidade dos dirigentes e autonomia técnica e financeira. Tal mudança efetivada pela MP n. 869/2018 pode comprometer a possibilidade da ANPD fiscalizar o Poder Público, pois essa atividade pode ser vista como inconstitucional em vista do princípio federativo, o que pode colocar em risco os direitos dos cidadãos quanto ao tratamento de dados por estados, municípios e órgãos públicos, bem como a transferência internacional de dados, já que o modelo

proposto afasta a ANPD das exigências estrangeiras para transferência de dados para outros países, impactando atividades que dependem dessa última, como a contratação de serviços em nuvem. (DOUEK; ADAMI; LANGENEGGER; LEMOS; FRANCO, 2018).

5. Conclusão

A sociedade da informação ou sociedade em rede apresenta modelos de negócios, estruturas de trabalho, formas de planejamento e organização de instituições privadas e públicas cada vez mais dependentes de dados, cujo processamento se intensificou com o barateamento dos meios de desempenhar essa atividade e com o aumento da capacidade de armazenamento de dados, por conta do desenvolvimento tecnológico. Tal cenário causa diversas preocupações em torno da proteção da privacidade e dos dados pessoais. Diante disso, a compreensão de que o dado pessoal é uma extensão da personalidade auxilia na aplicação de variadas normas do ordenamento jurídico às relações jurídicas que envolvem seu tratamento. É importante dizer, contudo, que a proteção de dados pessoais deve contar não só com a aplicação da Lei n. 13.709/2018 à solução de casos concretos, mas também com uma abordagem preventiva, exemplificada pela implementação de mecanismos de proteção, pelos próprios agentes econômicos, como podem ser consideradas a privacidade "by design" e a responsabilidade demonstrável das empresas. Desse modo, a integração entre uma lei de proteção de dados, técnicas de confecção de produtos e serviços e formas de promoção da transparência e confiança na relação entre empresa e cliente, junto à preocupação coletiva em torno dos dados pessoais é fundamental para a difícil missão de proteger os dados pessoais em uma economia cada vez mais marcada pela lógica de tratamento de volume exponencial de dados.

São Paulo, 15 de abril de 2019.

Referências

AGUIAR JÚNIOR, Ruy Rosado. (coord.). *Jornadas de direito civil I, III, IV e V*: enunciados aprovados. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2012. Disponível em: https://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-aprovados-da-i-iii-iv-e-v-jornada-de-direito-civil/compilacaoenunciadosaprovados1-3-4jornadadircivilnum.pdf/at_download/file.

ARTESE, Gustavo. Privacidade e proteção de dados pessoais: a diluição do consentimento e a responsabilidade demonstrável (accountability). *Revista Fórum de Direito na Economia Digital:* RFDED, Belo Horizonte, ano 1, n. 1, p. 141-162, jul./dez. 2017.

BARUH, Lemi; POPESCU, Mihaela. Big data analytics and the limits of privacy self-management. *New Media & Society*, Thousand Oaks, v. 19, n. 4, p. 579-596, 2017.

BELLANGER, Pierre. *Principes et pratiques des données personnelles en réseau*: contribution de Pierre Bellanger à l'étude 2014 du Conseil d'État: technologies numériques et libertés et droits fondamentaux, Sept. 2014. Disponível em: https://pierrebellanger.skyrock.com/3231110655-Principes-et-pratiques-des-donnees-personnelles-en-reseau.html. Acesso em: 30 jul. 2018.

BIONI, Bruno Ricardo. *Autodeterminação informacional*: paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. Dissertação (Mestrado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2016.

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

BIONI, Bruno Ricardo. *Xeque-Mate*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI, jul. 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil.

BOEHME-NEßLER, Volker. Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, Oxford, v. 6, n. 3, p. 210-221, Aug. 2016.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p. 193-220, Dec. 1890.

BRASIL. Conselho da Justiça Federal. *Jornadas de direito civil I, III, IV e V*: enunciados aprovados. Coordenador científico Ministro Ruy Rosado de Aguiar Júnior. Brasília, DF: Conselho da Justiça Federal, Centro de Estudos Judiciários, mar. 2012. Disponível em: https://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-aprovados-da-i-iii-iv-e-v-jornada-de-direito-civil/compilacaoenunciadosaprovados1-3-4jornadadircivilnum.pdf/at_download/file.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Portal do Planalto*, Brasília, DF, mar. 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRASIL. Ministério Público do Distrito Federal e Territórios. *Recomendação n. 01/2018*. Disponível em: http://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Recomendacao_Comissao_Protecao_Dados_2018_01.pdf. Acesso em: 14 ago. 2018.

BRITO, Felipe Timbó; MACHADO, Javam Castro. Preservação de privacidade de dados: fundamentos, técnicas e aplicações. *In:* DELICATO, Flávia C.; PIRES, Paulo F.; SILVEIRA, Ismar Frango. (org.). *Jornadas de atualização em informática 2017*. Porto Alegre: Sociedade Brasileira de Computação, 2017. p. 91-130. Disponível em: http://csbc2017.mackenzie.br/public/files/all/livro-jai.pdf.

CAVOUKIAN, Ann; DIX, Alexander; EMAM, Khaled El. *The unintended consequences of privacy paternalism*. Toronto: Information and Privacy Commissioner of Ontario, Mar. 2014. Disponível em: https://www.deslibris.ca/ID/242494.

CENTER FOR INFORMATION POLICY LEADERSHIP AT HUNTON & WILLIAMS LLP. Pontos de discussão. *Projeto de Lei n. 5.276/2016, do Poder Executivo, de Proteção de Dados*, abr. 2017. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_-_pontos_de_discuss%C3%A3o_pl_5276_de_2016_-_5_abril_de_2016__1_junho_de_2017_.pdf. Acesso em: 12 abr. 2019.

CENTER FOR INFORMATION POLICY LEADERSHIP. *Protecting privacy in a world of big data*. The role of enhanced accountability in creating a sustainable data- driven economy and information society. Oct. 2015. (Paper 1). Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf.

CHEE, Foo Yun. Presidente-executivo da Apple aponta para uso de dados de clientes como armas para aumentar lucro. *Portal Reuters*, out. 2018. Disponível em: https://br.reuters.com/article/internetNews/idBRKCN1MY26B-OBRIN. Acesso em: 17 fev. 2018.

CLARK, Kayleigh; ALMOND, Peter; ROOM, Stewart. Technology's role in data protection – the missing link in GDPR transformation. *PwC*, Oct. 2017. Disponível em: https://www.pwc.co.uk/legal/pdf/technologys-role-in-data-protection-the-missing-link-gdpr-transformation.pdf.

COMISSÃO EUROPEIA. Comunicado de imprensa. *Anti-trust*: comissão aplica coima de 4.43 mil milhões de EUR à Google por práticas ilegais relacionadas com dispositivos móveis Android destinadas a reforçar a posição dominante do motor de pesquisa da Google, jul. 2018. Disponível em: https://europa.eu/rapid/press-release_IP-18-4581_pt.htm. Acesso em: 25 jul. 2018.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DÖPKE, Christian. The importance of big data for jurisprudence and legal practice. *In*: HOEREN, Thomas; KOLANY-RISER, Barbara. *Big data in context*: legal, social and technological insights. Münster: Springer Nature, 2018. p. 13-19. Disponível em: https://link.springer.com/content/pdf/10.1007%2F978-3-319-62461-7_2.pdf.

DOUEK, Daniel; ADAMI, Mateus Piva; LANGENEGGER, Natalia; LEMOS, Ronaldo; FRANCO, Sofia Lima. A criação da Autoridade Nacional de Proteção de Dados pela MP n. 869/2018. *Portal Jota*, São Paulo, dez. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-criacao-da-autoridade-nacional-de-protecao-de-dados-pela-mp-no-869-2018-29122018. Acesso em: 17 fev. 2018.

LEAL, Ana Alves. *Big data* e proteção de dados pessoais: desafios à luz do Regulamento Geral de Proteção de Dados. *Revista Vida Judiciária*, Porto, n. 207, p. 18-19, maio/jun. 2018.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2011.

MENDES, Laura Schertel. *Privacidade, proteção de dados pessoais e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica).

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL n. 5.276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. *Revista Brasileira de Políticas Públicas*, Brasília, v. 7, n. 3, p. 184-198, 2017.

MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?* Rio de Janeiro: Instituto Igarapé, dez. 2018. p. 1-17. Artigo estratégico 39. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf.

NISSENBAUM, Helen. Privacy as contextual integrity. *Washington Law Review*, Seattle, v. 79, p. 119-157, Feb. 2004.

OECD. *Síntese*: diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, 2003. Disponível em: http://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 20 maio 2018.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil* - RBDCivil, Belo Horizonte, v. 16, p. 35-56, abr./jun. 2018.

ROCHEFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva técnica e normativa da União Europeia em face dos gigantes da Internet. *Revista de Direito, Estado e Telecomunicações*, Brasília, v. 10, n. 1, p. 61-84, maio 2018.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, New York, NY, v. 86, n. 6, p. 1.814-1.894, Dec. 2011. Disponível em: http://scholarship.law.berkeley.edu/facpubs/1638. Acesso em: 13 ago. 2018.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. "Big data" – Big problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. *Copendi Law Review*, Florianópolis, v. 2, n. 3, p. 311-331, jan./jul. 2016.

SOLOVE, Daniel J. A taxonomy of privacy. *University of Pennsylvania Law Review*, Philadelphia, v. 154, n. 3, Jan. 2006.

SOLOVE, Daniel J. Introduction: privacy self-management and the consent dilemma. *Harvard Law Review*, Cambridge, v. 126, p. 1.880-1.903, 2013.

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

SPIEKERMANN, Sarah. The challenges of privacy by design. *Communications of the ACM*, New York, v. 55, n. 7, p. 38-40, July 2012.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *In*: TEPEDINO, Gustavo. *Temas de direito civil*. 3. ed. Rio de Janeiro: Editora Renovar, 2004.

UNIÃO EUROPEIA. Conselho da União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. (Texto relevante para efeitos do EEE). Disponível em: http://data.europa.eu/eli/reg/2016/679/oj. Acesso em: 30 maio 2018.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. Dissertação (Mestrado) – Faculdade de Direito, Universidade de Brasília, Brasília, 2007.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? *In*: ENCONTRO DA REDE DE GOVERNANÇA DA INTERNET, 1., nov. 2017, Rio de Janeiro. Disponível em: https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica. Acesso em: 3 ago. 2018.