BIG DATA E O CONFLITO ENTRE A UTILIZAÇÃO DOS DADOS E A PROTEÇÃO À INTIMIDADE E À VIDA PRIVADA

BIG DATA AND THE CONFLICT BETWEEN THE USE OF DATA AND THE PROTECTION OF PRIVACY

Mariana Viale Pereira[1]
Mestre em Direito pela UFRGS

Maria Cláudia Cachapuz[2]
Doutora em Direito pela UFRGS

RESUMO: O *Big Data* representa uma enorme quantidade de dados e de informações alcançadas em uma velocidade recorde na história da humanidade. A questão que emerge, entretanto, é de que forma o uso desses dados, a partir de probabilidades e correlações, pode interferir no direito à privacidade e até mesmo na liberdade individual. Isso se reflete no conflito entre direitos fundamentais, que exige uma ponderação, a partir de bases empíricas, para se alcançar as soluções corretas aos novos problemas que decorrem da realidade da era *Big Data*.

PALAVRAS-CHAVE: *Big Data*; conflito; direitos fundamentais; ponderação.

***ABSTRACT**: Big Data represents an enormous quantity of data and information that has reached historical record speeds. However, the question that stems from this is in which manner the use of this data, in the midst of probabilities and correlations, could interfere in private rights and even in individuals freedoms. This is reflected in the conflict among fundamental human rights, that demands some balance, starting with empirical evidence to achieve concrete solutions to the new issues that come along with the reality of the age of Big Data.*

PALAVRAS-CHAVE: *Big Data*; conflito; direitos fundamentais; ponderação.

---

1 Servidora Pública do TJRS. *E-mail*: mari_viale@hotmail.com.

2 Professora da Faculdade de Direito da UFRGS e da Universidade Feevale, Magistrada do TJRS. *E-mail*: mcmcachapuz@tj.rs.gov.br.

***KEYWORDS**: Big Data; conflict; fundamental human rights; balance.*

***SUMMARY**: Introduction; 1 The current scenario and the concept of Big Data; 2 The right to privacy and the general right to freedom; 3 Informational self-determination and the current scenario; Final considerations; References.*

INTRODUÇÃO

As possibilidades geradas pela quantidade de dados que podem ser processados hoje, bem como as conexões que são possíveis a partir desses dados são inimagináveis. E, nesse panorama, a dificuldade vai desde a diferenciação entre o que são dados públicos e o que são dados privados, além da permissão para uso desses dados. Especialmente, porque não há como prever de antemão quais as conexões serão realizadas, ou para que finalidade esses dados serão utilizados. Nessa medida, torna-se também difícil definir a área de privacidade que deve ser preservada.

Já se escreveu em outra oportunidade que há uma relação mútua entre a construção de espaços ao privado e ao público na perspectiva de estabelecimento de uma autodeterminação informativa – e, portanto, o pleno controle sobre as informações nominativas de cada um –, justamente quando se busca promover o livre desenvolvimento da personalidade do homem: "Ou seja, tanto da liberdade decorrente do pensar, como da liberdade que obriga o homem a compartilhar experiências em sociedade. Até porque é também a partir da distinção entre espaços privados e públicos que resta reconhecido o ambiente social para a vida de convivência" (Cachapuz, 2006, p. 55). A questão de fundo é, na essência, o problema do chamado "impulso à autoexposição" (Arendt, 1993, p. 28), não apenas porque a pessoa participa de uma vida comum com os demais, partilhando experiência tecnológica e informações próprias a seu tempo, mas, fundamentalmente, porque também o indivíduo deseja *aparecer* e, em determinada medida, fazer-se visto, "por feitos e palavras" (Arendt, 1993, p. 28), pelos demais[3].

[3] Conferir o desenvolvimento do tema em estudo sobre liberdade e acesso à informação, pela análise da "autodeterminação informacional", de Tércio Sampaio Ferraz Júnior (2001, p. 242).

A ação e reação sistemática ao avanço da ciência, especialmente em áreas de maior desenvolvimento tecnológico – como a da Tecnologia da Informação –, revela a tendência do homem contemporâneo de aprender a lidar com a sua individualidade sem necessariamente abdicar de um benefício tecnológico que lhe facilita o contato com uma esfera pública de relacionamento. Paul Virilio, antes mesmo da consolidação de uma situação de controle informativo pela ideia do *Big Data*, menciona o exemplo de uma pessoa que, "para lutar contra os fantasmas que pareciam persegui-la" (Virilio, 1999, p. 61), instala câmeras de vídeo na residência, permitindo que os visitantes de seu espaço de divulgação na internet possam auxiliá-la no combate a eventuais fantasmas, num exercício não muito diferente daquele usufruído por quem explora a própria imagem em espaços destinados a efetivos diários de confissão pública, como o Facebook. Poder-se-ia, portanto, questionar em que medida a esfera pública – ou aquilo que a represente no mundo das aparências (Arendt, 1993) – tem-se traduzido em espaço de reflexão ao indivíduo – na essência, resguardado ao privado –, ou mesmo até que ponto se pode reconhecer uma nova concepção de liberdade para o desenvolvimento (livre) da personalidade na sociedade contemporânea.

A problematização trazida no presente estudo refere-se basicamente ao conflito gerado pelo *Big Data* e o direito à intimidade e privacidade. Trata-se, de uma lado, de uma fonte imensurável de possibilidades que surgem a partir do acesso e conexão de dados, que pode incluir o uso público ou privado dessas informações, seja na busca de solução de problemas de interesse público pelo Estado, seja por empresas privadas, detentoras de tais informações, visando a interesses privados específicos e interesses econômicos. De outro lado, isso se traduz em um momento novo, que passa a exigir uma mudança em relação ao que se tinha até então como proteção do direito de intimidade e vida privada, a partir de um conceito de autodeterminação informativa – em que se buscava garantir, a princípio, uma possibilidade de controle sobre os dados pessoais, pelo próprio indivíduo, o que parece não ser mais possível, nessa nova realidade. Impõe-se uma mudança em relação à tutela jurídica, a fim de continuar buscando uma efetiva garantia ao direito à privacidade em relação aos dados pessoais.

Para tanto, parte-se de uma breve explanação das mudanças trazidas pelo sistema *Big Data*, incluindo o que se pode entender por *Big Data* e as inovações e incertezas causadas por essa nova etapa de desenvolvimento do conhecimento informatizado. Após, serão introduzidas breves explanações acerca do

entendimento do direito de personalidade, a partir da teoria das esferas, como um princípio, a ser ponderado, quando em conflito com princípios opostos. Buscar-se-á ainda elucidar o regramento brasileiro acerca da questão.

1 CENÁRIO ATUAL E CONCEITO DE *BIG DATA*

Historicamente a coleta de dados tem sido difícil, com consumo muito grande de tempo e de recursos. O grande entusiasmo causado pelo *Big Data* decorre da percepção de que o armazenamento e cruzamento de dados informativos em larga escala oferece fácil acesso a uma quantidade massiva de dados (Boyd; Crawford, 2012, p. 673). *Sites* de mídias sociais, telefones inteligentes e outros dispositivos de consumo, como computadores, têm permitido que bilhões de indivíduos ao redor do mundo contribuam para a quantidade de dados disponíveis (Manyica et al., 2011, p. 1).

Quando se fala em *Big Data* – apesar de, geralmente, conseguir-se identificar que se está falando de uma grande quantidade de dados –, dificilmente se apreende, em um primeiro momento, o que realmente pode significar o fenômeno. E, de fato, *a priori*, a ideia de um *Big Data* só permite que se afirme que as possibilidades de trato disponíveis à informação são infinitas, a depender das conexões a serem realizadas, bem como da finalidade que se pretende alcançar com o conteúdo informativo predisposto.

Para elucidar a questão, Viktor Mayer-Schönenberger e Kenneth Cukier iniciam o seu livro intitulado *Big Data* explicando como o Google pôde antecipar a expansão da gripe H1N1, nos Estado Unidos da América, no ano de 2009, inclusive em regiões específicas. A conclusão é extraída de bilhões de pesquisas diárias, recebidas e salvas pela empresa. A partir dos dados dispostos, do poder de processamento e do conhecimento estatístico da empresa, restou realizada uma pesquisa baseada nos termos de busca mais comuns pesquisados pelos americanos e na comparação de tais informações com os registros dos CDCs (Centros de Controle e Prevenção de Doenças), a partir de correlações entre a frequência de pesquisas realizadas e da disseminação da gripe em épocas e localidades específicas (Mayer-Schonberger; Cukier, 2013, p. 1-2). A partir do cruzamento de informações, foi descoberta uma combinação de 45 termos de busca que, quando usados conjuntamente em um modelo matemático, mantinham correlação entre a previsão de manifestação da doença e o número oficial de pessoas atingidas pela doença. Ao contrário dos dados oficiais,

contudo, a informação apurada permitia apontar a disseminação do vírus quase em tempo real, antecipando a situação de ocorrência entre uma ou duas semanas em relação à estatística oficial (Mayer-Schonberger; Cukier, 2013, p. 2).

Tal exemplo, assim como tantos outros já registrados, demonstram o quão potente pode ser o uso dos dados informativos como uma ferramenta de auxílio a diversas questões sociais, incluindo as áreas de pesquisas relacionadas a doenças, à segurança – inclusive para combate ao terrorismo –, à adaptação climática (Boyd; Crawford, 2012, p. 663-664). É visto ainda como uma revolução do uso da tecnologia da informação em termos de gestão de negócios para a tomada de decisões – das mais diversas ordens –, possibilitando a medição de variáveis e condições diversas para a escolha da decisão acertada (Mcafee; Brynjolfsson, 2012, p. 4). No varejo de venda de livros, por exemplo, a partir das compras *online*, o cruzamento de informações qualificadas permite a compreensão sobre o público a ser atingido, de forma a potencializar o gosto e as preferências do consumidor para que o fornecedor tenha a capacidade de antecipar o que poderia sensibilizar as preferências de determinado consumidor, cooptando-o para o ato de compra. Mais ainda, desenvolvem-se algoritmos para prever quais livros o consumidor gostaria de ler depois da aquisição que está sendo feita ou mesmo algoritmos que executam, de forma cada vez mais ágil, a própria preferência daquele consumidor com a política de fidelização, para apontar, inclusive, se o cliente responde ou ignora a recomendação (Mcafee; Brynjolfsson, 2012, p. 4).

Um modelo de previsões com uma vasta quantidade de dados, inclusive de forma transnacional, pode ser feito substancialmente de maneira mais acurada pelo aumento dos dados a uma escala massiva. Daí por que uma maior quantidade de dados é potencialmente mais valiosa quando as informações são utilizadas para uma análise de previsões. As instituições capazes de armazenar e trabalhar com o cruzamento de um número significativo de dados – acrescidas da habilidade de tirar alguma vantagem informativa desses dados – potencialmente podem obter uma vantagem competitiva substancial sobre instituições sem acesso a mesmos bancos de dados com semelhante potencial ou sem a habilidade de lidar com eles (Fortuny; Martens; Provost, 2013, p. 223).

No âmbito público, principalmente pela possibilidade de compartilhamento aberto de dados, o *Big Data*, sem dúvida, pode se transformar em instrumento de potente partilha de conhecimento e transparência de informações, capaz de

potencializar soluções para inúmeros problemas sociais. No entanto, trata-se de fenômeno que desafia essa mesma sociedade global com relação ao correto tratamento da informação e de como o aproveitamento da tecnologia pode alterar as relações entre as instituições e as pessoas (Mayer-Schonberger; Cukier, 2013, p. 11). E isto assim se compreende justamente porque o fenômeno do *Big Data* permite o desenvolvimento de habilidades e de capacidades à obtenção permanente de informações e serviços de valor e utilidade significativos, a partir da correlação de dados visando a um fim específico. Tais correlações permitem, a partir de probabilidades, talvez não ainda dizer *por que* algo acontece, mas alertam sobre o fato de que *algo* acontece, antevendo situações para futuro capazes de alterarem relações de causalidade atuais em sociedade (Mayer-Schonberger; Cukier, 2013, p. 8-10).

A grande questão relacionada com o *Big Data* é que as informações geradas com um objetivo são arquivadas, transformadas em dados e depois reutilizadas para outros objetivos. A partir dessa realidade, tem-se que o valor dos dados não diminui com o uso, na medida em que eles podem ser reprocessados e utilizados várias vezes com o mesmo objetivo, ou com objetivos diversos. O valor dos dados está mais relacionado com o seu uso do que com a sua detenção (Mayer-Schonberger; Cukier, 2013, p. 71-85). Assim, as finalidades e utilidades dos dados não são possíveis de serem previstas pelo consumidor, ou usuário dos dados, quando de sua disponibilização, e muitas vezes nem mesmo pelo próprio coletor e depois detentor dos dados, em razão das infinitas possibilidades de usos secundários (Mayer-Schonberger; Cukier, 2013, p. 107). Nessa medida, a autorização para a coleta da informação, baseada na informação acerca do uso imediato das informações, talvez já não se preste a uma proteção efetiva em termos de privacidade.

Tal é a amplitude de exposição pública a partir do desenvolvimento do fenômeno do *Big Data*, que, em termos jurídicos, o reflexo é justamente no âmbito de construção de ferramentas que possam garantir a preservação de uma esfera privada. A questão é que, dado o volume e a capacidade de cruzamento de dados informativos, três das principais estratégias utilizadas para garantir privacidade – o consentimento individual, a opção de exclusão e a anonimização referentemente aos dados – cada vez mais perdem terreno jurídico e mesmo uma solução eficaz em termos de proteção. Veja-se, recentemente, a alteração

de posicionamento jurídico do STJ em relação ao dever de notificação prévia do consumidor – a exemplo da construção dogmática até então prevalente em relação ao armazenamento de dados negativos e de aplicação da Lei nº 12.414/2011 para a justificação de armazenamento de dados em cadastros positivos – para a obtenção de consentimento ao armazenamento de informações utilizadas em bancos de análise de risco de crédito. Na argumentação proposta e acolhida no Recurso Especial nº 1.419.697/RS[4], essa notificação prévia não mais é necessária e depende, unicamente, de uma atividade de busca pelo consumidor. É ele que passa a ter a responsabilidade de querer garantir a sua privacidade frente ao gestor de um banco cadastral de cruzamento de informações para análise e tratamento estatístico sobre suas qualidades como tomador de um crédito.

Há indicativos de que, inclusive, as campanhas eleitorais têm sido influenciadas de forma significativa pelo cruzamento de informações dispostas no *Big Data*, uma vez que as campanhas políticas contemporâneas acumulam significativas bases de dados informativos e contratam analistas de dados de campanhas para criar modelos prevendo os comportamentos dos indivíduos, disposições eleitorais – inclusive quanto à participação ativa e capacidade de influenciar terceiros – e respostas ao contato de promotores de uma campanha eleitoral. Esse novo modo de direcionamento dos dados nas campanhas oferece aos candidatos e aos seus assessores poderosas ferramentas para manejo da estratégia eleitoral (Nickerson; Rogers, 2014, p. 3).

[4] Como estabelecido no Recurso Especial Representativo de Controvérsia nº 1.419.697/RS, são definidas as seguintes teses para aplicação, por analogia, em demandas judiciais assemelhadas 1) O sistema *credit scoring* é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito); 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei nº 12.414/2011 (lei do cadastro positivo); 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei nº 12.414/2011; 4) *Apesar de desnecessário o consentimento do consumidor consultado*, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas; 5) O desrespeito aos limites legais na utilização do sistema *credit scoring*, configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei nº 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei nº 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

2 O DIREITO À INTIMIDADE E À VIDA PRIVADA E O DIREITO GERAL DE LIBERDADE

Em aparente sentido contrário ao movimento do *Big Data*, sem dúvida se reconhece um movimento de busca à proteção dos dados nominativos, justamente porque capazes de revelarem um passo à violação do que se tem como relacionado ao espaço privado dos indivíduos. De forma ampla, o direito à intimidade e à vida privada está previsto no ordenamento jurídico brasileiro como direito fundamental (art. 5º, X, da Constituição Federal de 1988), incluído, no reflexo possível nas relações entre privados, igualmente no art. 21 do Código Civil brasileiro, no que toca à identificação de efetivos direitos de personalidade.

Para possibilitar a efetiva proteção à vida privada, tem-se como possível o reconhecimento de espaços distintos de atuação do ser humano, relacionados com um âmbito de atuação privado ou público, e que, portanto, merecem uma tutela jurídica diversa. A esfera mais interior, ou mais íntima, seria o último e inviolável âmbito de liberdade humana, que deveria ser protegido de forma absoluta, responsável pela configuração da vida privada; a esfera privada ampliada, que inclui o âmbito privado que não pertence a essa esfera mais íntima; e a esfera social, que inclui tudo aquilo que não for atribuído às duas esferas anteriores (Alexy, 2006, p. 360-361). Como se pode ver, a garantia de liberdade geral de ação está relacionada com o livre desenvolvimento da personalidade. E a distinção entre esferas de proteção com diferentes intensidades seria o resultado de ponderações do princípio da liberdade negativa conjuntamente com outros princípios, em face de princípios colidentes. Assim, tem-se que o que a diferenciação entre as esferas privada e social destaca é que a proteção dos direitos fundamentais deve ser tão maior, quanto maior for o peso dos princípios que protegem a privacidade e que estejam aliados ao princípio da liberdade geral de ação (Alexy, 2006, p. 361-364).

A relação entre os princípios contrapostos ocorre a partir da relação de ponderação entre eles, capaz de gerar a conexão entre as possibilidades fáticas e jurídicas de um caso concreto. Assim, quando uma norma de direito fundamental com caráter de princípio – como o direito à intimidade e a vida privada – colide com um princípio contrário – como o interesse público em relação à segurança do Estado –, a possibilidade jurídica para a realização dessa norma depende do princípio contrário. Para se chegar a uma decisão, é preciso realizar uma ponderação (Alexy, 2006, p. 116-117). Considerando que a aplicação de princípios

válidos – caso sejam aplicáveis – é ordenável, e, considerando que, para essa aplicação, nos casos de colisão, se faz necessária uma ponderação, o caráter principiológico das normas de direito fundamental implica a necessidade de uma ponderação quando elas colidem com princípios contrários. O que significa que a máxima da proporcionalidade em sentido estrito pode ser deduzida do caráter principiológico das normas de direitos fundamentais (Alexy, 2006, p. 117-118). O princípio da proporcionalidade exige a observação das três máximas parciais da adequação, da necessidade e da proporcionalidade em sentido estrito. As duas primeiras decorrem da natureza dos princípios como mandamentos de otimização em face das possibilidades fáticas, enquanto a última decorre do fato de os princípios serem mandamentos de otimização em face das possibilidades jurídicas (Alexy, 2006, p. 117-118). Por isso, toda a solução jurídica que acabe restringindo o exercício de uma liberdade individual, tanto para privilegiar uma situação relacionada à privacidade, quanto para privilegiar uma liberdade de expressão do pensamento em nome do interesse público, deve resultar de uma ponderação entre princípios, em que todas as circunstâncias fáticas e jurídicas estarão disponíveis à análise do intérprete. Isso é garantido pela adoção de uma argumentação jurídica baseada no discurso (Cachapuz, 2006, p. 146-147).

A importância de tal construção jurídica para a compreensão dos espaços destinados ao público e ao privado no ordenamento jurídico torna-se essencial na medida em que se inaugura, pela Lei nº 10.406, de 2002, um capítulo exclusivo aos direitos de personalidade no Código Civil brasileiro. Traduz, assim, o art. 21 do Código Civil um efetivo direito subjetivo à proteção da intimidade e da vida privada, permitindo reconhecer que o ordenamento jurídico brasileiro oferece hoje uma estrutura suficiente à configuração de uma proteção à esfera privada, não apenas por oferecer as ferramentas essenciais para a proteção desta esfera no âmbito específico das relações jurídico-privadas, mas por criar uma cláusula geral ao juiz, para ver aplicada a tutela específica ao caso concreto. O que inclui não apenas a solução indenizatória tradicional, como a possibilidade de exame de uma tutela preventiva.

E nisso assume papel essencial a leitura conjunta do art. 21 ao art. 187 do Código Civil brasileiro. Mesmo que uma primeira doutrina (Theodoro Jr., 2003) tenha descrito, na apreciação do art. 187, a manifestação jurídica do instituto do abuso do direito, quer-se, aqui, defender premissa diversa, no sentido de que o direito subjetivo à intimidade e à vida privada é, em sua essência, ilimitado

quanto à liberdade que tutela – o que não quer dizer que não possa sofrer restrições. Estas, porém, partem não de uma configuração abstrata (no conceito), mas das condições fáticas e jurídicas que são impostas pelo caso concreto.

Nessa medida, a ideia de boa-fé, como um dos elementos da conduta lícita do indivíduo pelo art. 187, aproxima-se da concepção de confiança, visando assegurar a relação do particular com o universal, não dispensando relevância ao princípio da igualdade na esfera pública. Há a pretensão de afirmar um princípio de igualdade do ponto de vista formal em relação ao exame das liberdades em conflito, permitindo o conceito de boa-fé que a ideia de confiança seja avaliada a partir das particularidades do caso concreto proposto à discussão. A boa-fé estabelece uma ponte entre o discurso real e o ideal para que, em última análise, o imperativo categórico, reconhecido na característica universal da norma, sirva como *cânone* hermenêutico ao teste de uma máxima de ação particular.

A ligação estrita entre confiança e boa-fé para a caracterização de eventual ilicitude civil é revelada pela necessidade de que se identifique, frente à situação particular, a relação de confiança antes pressuposta no plano formal. Como proposto no art. 187, o conceito de boa-fé identifica a relação de confiança (interna ou externa) estabelecida em face do caso particular, conectando-a à universalidade de conduta exigida do ponto de vista formal e assim possibilitando que se identifique eventual situação de ilicitude em relação ao caso concreto. A conexão promovida pelo elemento da boa-fé, por consequência, é dirigida tanto à relação do particular com o universal, como, na mesma medida, à relação da exclusividade (esfera privada) com a igualdade (esfera pública), de forma a tornar possível uma avaliação do tipo de confiança depositado pelos indivíduos nas suas relações de convívio. Pela ideia de boa-fé, pode-se analisar a extensão da autoexposição promovida pelo indivíduo e medir como quer a pessoa aparecer no espaço público, tornar-se vista. Tal condição é relevante para a própria compreensão da necessidade ou não de se restringir uma liberdade subjetiva, a fim de tutelar a intimidade ou a vida privada de alguém.

3 AUTODETERMINAÇÃO INFORMATIVA E O CENÁRIO ATUAL

Na era da informática e da internet, já era possível se reconhecer uma mudança na forma como o homem contemporâneo lida com a sua individualidade e com a sua exposição. A ideia de autodeterminação informativa a todo o indivíduo foi garantida, já em 1983, pelo Tribunal Constitucional Federal da

Alemanha, em decisão relacionada à Lei do Censo Alemã, no sentido de que toda e qualquer informação pessoal só se tornasse pública se tutelada por um determinado interesse público, porque conhecida pelo titular a sua existência, bem como com quem é compartilhada, a fim de não frear a liberdade do indivíduo de planejar ou decidir segundo sua própria determinação (Cachapuz, 2006, p. 249). Esse fato acaba por reafirmar a adoção da teoria das esferas, a partir do entendimento de que o direito de liberdade não é anulado por uma proteção à esfera de exclusividade do indivíduo, impondo a ponderação a partir de circunstâncias fáticas e jurídicas concretas para evidenciar o grau que pode ser restringida qualquer liberdade, em que também o âmbito absolutamente inviolável, concernente a posições protegidas concretamente de forma definitiva, é o resultado de ponderações (Cachapuz, 2006, p. 249).

Assim, para que o indivíduo possa ser livre, pressupõe-se que este possa determinar a sua ação numa esfera pública, e isso apenas é possível na medida em que haja também uma autolimitação (Cachapuz, 2006, p. 253). A ideia, portanto, para garantir uma efetiva proteção às informações pessoais dos indivíduos é que o titular das informações possa ter o controle sobre o armazenamento e a transmissão dos dados, reconhecendo a possibilidade de interferência do titular a qualquer momento. No Brasil, a preocupação com a proteção de dados pessoais se deu principalmente em relação às leis de consumo, a partir da Lei nº 8.078/1990, que disciplina a atuação dos bancos cadastrais relacionada ao consumo. Busca-se garantir ao indivíduo a existência do registro, a fim de que seja lhe possibilitado verificar desde a extensão até a veracidade das informações armazenadas, a fim de, eventualmente, ser possível promover a sua correção.

A ideia de autodeterminação informativa está marcada, nessa medida, por um princípio da transparência ou publicidade em relação ao armazenamento de dados, uma vez que não é efetiva a existência de um registro de informações pessoais se não existir, de forma efetiva, a possibilidade de fiscalização do conteúdo existente no registro. E isso se mostra relevante não apenas no que diz com a restrição do conteúdo informativo, como também a hipótese de verificação da pertinência do registro sobre determinado interesse público, a partir da qualidade da informação – que aparece como uma das condições de proteção de uma esfera de privacidade, na medida em que está vinculada a uma correção e atualidade da informação, além de uma vinculação às finalidades de sua coleta e armazenamento (Cachapuz, 2006, p. 259-262).

Ainda, a Lei nº 12.965/2014 introduziu princípios, garantias, direitos e deveres para o uso da internet no Brasil, prevendo, entre os seus princípios, a proteção dos dados pessoais, na forma da lei (art. 3º, III), bem como a responsabilização dos agentes de acordo com suas atividades, nos termos da lei (art. 3º, VI), além da liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta lei (art. 3º, VII). Verifica-se, nesse último inciso, uma abertura no que diz com o conhecimento acerca do uso que é feito dos dados, nessa nova realidade *Big Data*, bem como a inocorrência de proibição *a priori*, mas de uma possibilidade de restrição, quando verificada uma afronta aos princípios contrários, como o da proteção dos dados, o que deixa aberto o espaço a uma ponderação a ser realizada, a partir das peculiaridades do caso concreto, a ser realizada pelo aplicador do Direito, quando verificada uma situação de conflitos de liberdades.

A própria lei, apesar de não falar especificamente em *Big Data*, reconhece uma nova realidade, a ser considerada, uma vez que, no seu art. 6º, estabelece que "na interpretação desta lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural". No entanto, no artigo seguinte (7º), garante expressamente aos usuários a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação" (inciso I); a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (inciso III); "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicação de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (inciso VII); "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet" (inciso VIII, *a*, *b* e *c*); "consentimento expresso sobre coleta, uso armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (inciso IX); "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei" (inciso X).

A lei, inclusive, garante o direito à privacidade e à liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet (art. 8º), considerando nulas de pleno direito as cláusulas contratuais que violem isso, tais como aquelas que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet ou, em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil (parágrafo único, incisos I e II do art. 8º). A Lei nº 12.965/2014, nos arts. 10 a 12, especifica de que forma ocorrerá à proteção aos registros, aos dados pessoais e às comunicações privadas e, nos arts. 18 a 21, estabelece a responsabilidade por danos decorrentes do conteúdo gerado por terceiros.

Não há, portanto, como se desconhecer a preocupação, no ordenamento jurídico brasileiro, com a situação de proteção à esfera privada, especialmente em face da potencialidade identificada frente a fenômenos como o do *Big Data*, pela possibilidade de tratamento massivo da informação por meio de ferramentas complexas de cruzamento de dados. Caberá ao intérprete jurídico combinar os instrumentos de freio à automação para realizar a ponderação necessária em face das situações que se imponham em concreto.

CONSIDERAÇÕES FINAIS

É preciso ter em mente que, na era do *Big Data*, as pessoas estão dispostas a compartilhar informações *online*, uma vez que esse é um requisito necessário para utilização dos serviços virtuais, por isso, em certa medida, estão cientes de uma maior vulnerabilidade em relação aos dados, inerente ao momento em que vivemos. No entanto, isso implica uma mudança na forma como as leis devem proteger as informações.

Na medida em que a precaução torna-se cada vez mais difícil, a responsabilização acaba sendo enfatizada. Apesar de talvez não se poder mais ter esse controle prévio sobre quais informações circulam e para que finalidades específicas estão sendo utilizadas, nessa nova realidade *Big Data*, sempre é possível uma responsabilização pelo uso indevido da informação, tanto a partir de procedimentos administrativos específicos, que visem supervisionar e controlar *a priori* uma eventual gestão abusiva de dados, como uma responsabilidade, posterior, decorrente de um uso indevido de dados particulares, desconectados com a finalidade de seu armazenamento e, mais ainda, que afrontem uma esfera

de privacidade, que deveria ser exclusiva ao indivíduo. E isso parece estar garantido pela legislação brasileira vigente.

Ademais, quando julgada a questão, sempre é possível, a partir do caso concreto envolvendo direitos fundamentais, em que evidenciadas liberdades conflitantes, o exercício da ponderação, a fim de se encontrar, na situação específica, a afronta ou não do direito de personalidade do titular dos dados.

REFERÊNCIAS

ALEXY, Robert. *Teoria de los derechos fundamentales*. 2. ed. Madrid: CEPC, 2001.

_____. *Teoria dos direitos fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2006.

ARENDT, Hannah. *A vida do espírito*: o pensar, o querer, o julgar. 2. ed. Rio de Janeiro: Relume Dumará, 1993.

BOYD, Danah; CRAWFORD, Kate. Critical questions for Big Data. In: *Information, Communication & Society*, 2012. Disponível em: <https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf>. Acesso em: 30 maio 2017.

CACHAPUZ, Maria Cláudia. Informática e proteção de dados. Os freios necessários à automação. *Ajuris*, a. XXIV, v. 70, jul. 1997.

_____. *Intimidade e vida privada no novo Código Civil brasileiro*: uma leitura orientada no discurso jurídico. Porto Alegre: Sergio Antonio Fabris, 2006.

FERRAZ JR., Tércio Sampaio. A liberdade como autonomia de acesso à informação. In: GADAMER, Hans-Georg. *Histórica y linguaje*: uma respuesta. In: KOSELLECK, Reinhart; GADAMER, Hans-Geor. *Historia y hemenêutica*. Barcelona: Ediciones Piados, 1997.

FORTUNY, Enric Junqué de; MARTENS, David; PROVOST, Foster. Predictive modeling with Big Data: Is bigger really better? 2013. Disponível em: <http://online.liebertpub.com/doi/pdf/10.1089/big.2013.0037>. Acesso em: 30 maio 2017.

MANYICA, James et al. Big Data: the next frontier for inovation, competition and productivity, 2011. Disponível em: <https://bigdatawg.nist.gov/pdf/MGI_big_data_full_report.pdf>. Acesso em: 30 maio 2017.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big Data*: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Trad. Paulo Polzonoff Junior. 1. ed. Rio de Janeiro: Elsevier, 2013.

MCAFEE, Andrew; BRYNJOLFSSON, Erik. Big Data: the management revolution, 2012. Disponível em: <http://www.tias.edu/docs/default-source/Kennisartikelen/mcafeebrynjolfson_bigdatamanagementrevolution_hbr2012.pdf>. Acesso em: 30 maio 2017.

NICKERSON, David W.; ROGERS, Todd. Political Campaigns and Big Data. *HKS Faculty Research Working Paper Series RWP13-045*, Revised February 2014.

THEODORO JR., Humberto. *Comentários ao novo Código Civil*. Rio de Janeiro: Forense, v. III, t. II, 2003.

VIRILIO, Paul. *A bomba informática*. São Paulo: Estação Liberdade, 1999.