Universidade do Estado do Rio de Janeiro
Centro de Ciências Sociais
Faculdade de Direito

Rodrigo Dias de Pinho Gomes

Big data: desafios à tutela da pessoa humana na sociedade da informação

Rio de Janeiro
2017

Rodrigo Dias de Pinho Gomes

Big data: desafios à tutela da pessoa humana na sociedade da informação

Dissertação apresentada ao Programa de Pós-graduação *Stricto Sensu* da Faculdade do Estado do Rio de Janeiro como requisito para a obtenção do grau de Mestre em Direito Civil. Área de Concentração: Pensamento Jurídico e Relações Sociais. Linha de Pesquisa: Direito Civil.

Orientador: Prof. Dr. Carlos Affonso Souza

Rio de Janeiro

2017

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

G633 Gomes, Rodrigo Dias de Pinho.

Big data: desafios à tutela da pessoa humana na sociedade da informação / Rodrigo Dias de Pinho Gomes. - 2017.
145f.
Orientador: Prof. Dr. Carlos Affonso Souza.

Dissertação (Mestrado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito.

1. Direito civil - Teses. 2. Proteção de dados –Teses. 3. Consentimento (Direito) – Teses. I. Souza, Carlos Affonso. II. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. III. Título.

CDU 342.7

Bibliotecária: Marcela Rodrigues de Souza CRB7/5906

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta tese, desde que citada a fonte.

_____ _____

Assinatura Data

Rodrigo Dias de Pinho Gomes

Big data: desafios à tutela da pessoa humana na sociedade da informação

Dissertação apresentada, ao Programa de Pós-graduação *Stricto Sensu* da Faculdade do Estado do Rio de Janeiro como requisito para a obtenção do grau de Mestre em Direito Civil. Área de concentração: Pensamento Jurídico e Relações Sociais. Linha de Pesquisa: Direito Civil.

Aprovada em 20 de fevereiro de 2017.

Banca Examinadora:

_____

Prof. Dr. Carlos Affonso Souza (orientador)

Faculdade de Direito – UERJ

_____

Prof. Dr. Ronaldo Lemos

Faculdade de Direito – UERJ

_____

Prof. Dr. Sergio Branco

Faculdade de Direito – Instituto Brasileiro de Mercado de Capitais - IBMEC-RJ

Rio de Janeiro

2017

RESUMO

GOMES, Rodrigo Dias de Pinho. *Big data*: desafios à tutela da pessoa humana na sociedade da informação. 2017. 145 f. Dissertação (Mestrado em Direito Civil) – Faculdade de Direito. Universidade do Estado do Rio de Janeiro. Rio de Janeiro. 2017.

O crescimento da dados gerados a cada dia impulsiona novas formas de coleta, armazenamento e tratamento de dados pessoais. Na chamada sociedade da informação, o tratamento de grande volume de dados (big data) viabiliza que corporações e governos possam captar, analisar e armazenar enormes bancos de dados, extraindo benefícios, gerando riquezas e promovendo avanços sociais. Ao lado dos benefícios trazidos pelo big data, esta prática pode ocasionar violações aos direitos da personalidade, especialmente à privacidade e na proteção dos dados pessoais. Pretende-se analisar modelos regulatórios da privacidade e do consentimento para o tratamento dos dados pessoais em tempos de big data, demonstrando ainda propostas doutrinárias e legislativas capazes de compatibilizar esta prática com os direitos da personalidade, levando em consideração a necessidade de tutelar integralmente a pessoa humana e a autodeterminação informativa. Procura-se, por fim, analisar o cenário brasileiro à luz das experiências internacionais, para buscar compreender a direção para a qual se orientam as futuras reformas legislativas pelas quais o Brasil precisará passar para promover os objetivos acima indicados.

Palavras-chave: Direito civil. Proteção de dados pessoais. Consentimento. Autodeterminação informativa. Direitos da personalidade. Privacidade.

ABSTRACT

GOMES, Rodrigo Dias de Pinho. *Big data*: challenges to the protection of the human person in the information society. 2017. 145 f. Dissertation (Masters degree in Civil Law) – Law Faculty. University of Estado do Rio de Janeiro. Rio de Janeiro. 2017.

The growth of the data generated every day drives new ways of collecting, storing and processing personal data. In the so-called information society, large data processing enables corporations and governments to capture, analyze and store huge databases, extracting benefits, generating wealth and promoting social advancement. Beside the benefits brought by big data, this practice can lead to violations of the rights of the personality, especially privacy and protection of personal data. The intention is to analyze regulatory models of privacy and consent regarding the treatment of personal data in the big data era, demonstrating also doctrinal and legislative proposals capable of making this practice compatible with the rights of the personality, taking into account the need to fully protect the person and information self-determination. Finally, this dissertation seek to analyze the Brazilian scenario in the light of international experiences, in order to understand the direction for the future legislatibe reforms that Brazil must aprove to in order to promote the above objectives.

Keywords: Civil law. Protection of personal data. Consent. Informational self-determination. Personality rights. Privacy.

SUMÁRIO

	INTRODUÇÃO	7
1	**O TRATAMENTO DE GRANDES VOLUMES DE DADOS E SEUS IMPACTOS**	12
1.1	**Contextualizando o tratamento de grandes volumes de dados**	12
1.1.1	Definição de *big data*	19
1.2	**Os benefícios do *big data***	24
1.2.1	Funcionalidade de aplicativos	24
1.2.2	Impactos no setor de saúde	28
1.2.3	Agricultura de precisão	30
1.3	**O outro lado da moeda: os riscos do *big data***	33
1.3.1	Discriminação	39
1.3.2	Monitoramento e vigilantismo	43
1.3.3	*Big data* e o sistema de crédito social Chinês	46
1.3.4	Os dados pessoais são o novo petróleo?	48
2	***BIG DATA* E A PROTEÇÃO DOS DADOS PESSOAIS**	51
2.1	**Da privacidade aos dados pessoais – evolução histórica**	51
2.1.1	Privacidade como isolamento	51
2.1.2	Tutela dos dados pessoais	54
2.2	**Modelos de proteção dos dados pessoais**	56
2.2.1	O cenário europeu de proteção de dados	57
2.2.2	A proteção dos dados pessoais nos EUA	68
2.3	**Aplicação dos diferentes modelos de proteção**	73
2.3.1	Consentimento e *big data*	73
2.3.2	Responsabilidade e transparência	86
2.3.3	Um exemplo de mudança do paradigma	89
3	**A REGULAÇÃO DO *BIG DATA* NO BRASIL**	94
3.1	**O cenário legislativo nacional sobre proteção de dados**	94
3.1.1	O Marco Civil da Internet e sua regulamentação	97
3.1.2	Projetos de Lei sobre proteção de dados	102

3.2 **O Brasil na encruzilhada: para onde caminha a proteção de dados no País?** 106
CONCLUSÃO 120
REFERÊNCIAS 123

INTRODUÇÃO

Atualmente, metade da população mundial[1] utiliza a Internet[2], ao passo que o tráfego de dados pela rede cresce a taxas de dois dígitos por ano[3], com 90% destes gerados nos últimos 2 anos, na velocidade de 2,5 quintilhões de bytes por dia.[4] Os usuários passam em média 4 horas por dia diante da tela de seus aparelhos móveis, resultando em mais de 3 bilhões de fotos enviadas e compartilhadas em redes sociais[5], juntamente com 200 horas de vídeo a cada minuto.[6]

A internet não mais representa um luxo ou privilégio, versando, especialmente para as novas gerações, do epicentro do mundo, onde se estabelece e se cultivam amizades, onde livros e filmes são escolhidos e consumidos, onde o engajamento político se organiza e ganha força, e sobretudo, local no qual os dados pessoais são criados e arquivados.[7]

---

1 População mundial é de 7.3 bilhões de pessoas, de acordo a Organização das Nações Unidas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *World population 2015*. Disponível em: <http://esa.un.org/unpd/wpp/Publications/Files/World_Population_2015_Wallchart.pdf>. Acesso em: 20 jan. 2016).

2 INTERNATIONAL TELECOMMUNICATION UNION (ITU). *ICT Facts & Figures 2015*: The world in 2015. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>. Acesso em: 28 ago. 2015.

3 O tráfego de dados pela internet cresceu 31% em 2012, 24% em 2013 e 21% em 2014. Quando considerado apenas a utilização de dispositivos móveis, este volume cresceu 57% em 2012, 62% em 2013 e 64% em 2014. Somente pelo aplicativo WhatsApp, mais de 30 bilhões de mensagens são enviadas todos os dias. (KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 jan. 2016).

4 INTERNATIONAL BUSINESS MACHINES (IBM). *Bringing big data to the enterprise*: What is big data? Disponível em: <https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>. Acesso em: 06 ago. 2016.

5 KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 09 ago. 2016.

6 WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 jan. 2016.

7 GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.5-6.

Some-se isso a 10 bilhões[8] sensores conectados à rede mundial de computadores, capazes de captar, transmitir e analisar dados, já fazendo parte do cotidiano da sociedade contemporânea, em cenário similar ao retratado nos filmes de ficação científica, que até pouco tempo descreviam um futuro distante. Respeitáveis previsões dão conta da existência de 1 trilhão de sensores inteligentes em funcionamento no ano de 2025[9], cuja atividade movimentará mais de 1 trilhão de dólares.[10]

No ano de 2012, durante o Fórum Econômico Mundial realizado em Davos, reunindo as mais altas autoridades públicas e maiores líderes empresariais no planeta, um dos mais relevantes painéis lançou o *big data* como tema chave[11], levando à afirmação, meses depois, pelo New York Times, que vivemos na era do *big data*.[12]

O *big data* retrata uma nova forma de captar, analisar, armazenar, extrair valor de grande quantidade de informações, possibilitando, dentre outros, a tomada de decisões automatizadas, aumento na eficiência empresarial e governamental, criando novos modelos de negócios e gerando substancial riqueza, além de economia de preciosos recursos.

Representa, portanto, algo sem precedentes na história da humanidade, cuja relevância foi comparada ao iluminismo[13], funcionando ainda como verdadeiro

---

8 ABIRESEARCH. *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*. London, United Kingdom, 09 May 2013. Disponível em: <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/>. Acesso em: 04 ago. 2015.

9 PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.85-176, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015.

10 *"The latest Machina Research report predicts the M2M market will grow from $200bn in 2011 to $1.2 trillion in 2022."* (ZDNET. *M2M and the Internet of Things*: A guide. Disponível em: <http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide/>. Acesso em: 25 jun. 2015). Tradução livve: "O último relatório da Machina Research prevê que o mercado M2M crescerá de US $ 200 bilhões em 2011 para US $ 1,2 trilhão em 2022."

11 WORLD ECONOMIC FORUM. *Big Data, Big Impact*: New Possibilities for International Development. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em: 02 jan. 2017.

12 LOHR, Steve. The Age of Big Data. *The New York Times*, Feb. 2012. Disponível em: <http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0>. Acesso em: 10 ago. 2016.

13 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.96.

combustível[14] para técnicas revolucionárias, como a inteligência artificial, algo que só tornou possível diante do constante barateamento e da onipresença da tecnologia na sociedade da informação.

Apesar dos sedutores benefícios trazidos por esta tecnologia imprevista e verdadeiramente desruptiva, que melhora a funcionalidade de aplicativos, gera bilhões de economia para sistemas de saúde, possibilita maior eficiência na agricultura, lançam-se diversos questionamentos diante da sua utilização desenfreada e, acima de tudo, desregulada, não sendo poucas as situações onde os direitos da personalidade restaram violados, especialmente no tocante à privacidade, posto que seu principal insumo consiste na utilização massiva de dados pessoais.

As revelações de Edward Snowden sobre coleta de dados sem precedentes[15] pelo sistema de inteligência norte-americano, que contemplava ainda espionagem diplomática e financeira[16], o tratamento de dados pessoais por empresas de tecnologia como um verdadeiro ativo financeiro em troca por um serviço supostamente gratuito, o sistema de crédito social chinês[17], são todos exemplos claros no sentido de que a privacidade está em momento de verdadeira tensão, especialmente naquilo que se refere ao controle dos dados pessoais, cuja tutela jurídica foi concebida em uma realidade social e tecnológica diversa da atual.

---

14 *"Artificial intelligence and complex algorithms in general, fueled by big data and deep-learning systems, are quickly changing how we live and work – from the news stories we see, to the loans for which we qualify, to the jobs we perform."* (KNIGHT FOUNDATION. *Knight Foundation, Omidyar Network and Linkedin Founder Reid Hoffman Create $27 Million Fund to Research Artificial Intelligence for the Public Interest*. Jan. 2017. Disponível em: <http://www.knightfoundation.org/press/releases/knight-foundation-omidyar-network-and-linkedin-founder-reid-hoffman-create-27-million-fund-to-research-artificial-intelligence-for-the-public-interest>. Acesso em: 11 jan. 2017). Tradução livre: "A inteligência artificial e os algoritmos complexos em geral, alimentados por big data e sistemas de aprendizagem profunda, estão mudando rapidamente a forma como vivemos e trabalhamos – desde as notícias que vemos, até os empréstimos para os quais nos qualificamos e os empregos que desempenhamos."

15 Em 2013, apenas em um periodo de 30 dias, mais de 97 bilhões de emails e 124 bilhões de registros de chamadas telefônicas foram interceptados e arquivados pela National Secuity Agency dos Estados Unidos da América, tendo significativa parte destas dados captados de brasileiros. (GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.92).

16 Ibid., p.94.

17 DENYER, Simon. China wants to give all of its citizens a score: and their rating could affect every area of their lives. *Independent*, Oct. 2016. Disponível em: <http://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html>. Acesso em: 13 nov. 2016.

Gustavo Tepedino, em recente reflexão sobre as novas tecnologias, registou esta preocupação:

> Surgem a cada dia questões inovadoras, sequer cogitadas pelo legislador, muito distantes das previsões abstratas pretensamente capazes de regular o comportamento social. Basta pensar no impacto das tecnologias de captação, armazenamento e divulgação de imagens na tutela da personalidade; [...][18]

Diante das breves consirações acima expostas, pretende-se pela presente obra analisar os contornos do *big data*, verificar alguns de seus benefícios e os riscos à pessoa humana, com ênfase na privacidade, especificamente no tocante aos dados pessoais.

Para a melhor exposição e compreensão do tema, o estudo é dividido em três capítulos.

No primeiro capítulo se pretende contextualizar o tratamento de grande volume de dados, trazendo definições do que é *big data*, elencar os benefícios decorrentes da prática, como na funcionalidade de aplicativos, os impactos no setor da saúde e a melhora da eficiência na agricultura. Serão demonstrados também alguns de seus riscos, tais como a possibilidade de práticas danosas aos direitos da personalidade, ações discriminatórias, monitoramento e vigilantismo, fornecendo exemplos, como o sistema de crédito social Chinês.

Já no segundo capítulo será analisada a tutela da privacidade, voltada aos dados pessoais, compreendendo a evolução histórica até o seu atual significado, bem como elencar a forma de tutela no Brasil, analisando ainda a tutela da privacidade e dados pessoais na Europa e nos Estados Unidos da América, de forma a traçar algumas similaridades e antíteses entre o Brasil e os sistemas. Será feita breve explanação acerca de diferentes modelos de proteção, analisando o *big data* à luz do consentimento, com análise crítica sobre o aludido instituto, mencionando ainda sugestões doutrinarias versando sobre maior ênfase à responsabilização dos

---

[18] TEPEDINO, Gustavo. O papel atual da doutrina do direito civil entre o direito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Coord.). *O direito civil entre o sujeito e a pessoa*: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p.29.

agentes e dever de transparência no tratamento de dados pessoais, concluindo o capítulo com um exemplo de mudança de paradigma no sistema jurídico brasileiro.

O terceiro e último capítulo tem como tema a análise da regulamentação do *big data* no Brasil, verificando na legislação nacional quais os dispositivos aplicáveis, com especial atenção ao Marco Civil da Internet e sua regulamentação, além dos mais relevantes Projetos de Lei em trâmite no Congresso nacional, terminando com possíveis rumos a serem seguidos pelo cenário jurídico pátrio sobre o tema.

1 O TRATAMENTO DE GRANDES VOLUMES DE DADOS E SEUS IMPACTOS

1.1 Contextualizando o tratamento de grandes volumes de dados

Captar, armazenar e analisar dados não é algo novo. Aliás, historiadores[19] defendem que a escrita foi inventada pelos Sumérios por volta do ano de 3.000 A.C. com o objetivo[20] de guardar e controlar informações. A coleta de informações e seu armazenamento se transformaram ao logo da história. Na idade contemporânea, empresas e governos dedicam-se cada vez mais a gerar técnias e métodos com este intento, como por exemplo, o último censo[21] realizado no Brasil, que captou dados de mais de 67 milhões de domicílios em 5.565 cidades.

Ocorre que, diante do grande crescimento do número de pessoas e dispositivos conectados à rede mundial de computadores e do exponencial barateamento dos custos para armazenamento de dados, a quantidade de informação gerada e armazenada não para de crescer a cada dia.[22]

Segundo pesquisa realizada pela União Internacional de Telecomunicações – agência especializada do tema nas Nações Unidas, atualmente existem 3.2 bilhões

---

19 KRAMER, Samuel Noah. *The Sumerians*: Their History, Culture, and Character. Chicago: University of Chicago Press, 1963. p.302.

20 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.14.

21 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Censo 2010*. Disponível em: <http://censo2010.ibge.gov.br/resultados.html>. Acesso em: 11 ago. 2016.

22 O tráfego de dados pela internet cresceu 31% em 2012, 24% em 2013 e 21% em 2014. Quando considerado apenas a utilização de dispositivos móveis, este volume cresceu 57% em 2012, 62% em 2013 e 64% em 2014. Somente pelo aplicativo WhatsApp, mais de 30 bilhões de mensagens são enviadas todos os dias. (KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 jan. 2016).

de pessoas utilizando a Internet em todo o planeta[23], demonstrando que quase metade da população mundial[24] dispõe de conexão à rede.

Estatísticas da IBM[25] revelam que 90% dos dados disponíveis em todo o mundo foram gerados nos últimos 2 anos, na velocidade de 2,5 quintilhões de bytes de dados por dia. Significativa parcela dos dados disponíveis na rede são voluntariamente compartilhados pelos próprios usuários, que passam em média 4 horas por dia[26] diante da tela de seus aparelhos móveis: diariamente, mais de 3 bilhões de fotos são enviadas e compartilhadas em redes sociais[27], juntamente com 200 horas de vídeo a cada minuto[28], e mais de 14 milhões de avaliações escritas são submetidas pelos usuários para o aplicativo *Airbnb* em um período de 12 meses.[29]

Além de pessoas criando conteúdo refletido em dados disponíveis na internet, vivemos a era da Internet das Coisas, ou *Internet of Things*[30], o que significa dizer

---

23 INTERNATIONAL TELECOMMUNICATION UNION (ITU). *ICT Facts & Figures 2015*: The world in 2015. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>. Acesso em: 28 ago. 2015.

24 População mundial é de 7.3 bilhões de pessoas, de acordo a Organização das Nações Unidas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *World population 2015*. Disponível em: <http://esa.un.org/unpd/wpp/Publications/Files/World_Population_2015_Wallchart.pdf>. Acesso em: 20 jan. 2016).

25 INTERNATIONAL BUSINESS MACHINES (IBM). *Bringing big data to the enterprise*: What is big data? Disponível em: <https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>. Acesso em: 06 ago. 2016.

26 KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 09 ago. 2016.

27 KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 09 ago. 2016.

28 WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 jan. 2016. Apenas na rede social facebook, os seus mais de 1 bilhão de usuários enviam por volta de 350 milhões de fotos por dia. (WISHPOND. *41 Up-to-Date Facebook Facts and Stats*. Disponível em: <http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats>. Acesso em: 22 jan. 2016).

29 KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 jan. 2016.

30 O termo *"Internet of Things"* foi criado em 1999 por Kevin Ashton, gerente de marcas, à época, da multinacional Procter & Gamble. Ashton inventou a expressão quando preparava uma apresentação à sua equipe, cujo objetivo era tornar mais eficiente a distribuição dos produtos no mercado. (ASHTON, Kevin. That 'Internet of Things' Thing. *RFID Journal Live*, June 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: 25 jun. 2015).

que sensores de todos as formas se encontram espalhados no ambiente, captando grande quantidade de dados como imagens, temperatura, localização, dentre outros.[31]

Este cenário, intimamente ligado ao *big data*[32], não retrata um filme de ficção científica, muito pelo contrário, pois já se reflete em uma realidade empresarial[33], residências automatizadas[34] e locais públicos[35], propiciado sobretudo pelo barateamento

---

31 *"What does Internet of Things (IoT) mean? The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it also may include other sensor technologies, wireless technologies or QR codes."* (TECHOPEDIA. *Internet of Things (IoT)*. Disponível em: <http://www.techopedia.com/ definition/ 28247/internet-of-things-iot>. Acesso em: 04 ago. 2015). Tradução livre: "O que a Internet das Coisas (IoT) significa? A Internet das Coisas (IoT) é um conceito de computação que descreve um futuro onde objetos físicos cotidianos estarão conectados à Internet e poderão se identificar com outros dispositivos. O termo está intimamente identificado com a RFID como o método de comunicação, embora também possa incluir outras tecnologias de sensores, tecnologias sem fio ou códigos QR."

32 *"Big data is closely connected to the Internet of Things."* (HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.99). Tradução livre: "Big data está intimamente conecatado com a Internet das Coisas."

33 *"The Internet of Everything (IoE) is having an enormous impact on business. This phenomenon is completely reinventing the way businesses operate. It is bringing productivity and competitiveness to higher levels along with opening up many doors to new and exciting opportunities."* (TECHOPEDIA. *Internet of Things (IoT)*. Disponível em: <http://www.techopedia.com/definition/ 28247/internet-of-things-iot>. Acesso em: 04 ago. 2015). Tradução livre: "A Internet de Tudo (IoE) está tendo um enorme impacto nos negócios. Este fenômeno é completamente reinventar a forma como as empresas operam. Ele está trazendo produtividade e competitividade para níveis mais elevados, além de abrir muitas portas para novas e excitantes oportunidades."

34 *"But Brillo isn't just Brillo – it's also Weave, a communication layer that will enable IoT devices to talk to one another, the cloud, and of course, your phone. Pichai says Weave gives the growing world of connected, smart devices a common language. The actions each of these things is responsible for – smart ovens change temperatures, smart doors unlock and lock – won't be so singular."* (WIRED. *The Internet of Everything Will Impact Everything, Including Your Next Tech Job*. Disponível em: <http://www.wired.com/2015/02/internet-of-everything-your-next-tech-job/>. Acesso em: 04 ago. 2015). Tradução livre: "Mas Brillo não é apenas Brillo - é também Weave, uma camada de comunicação que permitirá que dispositivos IoT conversem entre si, com a nuvem e, claro, com o seu telefone. Pichai diz que o Weave dá ao mundo crescente de dispositivos conectados e inteligentes uma linguagem comum. As ações de cada uma dessas coisas é responsável por – fornos inteligentes mudarem as temperaturas, portas inteligentes abrirem e fechar – ser tão singular."

35 *"Governments are deploying sensors to alert them to failed street lights, leaks in water systems, and full trash cans. Sensors will likely have a major role in traffic control, fighting forest fires and landslide detection."* (THIERER, Adam. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. p.15-16. Disponível em: <http://jolt.richmond.edu/v21i2/article6.pdf>. Acesso em: 04 ago. 2015). Tradução livre: "Os governos estão implantando sensores para alertá-los para falha na sinalização de trânsito, vazamentos em sistemas de água e latas de lixo cheias. Sensores provavelmente terão um papel importante no controle de tráfego, combate a incêndios florestais e detecção de deslizamento de terra."

dos sensores[36] e demais *hardwares*, das conexões em alta velocidade e do armazenamento e circulação de dados na nuvem.[37]

Percebe-se que a difusão em larga de escala de dispositivos conectados pela internet, captando, analisando e armazenando grande quantidade de dados, estabelecendo conexões entre si e realizando tarefas de maneira autônoma, deu início a uma verdadeira revolução digital[38] e comportamental[39], abrindo novas

---

36 *"Microelectromechanical systems (MEMS) sensors translate physical phenomenon, such as movement, heat, pressure, or location, into digital information. MEMS were developed in the 1980s, but in the last few years the cost of such sensors has dropped from twenty-five dollars to less than a dollar per unit. These sensors are thus no longer the stuff of experimental laboratories; they are incorporated into consumer products available at scale. Some estimate that by 2025 over one trillion sensor-based devices will be connected to the Internet or each other."* (PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.85-176, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015). Tradução livre: "Os sensores de sistemas microelectromecânicos (MEMS) traduzem fenômeno físico, como movimento, calor, pressão ou localização, em informações digitais. MEMS foram desenvolvidos na década de 1980, mas nos últimos anos o custo de tais sensores caiu de vinte e cinco dólares para menos de um dólar por unidade. Estes sensores não são mais o material de laboratórios experimentais; Eles são incorporados em produtos de consumo disponíveis em escala. Alguns estimam que em 2025 mais de um trilhão de dispositivos baseados em sensores serão conectados à Internet ou uns aos outros."

37 *"Yet that impressive growth is about to be overshadowed as the things around us start going online as well, part of what is called 'the Internet of Things.' Thanks to advances in circuits and software, it is now possible to make a Web server that fits on (or in) a fingertip for $1."* (GERSHENFELD, Neil; VASSEUR, J. P. *As objects go online*. Foreign Affairs. Disponível em: <http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/asobjects-go-online>. Acesso em: 26 maio 2015). Tradução livre: "No entanto, esse crescimento impressionante está prestes a ser ofuscado na medida em as coisas em torno de nós começam a ficar on-line também, parte do que é chamado de" Internet das Coisas ". Graças aos avanços em circuitos e software, agora é possível fazer um servidor Web que se cabe na ponta do dedo por US$1."

38 *"Together, these consumer products fundamentally change our knowledge of self, other, and environment."* (PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.85-176, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015). Tradução livre: "Juntos, esses produtos de consumo mudam fundamentalmente nosso conhecimento de nós mesmos, dos outros e do meio ambiente."

39 *"The dramatic rise of smart machines and autonomous devices is driving radical shifts in business practices and individual behaviors."* (GARTNER. *Top Strategic Predictions for 2016 and Beyond*: The Future Is a Digital Thing. Disponível em: <https://www.gartner.com/doc/3142020?refval=&pcp=mpe>. Acesso em: 09 ago. 2016). Tradução livre: "O aumento dramático de máquinas inteligentes e dispositivos autônomos está conduzindo mudanças radicais nas práticas de negócios e comportamento dos indivíduos."

oportunidades de negócios[40] e sobretudo desafiando a sociedade e, consequentemente, o Direito.[41,42]

Para ser ter uma singela noção da onipresença[43] destes produtos componentes do universo da Internet das Coisas, em 2012 foram baixados 44 milhões de aplicativos para monitoramento de dados vitais e médicos[44], com previsão de aumento para 142 milhões em 2016.[45] Quase 30 milhões de pulseiras inteligentes – como exemplo FitBit/Nike+ Fuel Band – foram vendidas em 2012.[46]

Esta nova realidade digital caminha a passos largos[47] e se revela um verdadeiro caminho sem volta[48], conforme já se afirmou:

---

40 *"The latest Machina Research report predicts the M2M market will grow from $200bn in 2011 to $1.2 trillion in 2022."* (ZDNET. *M2M and the Internet of Things*: A guide. Disponível em: <http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide/>. Acesso em: 25 jun. 2015). Tradução livre: "O último relatório da Machina Research prevê que o mercado M2M crescerá de US $ 200 bilhões em 2011 para US $ 1,2 trilhão em 2022."

41 TEPEDINO, Gustavo. O papel atual da doutrina do direito civil entre o direito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Coord.). *O direito civil entre o sujeito e a pessoa*: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p.29.

42 *"In AmI enviroments where people and items are connected to each other and are always online will be more difficult to apply the principle of reasonable expectations of privacy."* (MONTELEONE, Shara. Ambient Intelligence: Legal Challenges and Possible Directions for Privacy Protection. In: AKRIVOPOULOU, Christina. *Personal data privacy and protection in a surveillance era*: technologies and practices. Hershey, PA: Information Science Reference, 2011. p.213). Tradução livre: "Em ambientes AmI onde as pessoas e itens estão conectados uns aos outros e estão sempre on-line será mais difícil aplicar o princípio de expectativas razoáveis de privacidade."

43 *"In our increasingly networked world, the building blocks of big data are everywhere."* (WHITE HOUSE. *Big Data*: A Report on Algorithmic Systems, Opportunity, and Civil Rights. Executive Office of the President. May 2016. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Acesso em: 29 ago. 2016). Tradução livre: "Em nosso mundo cada vez mais em rede, os blocos de construção do big data estão em toda parte."

44 Chamados *mobile health-care and medical apps*.

45 MARKET WIRED. *Mobile Healthcare and Medical App Downloads to Reach 44 Million Next Year, Rising to 142 Million in 2016, Finds Juniper Research Limited*. Nov. 2011. Disponível em: <http://www.marketwired.com/press-release/mobile-healthcare-medical-app-downloads-reach-44-million-next-year-rising-142-million-1591994.htm>. Acesso em: 06 ago. 2015.

46 ABIRESEARCH. *Sports and Wellness Drive Health Device Shipments to Nearly 30 Million in 2012*. New York, Dec. 2012. Disponível em: <https://www.abiresearch.com/press/sports-and-wellness-drive-mhealth-device-shipments/>. Acesso em: 06 ago. 2015.

47 *"ABI Research's latest data on the Internet of Everything (IoE) shows that there are more than 10 billion wirelessly connected devices in the market today; with over 30 billion devices expected by 2020."* (ABIRESEARCH. *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*. London, United Kingdom, 09 May 2013. Disponível em:

> *Target knows. Apple Computer knows, too. So do LinkedIn, Netflix, Facebook, Twitter, Expedia, national and local political campaigns, and dozens of other organizations that all generate enormous economic, social, and political value. They know that that the age of Big Data is here and it's here to stay*.[49]

Diante deste quadro, questionamentos diversos[50] são lançados pela utilização destas tecnologias[51], especialmente diante dos enormes bancos de dados captados, armazenados e analisados por governos, pessoas físicas e jurídicas.

<https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/>. Acesso em: 04 ago. 2015). Tradução livre: "Os dados mais recentes da ABI Research sobre a Internet de Tudo (IoE) mostram que há mais de 10 bilhões de dispositivos conectados sem fio no mercado hoje; Com mais de 30 bilhões de dispositivos previstos para 2020." Ainda neste sentido: *"We predict, for example, that in 2016 spending on new Internet of things (IoT) hardware will exceed $2.5 million a minute. And, as mind boggling as that number is, it pales in comparison with the corresponding prediction that, by 2021, 1 million IoT devices will be purchased and installed every single hour."* (GARTNER. *Top Strategic Predictions for 2016 and Beyond*: The Future Is a Digital Thing. Disponível em: <https://www.gartner.com/doc/3142020?refval=&pcp=mpe>. Acesso em: 09 ago. 2016). Tradução livre: "Predizemos, por exemplo, que em 2016 os gastos com novos hardwares de Internet de coisas (IoT) excederão US $ 2,5 milhões por minuto. E, por mais alucinante como esse número possa parecer, ele empalidece em comparação com a previsão correspondente que, em 2021, 1 milhão de dispositivos IoT serão comprados e instalados a cada hora."

48 *"We'd better start thinking long and hard about what it means for human beings to lose the ability – practically speaking – to go offline."* (THE GUARDIAN. *Will the internet of things result in predictable people?* Aug. 2015. Disponível em: <http://www.theguardian.com/technology/2015/aug/10/internet-of- things-predictable-people>. Acesso em: 14 ago. 2015). Tradução livre: "É melhor começar a pensar longamente sobre o que significa para os seres humanos perder a capacidade – praticamente falando – para ficar offline."

49 DAVIS, Kord; PATTERSON, Doug. *Ethics of Big Data*. Sebastopol: O'Reilly Media, 2012. p.1. Tradução livre: "Target sabe. A Apple Computer também sabe. E também, LinkedIn, Netflix, Facebook, Twitter, Expedia, campanhas políticas nacionais e locais e dezenas de outras organizações que geram enormes valores econômicos, sociais e políticos. Eles sabem que a idade da Big Data está aqui e está aqui para ficar."

50 *"As with other new and highly disruptive digital technologies, however, IoT and wearable technology will challenge existing social economic, and legal norms."* (THIERER, Adam. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. Disponível em: <http://jolt.richmond.edu/v21i2/article6.pdf>. Acesso em: 04 ago. 2015). Tradução livre: "Como com outras tecnologias digitais novas e altamente disruptivas, entretanto, a IOT e a tecnologia wearable desafiarão as normais sociais, econômicas e legais existentes."

51 *"Apple lags behind Google, Facebook, and even Microsoft in the new battle for user attention: Prediction. A combination of several factors, including the prevalence of devices, sensors, and, by extension, data has made it harder than ever for people to stay on top of their digital lives."* (QUARTZ. *Why Apple is suddenly so obsessed with your privacy*. Disponível em: <http://qz.com/423320/apple-is-lagging-behind-google-in-context-so-its-fighting-back-with-privacy/. Acesso em: 25 jun. 2015). Tradução livre: "Apple fica atrás do Google, Facebook e até mesmo Microsoft na batalha para a atenção do novo usuário: Previsão. A combinação de vários fatores, incluindo a prevalência de dispositivos, sensores e, por extensão, os dados tornou mais difícil do que nunca para as pessoas a permanecer no topo de suas vidas digitais."

Esta explosão de informações, sem qualquer precedente na história da humanidade, como dito, vem gerando interesse de governos e empresas na utilização destes dados disponíveis para os mais variados fins, especialmente diante da tecnologia ubíqua[52] que as coleta, armazena e analisa. Afirma-se, portanto, que vivemos uma verdadeira era[53] do *big data*, onde a sua utilização é cada vez mais ampla, conforme recente constatação: *"[...] the technological trends of always-on networked devices, ubiquitous data collection, cheap storage, sensors, and computing power, will spur broader use of big data"*.[54]

Conforme se vê, novos modelos de negócios, especialmente na internet, culminam no desafio de uma miríade de institutos jurídicos, dentre eles, por exemplo, o consentimento, a privacidade e os dados pessoais, bem como a responsabilidade civil.

Durante o I Congresso Internacional de Direito Civil-Constitucional da Cidade do Rio de Janeiro, realizado entre os dias 21 e 23 de setembro de 2006 no Rio de Janeiro, Gustavo Tepedino, Maria Celina Bodin de Moraes e doutrinadores estrangeiros sintetizaram grande parte destes desafios:

---

52 WEISER, Mark. The computer for the 21st century. *Scientific American*, v.265, n.3, p.66-75, Sept. 1991. Vale ainda destacar: *"The ubiquity of computing and electronic communication technologies has led to the exponential growth of data from both digital and analog sources."* (WHITE HOUSE. *Big Data and Privacy: A Technological Perspective.* Executive Office of the President President's Council of Advisors on Science and Technology, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em: 10 set. 2016). Tradução livre: "A ubiqüidade das tecnologias de computação e comunicação eletrônica levou ao crescimento exponencial de dados de fontes digitais e analógicas."

53 *"We live in an age of 'big data'. Data has become the raw material of production, a new source of immense economic and social value."* (TENE, Omer; POLONETSKY, Jules. Privacy in The Age of Big Data: A Time for Big Decisions. (September 2, 2012). *Stanford Law Review*, v.64, n.63, 2012. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data>. Acesso em: 20 fev. 2016). Tradução livre: "Vivemos na era de 'big data'. Os dados se tornaram a matéria-prima da produção, uma nova fonte de imenso valor econômico e social." Ainda neste sentido: *"The era of big data has begun."* (BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016). Tradução livre: "A era do big data começou." *"Welcome to the Age of big data."* (LOHR, Steve. The Age of Big Data. *The New York Times*, Feb. 2012. Disponível em: <http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0>. Acesso em: 10 ago. 2016). Tradução livre: "Bem-vindo à era do big data."

54 WHITE HOUSE. *Big Data*: A Report on Algorithmic Systems, Opportunity, and Civil Rights. Executive Office of the President. May 2016. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Acesso em: 29 ago. 2016. Tradução livre: "[...] as tendências tecnológicas dos dispositivos sempre ligados em rede, a captação de dados onipresente, armazenamento barato, sensores e poder de computação, irão estimular o uso mais amplo do big data."

> Na agenda dos problemas contemporâneos, não escapou à refinada percepção da Professora Geneviève Viney, em sua conferência do primeiro dia, à identificação de três ordens de preocupações do direito civil atual: (i) as novas tecnologias e seus impactos na tutela da pessoa humana; [...] A primeira questão acima aludida diz respeito à exaustão das categorias jurídicas tradicionais diante da revolução tecnológica, que induz novos interesses e bens jurídicos insuscetíveis de serem tratados com base nos paradigmas do passado. O fenômeno é recorrente nos campos da engenharia genética e do ciberespaço, como ressaltou a Professora Maria Celina Bodin de Moraes, bastando pensar no conflito latente, que se intensifica no decorrer dos anos, entre, de um lado, a tutela da intimidade e da privacidade, e, de outro, o direito à informação e a autonomia privada.[55]

Para melhor compreensão destes desafios se faz necessário entender, sem pretensão de esgotar o tema, o que é *big data*, com enfoque da análise no campo da privacidade e na tutela dos dados pessoais, compreender a evolução histórica destes institutos até o seu atual significado, bem como elencar a forma de tutela no Brasil, analisando ainda a tutela da privacidade e dados pessoais na Europa e nos Estados Unidos da América, de forma a traçar algumas similaridades e antíteses entre o Brasil e os sistemas.

1.1.1 Definição de *big data*

O termo *big data* surgiu no início do século XXI[56], sendo inicialmente utilizado por astrônomos e geneticistas, em momento onde a memória dos computadores não se mostrava capaz de armazenar toda a quantidade de informação disponível, os obrigando a pensar em novas formas e instrumentos para analisar estes grandes bancos de dados.

---

55 TEPEDINO, Gustavo. O direito civil-constitucional e suas perspectivas atuais. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.8.

56 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.6.

Trata-se de uma expressão bastante ampla, vaga e imprecisa[57], muitas vezes até criticada[58], que comporta diversas interpretações e variados significados, principalmente por ser utilizada por vários setores, como especialistas em tecnologia, juristas e autoridades públicas.

Apesar de ser objeto de ampla difusão[59], não se alcançou uma definição uníssona do termo, valendo destacar algumas que servem como orientação ao presente estudo.

O professor da Universidade Oxford, Viktor Mayer-Schonberger defende que: *"big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more"*.[60]

O Instituto de Tecnologia & Sociedade do Rio o define na seguinte passagem:

> o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.[61]

---

57 *"Big data is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics."* (CRAWFORD, Kate; SCHULTZ, Jason. Big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, v.55, n.1, 2014. Disponível em: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>. Acesso em: 29 ago. 2016). Tradução livre: "Big data é um termo generalizado e impreciso, que se refere ao uso de grandes conjuntos de dados na ciência de dados e análise preditiva."

58 *"Big data is, in many ways, a poor term."* (BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, p.663, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016). Tradução livre: "big data é, em vários sentidos, um termo pobre."

59 Pesquisa pelo termo *"big data"* no google.com revela aproximadamente 263.000.000 resultados. (Acesso em: 15 ago. 2016).

60 Tradução livre: "big data refere-se a coisas que se podem fazer em grande escala, que não podem ser feitas em escala menor, de forma a extrair novas ideias ou criar novas formas de valor, de maneira que acabam mudando mercados, organizações, a relação entre os cidadãos e os governos, dentre outros." (MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.6).

61 INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. *Big data no projeto Sul Global*: relatório sobre estudos de caso. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

O Article 29 Working Party, organização de caráter consultivo e independente[62], criada pela Diretiva 95/46/EC do Parlamento Europeu, assim estabelece:

> *Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals*.[63]

Em 2001, Doug Laney[64] já previa este cenário, especialmente no campo empresarial, com o aumento crescente da relevância dos bancos de dados, lançando a pedra fundamental do que foi denominado “3 V” no universo do *big data*, ao afirmar que as companhias deveriam dar atenção especial ao substancial incremento do volume, velocidade e variedade das informações.

Volume se refere à grande quantidade de dados, velocidade seria aquela com a qual as informações são captadas e transmitidas – muitas vezes em tempo real e

---

62 *"The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently."* (EUROPEAN COMMISSION. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>. Acesso em: 30 out. 2016). Tradução livre: "O Grupo de Trabalho sobre Protecção de Dados do Artigo 29 foi criado ao abrigo da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Possui status de assessoria e age de forma independente."

63 Tradução livre: "Big data se refere ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado de informação: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grande porte, que são amplamente analisados (daí o nome: analytics) usando algoritmos de computador. Big data pode ser usado para identificar tendências mais gerais e correlações, mas também pode ser processado, de modo a afetar diretamente os indivíduos." (EUROPEAN COMMISSION. *Opinion 03/2013 on purpose limitation*. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 12 out. 2016).

64 LANEY, Doug. *3D Data Management*: Controlling Data Volume, Velocity and Variety. Feb. 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume- Velocity-and-Variety.pdf. Acesso em: 09 ago. 2016.

ininterruptamente, e variedade seria a multiplicidade de tipos de dados e fontes[65] para obtenção destes em larga escala. Em síntese: *“The evolving era of big data implies, by its very nature, a lack of control, since the volume of data is unprecedented, diverse in variety and moving with a velocity that is increasingly approaching real time”*.[66]

Afirma-se[67] ainda que, além destas três dimensões que compõem o *big data*, deve-se ainda incluir a veracidade[68] neste conjunto, pois, diante da enorme quantidade de informações contidas no banco de dados, certamente haverá dados imprecisos e até equivocados, urgindo por cautela e tecnologia de ponta para identificar e não se deixar enganar por estas imperfições.

Atualmente, não é exagero afirmar que o termo *big data* se tornou um verdadeiro jargão[69], sendo para alguns a expressão de um fenômeno[70] cultural e tecnológico.

---

65 *"Numerical data, categorical data, geospatial data, 3D data, audio and video, unstructured text, including logfiles and social media, all form part of the big data ecosystem."* (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016). Tradução livre: "Dados numéricos, dados categóricos, dados geoespaciais, dados 3D, áudio e vídeo, texto não estruturado, incluindo logs e mídias sociais, fazem parte do grande ecossistema do big data."

66 HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.96. Tradução livre: “A evolução da era do big data implica, por sua própria natureza, em falta de controle, uma vez que o volume de dados é sem precedentes, diverso em variedade e movendo-se com uma velocidade que se aproxima cada vez mais em tempo real.”

67 *"For the purpose of this report one more interesting dimension of big data is also veracity, which describes the incompleteness (inconsistency, inaccuracy) of data."* (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016). Tradução livre: "Para os propósitos deste relatório, uma outra dimensão interessante do big data é a veracidade, que descreve a incompletude (inconsistência, imprecisão) dos dados".

68 INTERNATIONAL BUSINESS MACHINES (IBM). Infographics & Animations: The Four V's of Big Data. Disponível em: <http://www.ibmbigdatahub.com/infographic/four-vs-big-data>. Acesso em: 15 ago. 2016.

69 INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. *Big data no projeto Sul Global*: relatório sobre estudos de caso. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

70 *“We define big data as a cultural, technological, and scholarly phenomenon.”* (BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, p.663, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016). Tradução livre: "Definimos big data como um fenômeno cultural, tecnológico e acadêmico."

Vale frisar que muitos dos benefícios provenientes do *big data* ocorrem através da análise e utilização secundária[71] do banco de dados, ou seja, distante da finalidade inicial para qual os dados foram coletados. Em outras palavras:

> *One of the main targets of big data analytics is to use data, alone or in combination with other data sets, beyond their original point and scope of collection. The scalability of storage allows for potential infinite space, which means that data can be collected continuously until a new value can be created from insights derived out of them*.[72]

Um exemplo contundente da utilização secundária das informações se verificou através da análise de mais de 350 milhões de tweets pela Organização das Nações Unidas, na tentativa de auxiliar o Poder Público no combate à fome em locais menos favorecidos.[73]

Sem qualquer pretensão de esgotar o tema ou oferecer uma definição jurídica precisa, parece possível entender que *big data* se refere, necessariamente, à análise

---

71 "*With big data, the value of information no longer resides solely in tis primary purpose. As we've argued, it is now in secondary uses."* (MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.153). Tradução livre: "Com o big data, o valor da informação já não reside apenas em seu propósito principal. Como argumentamos, agora está em usos secundários."

72 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016. Tradução livre: "Um dos principais objetivos da análise do big data é usar dados, isoladamente ou em combinação com outros conjuntos de dados, além de seu ponto original e escopo de coleta. A escalabilidade do armazenamento permite um potencial espaço infinito, o que significa que os dados podem ser coletados continuamente até que um novo valor possa ser criado a partir de insights derivados deles."

73 *"When correlations between social media conversations on food-related topics and official inflation data started to emerge, Jakarta's Global Pulse analysts were able to flag the likely local impacts of the crisis and deploy resources accordingly. In 2014 Global Pulse implemented over 25 joint data innovation projects worldwide. Implementation involved the analysis of over 350 million tweets."* (EVANS, Bryce. Using Big Data to Achieve Food Security. In: BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. *Big Data Challenges*: Society, Security, Innovation and Ethics. London: Palgrave Macmillan, 2016. p.129). Tradução livre: "Quando começaram a surgir correlações entre as conversas nas mídias sociais sobre tópicos relacionados com alimentos e dados oficiais sobre inflação, os analistas do Global Pulse de Jacarta puderam lidar com os prováveis impactos locais da crise e implementar recursos adequadamente. Em 2014, a Global Pulse implementou mais de 25 projetos conjuntos de inovação de dados em todo o mundo. A implementação envolveu a análise de mais de 350 milhões de tweets."

de grande quantidade de dados[74], realizada de maneira automatizada por algorítimos, por com intuito de extrair resultados e benefícios.

O acúmulo de conhecimento e informação, que um dia significou estudar, conhecer e compreender o passado, está se transformando, significando, com o *big data*, a habilidade de prever o futuro.[75]

Com isso, abre-se a possibilidade concreta de se achar a *agulha no palheiro*[76], utilizando-se de algorítimos, mecanismos de inteligência artificial, que alimentados de maneira continua com tais bancos de dados, extraem valores disso, permitindo até a tomada de decisões autônomas e fornecendo novos dados cuja análise humana jamais poderia conceber ou imaginar.

Serão demonstrados, nos itens seguintes, alguns destes benefícios.

1.2 **Os benefícios do *big data***

1.2.1 Funcionalidade de aplicativos

O simples ato, atualmente corriqueiro, de utilizar o telefone celular para realizar compras online, conversar com amigos e parentes através de redes sociais, realizar pesquisas em sites de busca, representam exemplos tangíveis de interação com o

---

74 *"Big data is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets."* (BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, p.663, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016). Tradução livre: "Big data é menos sobre dados que são grandes do que é sobre a capacidade de pesquisa, agregação e referência cruzada de grandes conjuntos de dados."

75 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.190.

76 *"However, big data changes the paradigm. One can collect large amounts of data and draw effect from it. In other words: one can find the needle in the haystack."* (HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.100). Tradução livre: "No entanto, o big data muda o paradigma. Pode-se coletar grandes quantidades de dados e desenhar efeitos a partir dele. Em outras palavras: pode-se encontrar a agulha no palheiro. "

universo do *big data*[77], culminando na melhora a funcionalidade de aplicativos em dispositivos eletrônicos, tornando mais simples, fácil e eficiente a utilização destes pelos usuários.

O *big data* torna as pesquisas no Google mais eficientes e rápidas, inclusive sugerindo termos em tempo real enquanto o usuário digita[78], denominado "preenchimento automático", pois o algoritmo do motor de pesquisa se baseia nas bilhões[79] de informações pesquisadas por outros usuários, porém filtrando e adaptando às especificidades daquele usuário específico.[80]

Quando comparada as vendas com sugestões de editores humanos com aquelas realizadas através de sugestões automatizadas por algoritmo, o segundo tem se mostrado muito mais bem sucedido em determinadas plataformas, como no website Amazon.com, onde 1/3 das transações decorrem das recomendações do próprio sistema com base na análise do perfil do usuário.[81]

---

77 PRIES, Kim; DUNNIGAN, Robert. *Big Data Analytics*: A Practical Guide for Managers. Boca Raton: Taylor & Francis Group, 2015. p.3.

78 As previsões de pesquisa vêm de: Termos que você está digitando. Aquilo que outras pessoas estão pesquisando, incluindo as tendências em pesquisas, que são histórias conhecidas na sua área que mudam ao longo do dia. As tendências em pesquisas não têm relação com seu histórico de pesquisa. Pesquisas relevantes que você fez no passado (se estiver conectado à sua Conta do Google e se a Atividade na Web e de apps estiver ativada). (GOOGLE. *Pesquisar usando o preenchimento automático*. Disponível em: <https://support.google.com/websearch/answer/106230?hl=pt-BR>. Acesso em: 21 ago. 2016).

79 O Googe recebe 40.000 pesquisas por segundo, ou 3.5 bilhões por dia. (INTERNET LIVE STATS. *Google Search Statistics*. Disponível em: <http://www.internetlivestats.com/google-search-statistics/>. Acesso em: 30 out. 2016).

80 *"It's based on analysis of the enormous dataset of everything everyone else in the world has searched for, narrowed down using personalization and location filters."* (ALL THINGS D. *Nearly a Decade Later, the Autocomplete Origin Story*: Kevin Gibbs and Google Suggest. Disponível em: <http://allthingsd.com/20130823/nearly-a-decade-later-the-autocomplete-origin-story-kevin-gibbs-and-google-suggest/>. Acesso em: 30 out. 2016). Tradução livre: "Baseia-se na análise de enormes conjuntos de dados de tudo que todos os outros no mundo tem procurado, reduzido usando filtros de personalização e localização.

81 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.51-52.

O *Spam*[82], especialmente através dos e-mails[83], vem sendo combatido de maneira cada dia mais eficaz graças ao desenvolvimento de ferramentas eletrônicas que se alimentam de grande quantidade de dados, os captando e analisando em tempo real, de forma a filtrar mensagens indesejadas.

O *Spam* constitui prática conhecida por todos que se utilizam do correio eletrônico, e que culmina em perda de produtividade, incômodos, congestionamento de servidores, e, não raro, em danos causados ao destinatário da mensagem. Se revela prática costumeira de violação da privacidade[84] na internet.

Os transtornos ocasionados não passam despercebidos pelos juristas, sendo certo que "Apesar de sua etimologia cômica, o spam consiste em um dos mais sérios inconvenientes da comunicação virtual"[85] o que gerou, em julho de 2002, a Diretiva n.º 2002/58/CE do Parlamento Europeu, que versa exclusivamente de tratamento de dados pessoais e à proteção da privacidade das comunicações

---

82 "O termo 'spam' é um neologismo surgido na esteira da popularização da Internet. Originalmente, refere-se a uma determinada marca de alimento enlatado. Não é possível precisar quando foi empregado pela primeira vez no contexto que agora examinamos: talvez em meados da década de 1980, quando um usuário de um sistema informatizado causou problemas técnicos com a repetição automática da palavra "spam" em um ambiente multi-usuário; ou então, na mesma época, alguns grupos de discussão da USENET começavam a enfrentar mensagens enviadas em massa. O que parece certo é que o termo foi inspirado em um célebre quadro do grupo humorístico Monty Python." (LEMOS, Ronaldo; DONEDA, Danilo; SOUZA, Carlos Affonso Pereira de; ROSSINI, Carolina Almeida A. *Estudo sobre a regulamentação jurídica do spam no Brasil*. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS),da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas. p.18. Disponível em: <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 18 jul. 2015). "O que caracteriza o spamming, portanto, é o fato de a mensagem não ter sido solicitada pelo internauta." (MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na internet*. São Paulo: Revista dos Tribunais, 2008. p.210).

83 "Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail)." (ANTISPAM. *O que é spam?* Disponível em: <http://www.antispam.br/conceito/> Acesso em: 23 abr. 2015).

84 "Diversas são as formas de invasão à privacidade atualmente discutidas, podendo-se destacar, para os fins desse estudo, algumas considerações sobre a utilização de cookies para o monitoramento e personalização da navegação, e posteriormente, o envio reiterado de mensagens eletrônicas (spams), como objeto do debate ora proposto e conseqüência por vezes imediata da coleta desautorizada de dados pessoais." (LEMOS et. al., op cit., p.15).

85 SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011. p. 59.

eletrônicas[86], determinando a necessidade de consentimento do indivíduo, permitido o disparo de “chamada automatizada sem intervenção humana” somente a quem expressamente autorize.[87]

Mesmo diante da ausência, no Brasil, de Lei específica[88] que impeça de maneira expressa o *Spam*, a tecnologia, através do desenvolvimento de sofisiticados algoritmos[89] que utilizam o *big data* como forma primordial de operação[90], tem se incumbido de impedir, muitas vezes com sucesso[91], o recebimento de mensagens indesejadas e consequentemente aumentando a produtividade e até impedindo violações de direitos da personalidade.

---

86 Em seu preambulo, o Parlamento Europeu pondera que “A internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infra-estrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações electrónicas. Os serviços de comunicações electrónicas publicamente disponíveis através da internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade.” Íntegra disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:pt:PDF>.

87 Artigo 13. Comunicações não solicitadas 1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrónico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio.

88 Apesar disso, renomados juristas entendem pela sua ilegalidade, por violação da privacidade, constitucional e legalmente garantia. (LEMOS, Ronaldo; DONEDA, Danilo; SOUZA, Carlos Affonso Pereira de; ROSSINI, Carolina Almeida A. *Estudo sobre a regulamentação jurídica do spam no Brasil*. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS),da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas. p.15. Disponível em: <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 18 jul. 2015).

89 LARDINOIS, Frederic. *Google Improves Gmail’s Spam Filters, Launches New Analytics Tool For Bulk Senders*. *Tech Crunch*, July 2015. Disponível em: <https://techcrunch.com/2015/07/09/google-improves-gmails-spam-filters-launches-new-analytics-tool-for-bulk-senders/>. Acesso em: 30 out. 2016.

90 *"The company credits the significant drop in large part to the introduction of brain-like “neural networks” into its spam filters that can learn to recognize junk mail and phishing messages by analyzing scads off the stuff across an enormous collection of computers."* (WIRED. *Google Says Its AI Catches 99.9 Percent of Gmail Spam*. Disponível em: <https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/>. Acesso em: 30 out. 2016). Tradução livre: "A empresa acredita a queda significativa, em grande parte, para a introdução de ‘redes neurais’ parecidas com o cérebro em seus filtros de spam que podem aprender a reconhecer correio não solicitado e mensagens de phishing, analisando scads fora do material em uma enorme coleção de computadores.”

91 "*Three years after it last released Gmail’s spam stats, Google says that its spam rate is down to 0.1 percent, and its false positive rate has dipped to 0.05 percent."* (WIRED. *Google Says Its AI Catches 99.9 Percent of Gmail Spam*. Disponível em: <https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/>. Acesso em: 30 out. 2016). Tradução livre: "Três anos depois de ter lançado as estatísticas de spam do Gmail, o Google diz que sua taxa de spam caiu para 0,1%, e sua taxa de falsos positivos caiu para 0,05%".

1.2.2 Impactos no setor de saúde

O *big data* traz benefícios de toda ordem no sistema de saúde, gerando eficiência, economia e salvando vidas, existindo diversos exemplos que comprovam esta assertiva.

Neste sentido, vale mencionar a implementação de técnicas de análise de grande quantidade de dados produzidos pelos setores público e privado, apenas nos Estados Unidos América, cujo potencial de geração de economia é estimado em até 450 bilhões de dólares[92], o que corresponde a aproximadamente 1.453.680.000.000,00 reais.[93]

Os serviços de saúde público norte-americano, denominados Medicare e Medicaid, utilizam um software que, analisando grande quantidade de informações submetidas pelos milhões de usuários do sistema, sinaliza casos prováveis de fraudes nos reembolsos solicitados, verificando pontos de convergência em pedidos comprovadamente fraudulentos.[94] O sistema de prevenção de fraude já economizou mais 115 milhões de dólares, possibilitando, inclusive, a extensão do programa de assistência até 2029.[95]

---

92 *"Overall, we believe our estimate of $300 billion to $450 billion in reduced healthcare spend could be conservative, as many insights and innovations are still ahead."* (GROVES, Peter; KAYYALI, Basel; KNOTT, David; VAN KUIKEN, Steve. The 'big data' revolution in health care: accelerating value and innovation. New York: McKinsey & Company, 2013. p.50). Tradução livre: "No geral, acreditamos que a nossa estimativa de US $ 300 bilhões a US $ 450 bilhões em redução de gastos com assistência médica poderia ser conservadora, já que muitas idéias e inovações ainda estão à frente."

93 Conversão realizada através do Banco Central do Brasil. (BANCO CENTRAL DO BRASIL. *Conversão de moedas*. Disponível em: <http://www4.bcb.gov.br/pec/conversao/conversao.asp>. Acesso em: 06 out. 2016).

94 WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 jan. 2016. Detalhes do programa: CENTER FOR MEDICARE & MEDICAID SERVICES. *Fraud Prevention Toolkit.* Disponível em: <https://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/FraudPreventionToolkit.html>. Acesso em: 18 ago. 2016.

95 *"The health care law ensures the protection of Medicare for years to come. The life of the Medicare Trust fund will be extended to at least 2029 – a 12-year extension due to reductions in waste, fraud and abuse, and Medicare costs, which will provide you with future savings on your premiums and coinsurance."* (MEDICARE. *The Affordable Care Act & Medicare*. Disponível em: <https://www.medicare.gov/about-us/affordable-care-act/affordable-care-act.html>. Acesso em: 21 ago. 2016). Tradução livre: "A *health care law* garante a proteção do Medicare nos próximos anos. A vida do fundo Medicare será estendida para pelo menos 2029 - uma extensão de 12 anos devido à redução de desperdício, fraude e abuso, e os custos do Medicare, que serão garantidos com futuras economias em seus prémios e co-seguro."

No Canadá, uma parceria[96] entre a IBM e o sistema de saúde público, compilou milhões de dados armazenados, obtidos dos aparelhos que monitoram os sinais vitais de bebês em unidades de terapia intensiva neonatal, captando e analisando mais de 1.256 informações por segundo, 24 horas por dia, o que seria humanamente impossível para qualquer profissional de saúde, por mais experiente, qualificado e dedicado que fosse.

Analisando a grande quantidade de dados obtidos, foi possível identificar diversos fatores que contribuíam para infecções, muitas vezes fatais, como aumentos de temperatura e frequência cardíaca. Diante disso, o sistema emite um sinal de alerta precoce, avisando aos médicos que uma infecção teria potencial de ocorrer naquele paciente, algo que os médicos jamais poderiam observar sem o auxílio da tecnologia, salvando vidas, otimizando recursos e melhorando a qualidade do serviço prestado à população.

Estes singelos exemplos demonstram de que maneira o *big data*, aliado à inteligência artificial, já representa uma ferramenta relevante ao sistema de saúde público e privado, revelando resultados positivos e constituindo importante método no auxílio para tomada de decisões apoiadas pela plataforma.[97]

---

96 INTERNATIONAL BUSINESS MACHINES (IBM). Disponível em: <http://www.ibm.com/smarterplanet/global/files/ca__en_us__healthcare__ca_brochure.pdf>. Acesso em: 18 ago. 2016.

97 *"For governments big data can be the basis for exponential improvements in policy-making. A telling example is health care where on the basis of large amounts of health records diseases can be detected and treated. Since not all patients are alike and individuals react differently to treatment, the use of vast amounts of data makes personalised treatment possible. Mobile devices connected to large datasets could help the detection of symptoms of illnesses."* (HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p 97). Tradução livre: "Para os governos o big data pode ser a base para melhorias exponenciais na formulação de políticas. Um exemplo revelador é o de saúde, onde, com base em grandes quantidades de registros de saúde, doenças podem ser detectadas e tratadas. Como nem todos os pacientes são iguais e os indivíduos reagem de forma diferente ao tratamento, o uso de grandes quantidades de dados torna possível o tratamento personalizado. Dispositivos móveis conectados a grandes conjuntos de dados podem ajudar na detecção de sintomas de doenças."

1.2.3 Agricultura de precisão

O crescimento populacional irá demandar, já em 2050, a necessidade de duplicação da produção de alimentos, se comparado com os índices atuais[98], para atender à demanda. Quase 1/3 dos alimentos produzidos no campo são perdidos ou descartadas durante o processo de distribuição e venda, o que revela ser um processo deveras ineficiente.[99]

Levando-se em consideração este cenário preocupante e desafiador, a tecnologia, especificamente com o *big data*, pode se transformar num dos vetores que possibilite e assegure o futuro alimentar do planeta. Aliás, a utilização do *big data* na agricultura já se mostra efetivamente presente[100], destacando-se a existência de dados científicos[101] que demonstram ser possível se alcançar as metas estabelecidas.

Ainda com base nestes desafios, a Organização das Nações Unidas, por ordem de seu secretário geral, administra programa denominado *Global Pulse*[102], cujo

---

98 FOOD AND AGRICULTURE ORGANIZATION (FAO). Disponível em: <http://www.fao.org/economic/ess/ess-home/food/en/>. Acesso em: 18 ago. 2016.

99 ROYTE, Elizabeth. How 'Ugly' Fruits and Vegetables Can Help Solve World Hunger. *National Geographic*, Mar. 2016. Disponível em: <http://www.nationalgeographic.com/magazine/2016/03/global-food-waste-statistics/. Acesso em: 18 ago. 2016.

100 *"For all the caution amongst analysts about Big Data, its use is already informing humanitarian food security initiatives of the twenty-first century."* (EVANS, Bryce. Using Big Data to Achieve Food Security. In: BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. *Big Data Challenges*: Society, Security, Innovation and Ethics. London: Palgrave Macmillan, 2016. p.128). Tradução livre: "Para toda a cautela entre analistas sobre Big Data, seu uso já está informando iniciativas de segurança alimentar humanitária do século XXI."

101 Utilizar a tecnologia através da coleta e análise de dados no campo pode gerar economia de água em 50%, segundo estudo do Departamento de Estado Americano. (US DEPARTMENT OF STATE. *Precision Agriculture and Global Food Security*. Disponível em: <http://www.state.gov/e/stas/series/212172.htm>. Acesso em: 18 ago. 2016).

102 *"Global Pulse is a flagship innovation initiative of the United Nations Secretary-General on big data. Its vision is a future in which big data is harnessed safely and responsibly as a public good. Its mission is to accelerate discovery, development and scaled adoption of big data innovation for sustainable development and humanitarian action. The initiative was established based on a recognition that digital data offers the opportunity to gain a better understanding of changes in human well-being, and to get real-time feedback on how well policy responses are working."* (UNITED NATIONS GLOBAL PULSE. *Global Pulse*. Disponível em: <http://www.unglobalpulse.org/about-new>. Acesso em: 02 nov. 2016). Tradução livre: "Global Pulse é uma iniciativa emblemática de inovação do Secretário-Geral das Nações Unidas sobre big data. A sua visão é um futuro em que o big data é aproveitado de forma segura e responsável como um bem público. Sua missão é acelerar a

principal foco consiste no *big data*, na tentativa de se utilizar da tecnologia para o desenvolvimento sustentável do planeta. Em relatório recente, o programa estudou formas de se detectar aumentos abruptos de preços de alimentos em áreas carentes na Indonésia, se utilizando da análise de grande quantidade de postagens na rede social twitter.[103]

Verifica-se ainda volume expressivo de investimentos[104] no setor agricultor, para que a tecnologia mais avançada seja onipresente não só dos grandes centros, mas igualmente revolucione[105] a zona rural. Maior produtor de veículos autônomos está no campo, através dos tratores automatizados fabricados pela John Deere[106], que dispensa humanos e se vale da coleta, análise e armazenamento de substancial

---

descoberta, desenvolvimento e adoção em escala para o desenvolvimento sustentável e ação humanitária. A iniciativa foi estabelecida com base no reconhecimento de que os dados digitais oferecem a oportunidade de compreender melhor as mudanças no bem-estar humano e obter feedback em tempo real sobre o quão bem as políticas implementadas estão funcionando."

103 EVANS, Bryce. Using Big Data to Achieve Food Security. In: BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. *Big Data Challenges*: Society, Security, Innovation and Ethics. London: Palgrave Macmillan, 2016. p.129.

104 *"Monsanto considered big data in agriculture to be worth multi-billion dollar investments, evidenced by their acquisition of several farm data analytics companies between May 2012 and February 2014. The technology has the potential to increase yield production, and as we near an era of history wrought with more people and less resources, this makes farming one of the most important careers in the world."* (GILPIN, Lyndsey. How big data is going to help feed nine billion people by 2050. *Tech Republic*. Disponível em: <http://www.techrepublic.com/article/how-big-data-is-going-to-help-feed-9-billion-people-by-2050/>. Acesso em: 18 ago. 2016). Tradução livre: "A Monsanto considerou que o big data na agricultura vale investimentos de vários bilhões de dólares, evidenciado pela aquisição de várias empresas de análise de dados agrícolas entre maio de 2012 e fevereiro de 2014. A tecnologia tem o potencial de aumentar a produção, e como nos aproximamos da era da história forjada com mais pessoas e menos recursos, isso torna a agricultura uma das carreiras mais importantes do mundo".

105 *"Farming is undergoing a digital revolution."* (BRONSON, Kelly; KNEZEVIC, Irena. Big Data in food and agriculture. *Big Data & Society*. Jan./June 2016. Disponível em <http://bds.sagepub.com/content/spbds/3/1/2053951716648174.full.pdf>. Acesso em: 1.º dez. 2016). Tradução livre: "Agricultura está passando por uma revolução digital."

106 "*The world's largest producer of autonomous four-wheeled vehicles isn't Tesla or Google, it's John Deere."* (MIMS, Christopher. To Feed Billions, Farms Are About Data as Much as Dirt. *The Wall Street Journal*, Aug. 2015. Disponível em: <http://www.wsj.com/articles/to-feed-billions-farms-are-about-data-as-much-as-dirt-1439160264>. Acesso em: 18 ago. 2016). Tradução livre: "O maior produtor mundial de veículos autônomos de quatro rodas não é a Tesla ou a Google, é a John Deere."

quantidade de informações[107] para operar, propiciando maior eficiência na tomada de decisões[108] e, consequentemente, gerando substancial aumento da produtividade.

Destacam-se ainda a previsão do tempo e os fatores climáticos como elementos igualmente cruciais na maximização da produção agrícola, funcionando o *big data* como mecanismo de grande valia para se alcançar este objetivo, através da instalação de sensores eletrônicos no campo[109], com coleta e análise de dados de inúmeras fontes, permitindo-se que decisões estratégicas sejam adotadas com o auxílio tecnológico, maximizando das chances de êxito.

Com base naquilo que foi posto acima, vê-se que a tecnologia, mais precisamente o *big data*, já se encontra em estágio avançado de utilização na agricultura em inúmeros locais como forma de otimização do processo produtivo, sendo entendido ainda como um dos fatores que podem salvar o planeta da prevista insuficiência de alimentos diante da explosão populacional que se avizinha.

---

107 "*Today there are more than 200,000 Deere machines that can wirelessly transmit agronomic data to remote servers to be organized, analyzed, and tapped for other applications (such as coordinating multiple machines in the same field).*" (LEV-RAM, Michal. What John Deere is Doing to Fight Slumping Sales. *Fortune*, Nov. 2016. Disponível em: <http://fortune.com/2015/11/15/john-deere-software-services-agriculture-data/>. Acesso em: 18 ago. 2016). Tradução livre: "Hoje existem mais de 200.000 máquinas Deere que podem transmitir dados agronômicos sem fio para servidores remotos para serem organizados, analisados e testados para outras aplicações (como coordenar várias máquinas no mesmo campo)."

108 *"John Deere fits all of its tractors with sensors that stream data about soil and crop conditions and the corporation invites farmers to subscribe (and pay) for access to information that can help them decide, for example, where to plant crops."* (BRONSON, Kelly; KNEZEVIC, Irena. Big Data in food and agriculture. *Big Data & Society*. Jan./June 2016. Disponível em <http://bds.sagepub.com/content/spbds/3/1/2053951716648174.full.pdf>. Acesso em: 1.º dez. 2016). Tradução livre: "A John Deere adapta todos os seus tratores com sensores que transmitem dados sobre as condições do solo e da cultura e a corporação convida os agricultores a subscrever (e pagar) o acesso a informações que podem ajudá-los a decidir, por exemplo, onde plantar."

109 *"In the recent years, driven by increasing investment in the Internet of Things, through data capture of wireless sensor networks, agricultural applications have started to close the "last mile" gap in meteorological services. An optimistic finding is that data capture and monitoring will be changing from observing the weather to observing data."* (TANG, Chunlei. *The data industry*: the business and economics of information and big data. New Jersey: Wiley, 2016. p.100). Tradução livre: "Nos últimos anos, impulsionado pelo aumento do investimento na Internet das Coisas, através da captura de dados de redes de sensores sem fio, as aplicações agrícolas começaram a fechar a última lacuna nos serviços meteorológicos. Uma conclusão otimista é que a captura e o monitoramento de dados estarão mudando de observar o tempo para observar dados."

1.3 **O outro lado da moeda: os riscos do *big data***

Nas breves considerações tecidas acima, foi possível verificar as diversas facetas positivas do *big data*, com exemplos claros dos benefícios e avanços paradigmáticos em uma miríade de atividades.

Porém, nem sempre se está diante de um cenário inteiramente positivo, como se verá de alguns exemplos que serão analisados. Como se cunhou recentemente, a tecnologia permitiu um novo tipo de viligância quase que onipresente, que até pouco tempo não passava de imaginação de autores de obras de ficção científica.[110]

O *big data* tem sido utilizado pelo sistema criminal do Poder Judiciário dos Estados Unidos da América para, com base na análise de dados pessoais dos réus, prever a possibilidade de reincidência dos crimes praticados, influenciando diretamente no resultado das decisões proferidas.

Estudos científicos[111] demonstram que o sistema tem cometido equívocos, especialmente quando externa resultados mais negativos para determinados grupos sociais.[112]

A pulseira inteligente comercializada pela fabricante de tênis Nike, chamada de *Nike+ FuelBand*, em sua política de privacidade[113], escreve que o *software* que a controla poderá captar e armazenar os hábitos do usuário, tais como localização,

---

110 GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.2.

111 STARR, Sonja B. Evidence-Based Sentencing and the Scientific Rationalization of Discrimination. *Stanford Law Review, Forthcoming; University of Michigan Law & Econ Research Paper n.13-014*, 2013. Disponível em: <https://ssrn.com/abstract=2318940>. Acesso em: 10 nov. 2016.

112 "*ProPublica found that the formula was particularly likely to flag black defendants as future criminals, labeling them as such at almost twice the rate as white defendants. In addition, white defendants were labeled as low risk more often than black defendants."* (ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). *Algorithms in the Criminal Justice System*. Disponível em: <https://epic.org/algorithmic-transparency/crim-justice/>. Acesso em: 26 nov. 2016). Tradução livre: "A ProPublica descobriu que a fórmula era particularmente suscetível de marcar os réus negros como futuros criminosos, rotulando-os como tal em quase o dobro da taxa dos réus brancos. Além disso, os réus brancos foram rotulados como de baixo risco mais frequentemente do que os réus negros."

113 NIKE. *APP & Device Support*. Disponível em: <https://secure-nikeplus.nike.com/plus/support#answers/detail/a_id/21061/kw/privacy%20policy> Acesso em: 07 ago. 2015.

distâncias percorridas, calorias queimadas, dentre outras, não deixando claro qual será a utilização destas informações[114] pela empresa.

Um bafômetro eletrônico que se conecta ao celular, chamado de *Breathometer*[115], sucesso de vendas com produção à época de 15.000 unidades por semana após o lançamento[116], não menciona qualquer ponto acerca de sua política de privacidade, especialmente de que forma irá captar, armazenar e tratar a grande quantidade de dados recebidas.

O interessado em ter ciência de seus termos deverá percorrer um tortuoso caminho pelo *website* da empresa para descobrir que todos os resultados dos testes de nível alcoólico serão armazenados indefinidamente nos servidores do fabricante, não poderão ser excluídos pelo usuário, poderão ser disponibilizados em caso de ordem judicial e ainda ser utilizados para aprimorar a estratégia de marketing do fabricante.

Da análise destes singelos exemplos, que versam sobre dados sensíveis de seus usuários, notadamente diante da grande quantidade de informações pessoais coletadas, armazenadas e analisadas, não resta dúvida no sentido de o *big data* desafia a sociedade e o ordenamento jurídico, especialmente naquilo que se refere à

---

114 *"What is missing is much of a sense of what this is worth, and what it may cost, and the terms under which we'll turn our data into a product. Nike and Fitbit already log a lot of personal data, and it is not clear what, if anything, they plan to do with it. Nike acknowledged an e-mail asking for details about its plans, but did not get back after that. The software license for Nike+ does say that "Nike+ Product Software may include software that collects information about how you use your Nike+ Product," but has no further details about what this means."* (HARDY, Quentin. Big Data in Your Blood. *Bits*, Sept. 2012. Disponível em: <http://bits.blogs.nytimes.com/2012/09/07/big-data-in-your-blood/?_php=true&_type=blogs&_r=0>. Acesso em: 25 jun. 2015). Tradução livre: "O que está faltando é uma boa idéia do que isso vale, e o que pode custar, e os termos sob os quais vamos transformar nossos dados em um produto. A Nike e a Fitbit já registram uma grande quantidade de dados pessoais, e não está claro o que, se alguma coisa, eles planejam fazer com isso. A Nike reconheceu um e-mail pedindo detalhes sobre seus planos, mas não respondeu. A licença de software da Nike + diz que "o Software Nike + Product pode incluir software que coleta informações sobre como você usa o Nike + Product", mas não tem mais detalhes sobre o que isso significa."

115 PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.90, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015.

116 PAI, Aditi. Breathometer tops $1M in sales for smartphone breathalyzer. *Mobi Health News*, May 2014. Disponível em: <http://mobihealthnews.com/33325/breathometer-tops-1m-in-sales-for-smartphone-breathalyzer/>. Acesso em: 07 ago. 2015.

privacidade, diante da tutela dos dados pessoais, sendo terreno fértil para práticas, por exemplo, discriminatórias, de vigilantismo excessivo, as quais não raro implicam em violações de direitos da personalidade.

Neste contexto, o escritório executivo do Presidente dos Estados Unidos da América produziu um profundo relatório onde constatam alguns destes desafios, conforme se vê do trecho em destaque:

> *Big data technologies, together with the sensors that ride on the 'Internet of Things', pierce many spaces that were previously private. Signals from home WiFi networks reveal how many people are in a room and where they are seated. Power consumption data collected from demand-response systems show when you move about your facial recognition technologies can identify you in pictures online and as soon as you step outside. Always-on wearable technologies with voice and video interfaces and the arrival of whole classes of networked devices will only expand information collection still further. This sea of ubiquitous sensors, each of which has legitimate uses, make the notion of limiting information collection challenging, if not impossible*.[117]

A vasta quantidade de dados pessoais captados, armazenados e disponíveis para consulta e venda a terceiros interessados, atualmente, levanta uma justificável preocupação da sociedade[118], das empresas[119] e sobretudo dos juristas[120], valendo transcrever a afirmação de Gustavo Tepedino:

---

117 WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 07 ago. 2015. Tradução livre: "As grandes tecnologias de dados, juntamente com os sensores que circulam na 'Internet das Coisas', atravessam muitos espaços que antes eram privados. Sinais de redes WiFi caseira revelam quantas pessoas estão em uma sala e onde eles estão sentados. Os dados de consumo de energia coletados dos sistemas de demanda e resposta mostram quando você se move, tecnologias de reconhecimento facial podem identificá-lo em imagens on-line e logo que você sai de casa. Tecnologias wearable sempre ligadas com interfaces de voz e vídeo e a chegada de classes inteiras de dispositivos em rede só irão expandir ainda mais a coleta de informações. Este mar de sensores ubíquos, cada um dos quais tem usos legítimos, tornam desafiadora, se não impossível, a noção de limitar a coleta de informações."

118 *"In Northern California, the Oakland City Council, under pressure from residents and civil liberties advocates, scaled back plans this year for a federally financed center that would have linked surveillance equipment around the city, including closed-circuit cameras, gunshot microphones and license plate readers. It also formed a committee to limit the use of this equipment and to develop privacy standards, like how long data may be kept and who will have access to it."* (WILLIAMS, Timothy. Facial Recognition Software Moves From Overseas Wars to Local Police. *The New York Times*, Aug. 2015. Disponível em: <http://mobile.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html>. Acesso em: 14 ago. 2015). Tradução livre: "No norte da Califórnia, o Conselho Municipal de Oakland, sob pressão dos defensores dos direitos civis e residentes, reduziu os planos este ano para um centro financiado pelo governo

> Com o avanço e o barateamento da tecnologia de informação, sofisticam-se os acessos e controles, o cruzamento e a circulação de dados, sendo urgente estabelecer mecanismos de tutela dos direitos fundamentais, especialmente no que tange aos dados sensíveis [...][121]

Este estado de alerta não é recente, já existindo vozes na década de 1980 que buscavam debater o assunto e já sugerir soluções, conforme se vê deste memorandum:

> *In considering current trends in the development of technology and growth of transborder data flows, it may be useful to begin by reviewing what the Explanatory Memorandum stated about the issues related to automatic data processing in 1980: Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks*.[122]

---

federal que teria ligado equipamentos de vigilância em torno da cidade, incluindo câmeras de circuito fechado, microfones que captam disparo de armas de fogo e leitores de placas. Ele também formou um comitê para limitar o uso destes equipamentos e para desenvolver padrões de privacidade, como quanto tempo os dados podem ser mantidos e quem terá acesso a ele."

119 "*A few years ago, users of Internet services began to realize that when an online service is free, you're not the customer. You're the product."* (COOK, Tim. *Apple's commitment to your privacy*. Disponível em: <https://www.apple.com/privacy/>. Acesso em: 06 ago. 2015). Tradução livre: "Alguns anos atrás, os usuários de serviços de Internet começaram a perceber que quando um serviço on-line é gratuito, você não é o cliente. Você é o produto."

120 "O processamento e a coleta dos dados são, muitas vezes, invisíveis ao interessado, que não tem noção clara (ou noção alguma) do que está sendo feito com suas informações, ficando impossibilitado de fazer valer seu direito no caso." (DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000. p.18).

121 TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v.110, n.419, p.69, jan./jun. 2014.

122 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016. Tradução livre: Ao considerar as tendências atuais no desenvolvimento da tecnologia e o crescimento dos fluxos de dados transfronteiriços, pode ser útil começar por revisar o que o Memorando Explicativo declarou sobre as questões relacionadas ao processamento automático de dados em 1980: Entre as razões para tal preocupação generalizada estão a onipresente utilização de computadores para o tratamento de dados pessoais, as vastas possibilidades de armazenar, comparar, ligar, selecionar e acessar dados pessoais e a combinação de computadores e tecnologias de telecomunicações que podem colocar dados pessoais simultaneamente à disposição de milhares de utilizadores em locais geograficamente dispersos e permitir o agrupamento de dados e a criação de complexas redes de dados nacionais e internacionais.

Neste turno, uma vez que o *big data* culmina na análise de grande quantidade de dados, comumente contendo informações pessoais, inúmeros riscos acabam aflorando, notadamente diante da possibilidade concreta e efetiva de captação e tratamento ilícito e abusivo de dados pessoais, com a consequente violação da privacidade.[123]

Some-se isso ao fato de que na sociedade contemporânea, está-se diante de uma cenário onde a relação com as grandes corporações e governos, na grande maioria das vezes, é desigual e assimétrica. A larga utilização do *big data*, seja como modelo de negócios de empresas, seja como forma de atuação do Poder Público, em muitos casos pode eclodir na criação de um novo Big Brother[124], sendo, portanto, uma prática de inegável impacto social: *"Big data has a societal impact, because of two main raisons d'être: big data enables unprecedented predictions on private lives and it shifts the power to those who hold the information and those who supply it"*.[125]

A utilização do *big data* de maneira maliciosa e sem controle tem potencial de alterar o curso da história, conforme estudo publicado em respeitável periódico científico, que demonstra a possibilidade de manipulação de eleições por mecanismos de buscas:

> *We present evidence from five experiments in two countries suggesting the power and robustness of the search engine manipulation effect (SEME). Specifically, we show that (i) biased search rankings can shift the voting preferences of undecided voters by 20% or more, (ii) the shift can be much higher in some demographic groups, and (iii) such rankings can be masked so that people show no awareness of the manipulation. Knowing the proportion of undecided voters in a population who have Internet access, along with the*
>
> *proportion of those voters who can be influenced using SEME, allows one to*

---

123 *"Privacy protection is undoubtedly the biggest challenge facing the data industry."* (TANG, Chunlei. *The data industry*: the business and economics of information and big data. New Jersey: Wiley, 2016. p.187). Tradução livre: "A proteção da privacidade é sem dúvida o maior desafio que a indústria de dados enfrenta."

124 "*On the other, big data is seen as a troubling manifestation of Big Brother, enabling invasions of privacy, decreased civil freedoms, and increased state and corporate control."* (BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016). Tradução livre: "Por outro lado, o bog data é visto como uma manifestação preocupante do Big Brother, permitindo invasões de privacidade, diminuição das liberdades civis e aumento do controle estatal e corporativo."

125 HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.98. Tradução livre: "O big data têm um impacto social, devido a duas razões principais: big data permite previsões sem precedentes sobre a vida privada e deslocam o poder para aqueles que detêm a informação e aqueles que a fornecem."

> *calculate the win margin below which SEME might be able to determine an election outcome*.[126]

Além de uma constante exposição dos dados pessoais, sobretudo na internet, por mais inofensivo que seu conteúdo possa parecer, como a chamada *metadata*[127], quando comparados, catalogados e classificados, podem revelar muito sobre determinada pessoa[128] e possuem grande potencial danoso, caso utilizados para

---

126 EPSTEIN, Robert; ROBERTSON, Ronald. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences*, 2015. Disponível em: <http://www.pnas.org/content/112/33/E4512.full.pdf>. Acesso em: 25 ago. 2016. Tradução livre: "Apresentamos evidências de cinco experimentos em dois países sugerindo o poder e a robustez do efeito de manipulação do mecanismo de busca (SEME). Especificamente, mostramos que (i) os rankings de busca tendenciosos podem mudar as preferências de voto de eleitores indecisos em 20% ou mais, (ii) a mudança pode ser muito maior em alguns grupos demográficos e (iii) essas classificações podem ser mascaradas de modo que as pessoas não mostram nenhuma consciência da manipulação. Saber a proporção de eleitores indecisos em uma população que tem acesso à Internet, juntamente com a proporção dos eleitores que podem ser influenciados usando SEME, permite calcular a margem de vitória abaixo da qual o SEME pode ser capaz de determinar um resultado eleitoral."

127 *"An equally profound question is whether certain types of data – specifically the "metadata" or transactions records about communications and documents, versus the content of those communications and documents – should be accorded stronger privacy protections than they are currently. "Metadata" is a term describing the character of the data itself. The classic example comes from telecommunications. The phone numbers originating and terminating a call, as metadata, are considered less revealing than the conversation itself and have been accorded different privacy protections. Today, with the advent of big data, both the premise and policy may not always be so straightforward."* (WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. p.15-21. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 ago. 2015). Tradução livre: "Uma questão igualmente profunda é se certos tipos de dados – especificamente os 'metadados' ou registros de transações sobre comunicações e documentos, versus o conteúdo dessas comunicações e documentos – devem ser protegidos de forma mais forte do que atualmente. 'Metadado' é um termo que descreve o caráter dos próprios dados. O exemplo clássico vem das telecomunicações. Os números de telefone que originam e terminam uma chamada, como metadados, são considerados menos reveladores do que a própria conversa e foram concedidas diferentes proteções de privacidade. Hoje, com o advento do big data, tanto a premissa como a política podem nem sempre ser tão diretas ".

128 *"The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals."* (WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. p.15-21. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 ago. 2015). Tradução livre: "O advento de análises mais poderosas, que podem discernir um pouco de até mesmo pequenos e desconectados pedaços de dados, levanta a possibilidade de que os dados recolhidos e detidos por terceiros podem ser amalgamados e analisados de forma a revelar ainda mais informações sobre os indivíduos"

perseguição ou discriminação, além de alcançarem cada vez mais valor de mercado[129], recebendo tratamento por muitas empresas como verdadeira mercadoria.[130]

Tendo em vista o que foi exposto, passa-se à análise específica de alguns breves exemplos nos quais o *big data* tem sido utilizado pela violação da privacidade, gerando práticas discriminatórias e monitoramento e vigilantismo dos indivíduos.

1.3.1 Discriminação

Recentemente se noticiou[131] que os anunciantes da rede social Facebook poderiam direcionar seus anúncios escolhendo, dentro das várias opções de perfil, a raça e etnia de seu público alvo de mais de 1,79 bilhão de usuários ativos mensais.[132] Além disso, foi revelada a possibilidade de identificação e qualificação dos usuários

---

[129] As empresas Equifax e Lotus dispunham de informações pessoais 120 milhões de americanos e mencionaram expressamente a intenção de vendê-las no mercado. (RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.99-100). Ainda neste sentido: "O valor econômico da informação torna ainda mais lucrativa a violação à privacidade, assim como enseja a proliferação de meios indiretos de usurpação de dados pessoais." (KONDER, Carlos Nelson. Privacidade e corpo: convergências possíveis. *Pensar* (UNIFOR), v.18, p.352-398, 2013. Disponível em: <http://ojs.unifor.br/index.php/rpen/article/view/2696/pdf>. Acesso em: 05 out. 2016).

[130] *"We pay no money for Google's services. But someone pays for its thousands of engineers, and that someone is advertisers. [...] We pay with our attention and with our data, the raw material of marketing."* (PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.66). Tradução livre: "Nós não pagamos dinheiro pelos serviços do Google, mas alguém paga pelos seus milhares de engenheiros, e esse alguém é o anunciante. [...] Pagamos com nossa atenção e com nossos dados, a matéria-prima do marketing".

[131] *"The ubiquitous social network not only allows advertisers to target users by their interests or background, it also gives advertisers the ability to exclude specific groups it calls 'Ethnic Affinities'" Ads that exclude people based on race, gender and other sensitive factors are prohibited by federal law in housing and employment."* (ANGWIN, Julia; PARRIS JR. Terry. Facebook Lets Advertisers Exclude Users by Race. *ProPublica*, Oct. 2016. Disponível em: <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>. Acesso em: 13 nov. 2016). Tradução livre: "A rede social onipresente não só permite que os anunciantes direcionem os usuários por seus interesses ou experiência, mas também dá aos anunciantes a capacidade de excluir grupos específicos chamados de 'afinidades étnicas'. Os anúncios que excluem pessoas com base em raça, sexo e outros fatores sensíveis são proibidos por Lei Federal sobre habitação e emprego."

[132] NEWSROOM. *Our History*. Disponível em: <http://newsroom.fb.com/company-info/>. Acesso em: 13 nov. 2016.

da rede social conforme suas orientações políticas, analisando o perfil de utilização da plataforma através de um algoritmo.[133]

Não há dúvidas, portanto, que as mais diversas atividades e práticas que contemplam em seu modelo a análise de grandes bancos de dados, geram a possibilidade de criação de práticas discriminatórias[134], principalmente quando diante de dados sensíveis, como orientação sexual e informações médicas[135], submetidos à análise de poderosos algoritmos que podem carregar uma programação segregativa.[136]

Esta conclusão não é nova e não se limita ao *big data*, pois o risco de práticas discriminatória se liga diretamente à tutela da privacidade. Aliás, trata-se de uma das razões pelas quais tanto se alardeia a necessidade de tratá-la como direito fundamental:

---

133 *"You may think you are discreet about your political views. But Facebook, the world's largest social media network, has come up with its own determination of your political leanings, based on your activity on the site."* (MERRILL, Jeremy B. Liberal, Moderate or Conservative? See How Facebook Labels You. *The New York Times*, Aug. 2016. Disponível em: <http://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html?_r=0>. Acesso em: 24 ago. 2016). Tradução livre: "Você pode pensar que você é discreto sobre seus pontos de vista políticos, mas o Facebook, a maior rede de mídia social do mundo, criou sua própria determinação de suas tendências políticas, com base na sua atividade no site."

134 *"But despite the potential for efficiency gains, algorithms fed by big data can also amplify structural discrimination, produce errors that deny services to individuals, or even seduce an electorate into a false sense of security. Indeed, there is growing awareness that the public should be wary of the societal risks posed by over-reliance on these systems and work to hold them accountable."* (DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How to Hold Algorithms Accountable. *MIT Technology Review*, Nov. 2016. Disponível em: <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/>. Acesso em: 26 nov. 2016). Tradução livre: "Mas, apesar do potencial de ganhos de eficiência, os algoritmos alimentados pelo big data também podem ampliar a discriminação estrutural, produzir erros que negam serviços a indivíduos ou até mesmo seduzir um eleitorado com um falso senso de segurança. Na verdade, há uma crescente consciência de que o público deve ser cauteloso com os riscos sociais colocados por excesso de confiança nesses sistemas e trabalhar para mantê-los responsáveis."

135 "Informações sobre raça, credo, opção sexual, convicções políticas e filosóficas, filiações partidárias e sobre o estado de saúde têm o potencial de ocasionar, isoladamente ou em conjunto, práticas discriminatórias ao seu titular e, por isso, têm sido historicamente tratadas como uma categoria especial." (BIONI, Bruno R. *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. p.247-248).

136 *"The effects of data practices without ethics can be manifold – unjust treatment, discrimination and unequal opportunities. But privacy is at its core."* (HASSELBALCH, Gry; TRANBERG, Pernille. Privacy is still alive and kicking in the digital age. *Tech Crunch*, Dec. 2016. Disponível em: <https://techcrunch.com/2016/12/25/privacy-is-still-alive-and-kicking-in-the-digital-age/>. Acesso em: 27 dez. 2016). Tradução livre: "Os efeitos das práticas de dados sem ética podem ser múltiplos – tratamento injusto, discriminação e oportunidades desiguais. Mas a privacidade está no seu âmago."

> Esse é um tema que pode ser examinado com referência a certos dados sensíveis específicos, como os relacionados à saúde. Antes se mencionou que a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações.[137]

Nesta toada, a Convenção de Oviedo[138], que versa sobre dados genéticos, em 1997 já previa a "não discriminação"[139] com base no tratamento de dados sensíveis. Mais recente, o Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho, editado em 27 de abril de 2016, cujas regras serão aplicáveis a partir de 25 de maio de 2018, também chamado de Regulamento Geral sobre a Proteção de Dados, reconhece este desafio, trazendo diversos balizamentos ao tratamento de dados pessoais, especialmente quando por processos automatizadfos, sendo salutar destacar a seguinte passagem do preâmbulo:

> O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para

---

137 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.106.

138 Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina. Adotada e aberta à assinatura em Oviedo em 4 de Abril de 1997. Entrada em vigor na ordem internacional em 1 de dezembro de 1999. (GABINETE DE DOCUMENTAÇÃO E DIREITO COMPARADO. Conselho da Europa. *Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina*. Disponível em: <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhregionais/convbiologiaNOVO.html>. Acesso em: 13 nov. 2016).

139 Genoma humano artigo 11.º Não discriminação. É proibida toda a forma de discriminação contra uma pessoa em virtude do seu património genético.

> garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.
> A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

O próprio legislador brasileiro, também diante do reconhecimento deste risco, trouxe regramentos com vistas a coibir ações discriminatórias na internet, como se observa no Marco Civil da Internet[140] e no Decreto n.º 8.771/16 sobre dados pessoais.[141]

Com base no acima exposto, extrai-se que o problema da discriminação diante do *big data*, de caráter deveras desafiador, não passou inteiramente despercebido pelos juristas, em que pese não haver uma solução jurídica integralmente eficiente para a questão.

---

[140] Art. 9.º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. [...] § 2.º Na hipótese de discriminação ou degradação do tráfego prevista no § 1.º, o responsável mencionado no caput deve: [...] IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

[141] Art. 10. As ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória.

Considerando ser cediço que a tecnologia deve evoluir como instrumento de promoção e valorização da pessoa humana[142], é de extrema relevância dispensar atenção para que não ocorra uma inversão axiológica, principalmente quando se adverte[143] que o *big data*, cuja prática muitas vezes se dá com tomadas de decisões automatizadas, pode ter como consequência a criação ou elevação de barreira sociais e econômicas dentro de uma sociedade.[144]

1.3.2 Monitoramento e vigilantismo

Além de discriminação, os avanços tecnológicos têm permitido que o *big data* seja utilizado para monitoramento constante e injustificado de cidadãos em vários países, criando situações verdadeiramente orwellianas. Não só o Estado, mas inúmeras empresas[145] também se utilizam do *big data* como forma de vigiar e

---

142 "De qualquer maneira que se queira ler a Constituição, não parece possível deixar de perceber que ela assenta sobre uma clara hierarquia de valores. Isto faz com que a atividade econômica, categoria do ter, deva ser instrumental à realização dos valores existenciais, à categoria do ser." (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p.522).

143 "Além disso, o big data e sua cadeia de consequências – classificação social, processos decisórios baseados em algoritmos, e assim por diante – podem ser usados para produzir discriminação ou mesmo tornar ainda mais fortes as barreiras econômicas e sociais na sociedade em alguns países." (INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. *Big data no projeto Sul Global*: relatório sobre estudos de caso. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016).

144 *"We must pay ongoing and careful attention to ensure that the use of big data does not contribute to systematically disadvantaging certain groups."* (WHITE HOUSE. *Big Data*: A Report on Algorithmic Systems, Opportunity, and Civil Rights. Executive Office of the President. May 2016. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Acesso em: 29 ago. 2016). Tradução livre: "Devemos prestar atenção contínua e cuidadosa para garantir que o uso do big data não contribua para prejudicar sistematicamente certos grupos."

145 *"Google recently announced that it would start including individual users names and photos in some ads. This means that if you rate some product positively, your friends may see ads for that product with your name and photo attached -- without your knowledge or consent. Meanwhile, Facebook is eliminating a feature that allowed people to retain some portions of their anonymity on its website."* (SCHNEIER, Bruce. 'Stalker economy' here to stay. *CNN*, Nov. 2013. Disponível em: <http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/>. Acesso em: 13 out. 2016). Tradução livre: "O Google anunciou recentemente que começaria a incluir nomes de usuários individuais e fotos em alguns anúncios, o que significa que, se você classificar algum produto de forma positiva, seus amigos poderão ver anúncios para esse produto com o seu nome e foto anexados – sem seu conhecimento ou consentimento. Enquanto isso, o Facebook está eliminando um recurso que permitia que as pessoas retivessem algumas partes de seu anonimato em seu site."

monitorar seus usuários, faturando altas cifras com práticas que se denominaram como "*stalker economy*".[146]

Os chamados "*Fusion Centers*"[147] nos Estado Unidos da América, geridos pela *Nation Secutiry Agency*, funcionam como um vasto banco de dados, que constantemente captam, armazenam e analisam informações, criando perfis de milhões de pessoas sob o pretexto de garantia da segurança e combate ao crime. Porém, o programa não fornece informações públicas que possibilitariam a fiscalização e controle pela população que é objeto de sua base de dados, operando como verdadeira caixa preta[148] e servindo de método deveras eficaz para vigiar e monitorar o povo norte-americano e de outras nacionalidades.

Glen Greenwald revela[149] que uma Lei de 2008, nos Estados Unidos, permite que a Nation Secutiry Agency solicite às empresas de tecnologia qualquer dado de comunicação de estrangeiros, sem a necessidade de fundamentar o pedido, e mesmo que este estrangeiro se comunique ou relacione com cidadãos americanos.

Além disso, investigações jornalísticas demonstram que os governos da Síria, Egito e Líbia se utilizaram da coleta, análise e armazenamento de grande quantidade de informações de seu povo, captados por meio de sofisticados mecanismos tecnológicos, com vistas a monitorar e, eventualmente, perseguir cidadãos.[150]

Destaca-se ainda a intenção do Departamento de Segurança Interna dos Estados Unidos de incorporar publicações em redes sociais em suas análises para

---

146 MICHALSKI, Jerry. Big Data and the Stalker Economy. *Forbes*, Mar. 2012. Disponível em: <http://www.forbes.com/sites/jerrymichalski/2012/03/10/big-data-stalker-economy/#1ec615604636>. Acesso em: 18 nov. 2016.

147 *"Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners."* (US DEPARTMENT OF HOMELAND SECURITY. *State and Major Urban Area Fusion Centers*. Disponível em: <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>. Acesso em: 18 nov. 2016). Tradução livre: "Os fusion centers funcionam como pontos focais estaduais e de grandes áreas urbanas para o recebimento, análise, coleta e compartilhamento de informações relacionadas a ameaças entre federais, estaduais, locais, tribais, territoriais (SLTT) e parceiros do setor privado."

148 PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.46-48.

149 GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.74.

150 Ibid., p.4.

concessão de vistos.[151] Após atentados terroristas em Paris e na Califórnia, ganhou força um projeto para inserir um campo no formulário de imigração onde os viajantes, cujo visto é dispensado, deverão inserir os dados de suas respectivas contas nas redes sociais para ingresso no país.[152]

É importante mencionar que a Corte de Justiça da União Europeia, divulgou em 21/12/2016 o resultado do julgamento dos Casos C-203/15 e C-698/15[153] que versavam sobre questionamentos de regras que impunham o arquivamento indiscriminado de dados relativos à localização de tráfego de dados em comunicações eletrônicas, envolvendo cidadãos na Irlanda, Noruega e Reino Unido, abrindo relevante debate sobre o acesso a tais informações, o que, por certo, implica em risco de vigilância excessiva[154], notadamente por parte das empresas que guardam os dados e dos Estados que podem ter acesso a eles.

Através de decisão definitiva da qual não cabe recurso, a Corte Europeia decidiu que os Estados-Membros não podem impor uma obrigação geral de conservar dados das comunicações eletrônicas, pois tal medida configuraria verdadeiro ato de vigilância indiscriminada, incompatível com os direitos fundamentais, violando a proporcionalidade, razoabilidade e os valores inscritos em uma sociedade democrática.

---

151 PALETTA, Damian. U.S. Working on Plan to Scrutinize Social Media in Visa Reviews. *The Wall Street Journal*, Dec. 2015. Disponível em: <http://www.wsj.com/articles/u-s-working-on-plan-to-scrutinize-social-media-in-visa-reviews-1450122633>. Acesso em: 18 ago. 2016.

152 NIXON, Ron. Visitors to the U.S. May Be Asked for Social Media Information. *The New York Times*, June 2016. Disponível em: <http://www.nytimes.com/2016/06/29/us/homeland-security-social-media-border-protection.html?_r=0> Acesso em: 18 nov. 2016.

153 THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf>. Acesso em: 23 dez. 2016.

154 *"The interference by national legislation that provides for the retention of traffic data and location data with that right must therefore be considered to be particularly serious. The fact that the data is retained without the users of electronic communications services being informed of the fact is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance."* (THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf>. Acesso em: 23 dez. 2016. Tradução livre: "A ingerência da legislação nacional que prevê a conservação dos dados de tráfego e dos dados de localização com esse direito deve ser considerada particularmente grave. O fato de os dados serem conservados sem que os utilizadores dos serviços de comunicações eletrónicas sejam informados do fato é suscetível de fazer com que os interessados sintam que a sua vida privada é objeto de vigilância constante."

Neste cenário onde a privacidade e o sigilo têm perdido espaço para a onipresença[155] da tecnologia, não é exagero afirmar que o estado de vigilância constante se tornou quase impossível de ser evitado[156] pela população, mais uma vez demonstrando a necessidade preeminente de se garantir a prevalência da democracia e no reestabelecimento da confiança entre população e governos.[157]

1.3.3 *Big data* e o sistema de crédito social Chinês

Com uma população superior a 1 bilhão de habitantes[158], a China pretende lançar um programa de pontuação, que compreende a gestão de um enorme banco de dados sobre seus cidadãos[159], alimentado com milhares de informações pessoais,

---

155 *"People can no longer evade surveillance through electronic means. This is the genuinely new dimension of this type of surveillance, related to the role now played by the internet in our daily lives."* (HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.120). Tradução livre: "As pessoas já não podem fugir à vigilância por meios eletrônicos. Esta é a dimensão genuinamente nova deste tipo de vigilância, relacionada com o papel agora desempenhado pela Internet na nossa vida diária."

156 *"Big data justifies a qualitative shift in thinking, because it enables unprecedented predictions on private lives and because it shifts power relations. Mass surveillance is the second phenomenon changing our societies, since surveillance is something people cannot avoid."* (Ibid., p.77). Tradução livre: "Big data justifica uma mudança qualitativa no pensamento, porque permite previsões sem precedentes sobre a vida privada e porque altera as relações de poder. A vigilância em massa é o segundo fenômeno que muda nossas sociedades, uma vez que a vigilância é algo que as pessoas não podem evitar."

157 Ibid., p.81.

158 1.382.323.000 habitantes. (UNDATA. *China*. Disponível em: <http://data.un.org/CountryProfile.aspx?crName=china>. Acesso em: 13 nov. 2016).

159 *"China's plan to organize its society relies on 'big data' to rate everyone."* (DENYER, Simon. China's plan to organize its society relies on 'big data' to rate everyone. *The Washington Post*, Oct. 2016. Disponível em: <https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html>. Acesso em: 13 nov. 2016). Tradução livre: "O plano da China para organizar sua sociedade depende do "big data" para avaliar todos."

sendo a maioria delas captadas pela internet[160], tais como histórico de navegação na internet, itens adquiridos em compras, probabilidade de adimplemento de obrigações, entre vários outros, de forma a perfilar e classificar cada um dos chineses.

Tal projeto tem sido objeto de inúmeras críticas[161], tido como um verdadeiro *big brother* moderno, pois será obrigatório para toda a população em 2020, atribuindo a todos uma pontuação entre 350 e 950, vinculado à identidade de cada indivíduo, valendo destacar alguns pontos polêmicos do projeto: o sistema é gerido por duas empresas que administram as redes sociais do país e, portanto, já têm acesso a uma enorme quantidade de dados pessoais sobre os indivíduos e suas respectivas relações sociais; entre elementos que podem prejudicar a pontuação de um cidadão estão a manifestação opiniões políticas, incluindo as manifestações de seus amigos; a compra de determinados bens melhora sua pontuação, enquanto outros pode reduzi-la; o acesso ao sistema permitirá que qualquer interessado verifique a pontuação de qualquer pessoa.

Seu intuito velado passa a ser a existência de um sistema de controle da moralidade social: *"Critics say China's internet is fast becoming a laboratory where big data meets big brother, where the march of technology combined with profit-*

---

160 *"Harnessing the power of big data and the ubiquity of smartphones, ecommerce and social media in a society where 700 million people live large parts of their lives online, the plan will also vacuum up court, police, banking, tax and employment records. Doctors, teachers, local governments and businesses could additionally be scored by citizens for their professionalism and probity."* (DENYER, Simon. China wants to give all of its citizens a score: and their rating could affect every area of their lives. *Independent*, Oct. 2016. Disponível em: <http://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html>. Acesso em: 13 nov. 2016. Tradução livre: "Aproveitando o poder do big data e a onipresença de smartphones, ecommerce e redes sociais em uma sociedade onde 700 milhões de pessoas vivem grandes partes de suas vidas on-line, o plano também irá captar dados judiciais, policiais, bancários, fiscais e registros de emprego. Médicos, professores, governos locais e empresas também poderiam ser avaliados pelos cidadãos por seu profissionalismo e probidade.

161 *"´This is the most staggering, publicly announced, scaled use of big data I've ever seen', says Michael Fertik, a Silicon Valley entrepreneur and author of The Reputation Economy."* (OBBEMA, Fokke; VLASKAMP, Marije; PERSSON, Michael. China rates its own citizens - including online behaviour. *The Volkskrant*, Apr. 2015. Disponível em: <http://www.volkskrant.nl/buitenland/china-rates-its-own-citizens-including-online-behaviour~a3979668/>. Acesso em: 13 nov. 2016). Ver ainda: STANLEY, Jay. China's Nightmarish Citizen Scores Are a Warning For Americans. *American Civil Liberties Union*, Oct. 2015. Disponível em: <https://www.aclu.org/blog/free-future/chinas-nightmarish-citizen-scores-are-warning-americans. Acesso em: 21 ago. 2016. Tradução livre: "Este é o uso mais impressionante, publicamente anunciado, escalado de big data que eu já vi, diz Michael Fertik, um empresário do Vale do Silício e autor de The Reputation Economy."

driven private companies, authoritarian politics and weak civil liberties is creating a toxic cocktail".[162]

Considerando este exemplo assombroso de má utilização do *big data* para práticas que claramente violam direitos da personalidade, renova-se a atenção necessária ao estabelecimento de mecanismos legais consentâneos com o atual estado da tecnologia, onde esta possa ser compatilizada e harmonizada com a privacidade e proteção de dados pessoais.

1.3.4 Os dados pessoais são o novo petróleo?

O exemplo do sistema de pontuação chinês revela, talvez, o lado mais sombrio até então noticiado do *big data*, onde a dignidade da pessoa humana acaba por ser colocada em segundo plano em detrimento da fome totalitária de um regime político afastado dos valores republicanos.

É fruto da sua combinação com práticas contrárias aos mais comezinhos princípios democráticos, trazendo luz ao tema da privacidade e da proteção de dados pessoais, ressaltando a urgente necessidade de sua melhor compreensão, de forma que medidas como esta sejam objeto de escrutínio da sociedade e autoridades, evitando que práticas análogas se proliferem mundo afora e garantindo que a tutela da privacidade seja efetiva, pondo a pessoa humana sempre no ápice do ordenamento jurídico, sobretudo no controle de seus dados pessoais. Salutar, portanto, a recente afirmação: *"Many have understandable concerns over big data and privacy. Let me be clear. Nothing we do should be at the expense of fundamental rights. Mastering big data means mastering privacy too".*[163]

---

[162] CLOVER, Charles. China: When big data meets big brother. *Financial Times*, Jan. 2016. Disponível em: <http://www.ft.com/cms/s/2/b5b13a5e-b847-11e5-b151-8e15c9a029fb.html#axzz4Hy8NUVqa>. Acesso em: 21 ago. 2016.

[163] Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda. ICT 2013 Event – Session on Innovating by exploiting big and open data and digital content/Vilnius, 7 November 2013.

Por estas e outras razões se cunhou frase repetida a esmo, *"data is the new oil"*[164], pois governos e empresas têm consistentemente tratado os dados pessoais como mercadoria, levando a vice-presidente da União Europeia a afirmar que os dados dos cidadãos europeus valeriam a quantia de 315 bilhões de euros em 2013, prevendo a cifra de 1 trilhão em 2020.[165]

Porém, não se pode deixar seduzir pela impactante expressão, posto que, apesar de aparentemente[166] fazer sentido diante de uma análise perfunctória, tal assertiva não pode se sustentar, sob pena de ruína do valor e princípio da dignidade da pessoa humana[167] e da própria indústria que tanto se alimenta da importância que os dados pessoais têm no contexto do *big data*.

Ou seja, o principal elemento que torna o *big data* de grande benefício para a sociedade, empresas e governos é o valor extraído das informações analisadas. Ora, caso não haja qualquer plataforma de proteção destes dados, sobretudo daqueles sensíveis, tornando todas as informações pessoais de acesso livre e sem qualquer regra ou procedimento, é certo que este valor se tornará mínimo, senão inexistente.

Por estas razões, o *big data* tem na tutela da privacidade um dos requisitos fundamentais de sua sobrevivência, sendo fundamental que os dados pessoais

---

164 "'*Data is the new oil,' Shivon Zilis, a partner with the venture capital firm Bloomberg Beta, said about data's increasing value."* (VANIAN, Jonathan. Why Data Is The New Oil. *Fortune*, July 2016. Disponível em: <http://fortune.com/2016/07/11/data-oil-brainstorm-tech/>. Acesso em: 20 nov. 2016). Ver ainda MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.16). Tradução livre: "'Os dados são o novo petróleo', disse Shivon Zilis, sócio da empresa de capital de risco Bloomberg Beta, sobre o aumento do valor dos dados."

165 READING, Viviane. *Data protection reform*: restoring trust and building the digital single market. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm>. Acesso em: 14 dez. 2016.

166 *"'Data is the new oil!' It's exciting stuff for marketing types, and it's an easy equation: big data equals big oil, equals big profits."* (THORP, Jer. Big Data Is Not the New Oil. *Harvard Business Review*, Nov. 2012. Disponível em: <https://hbr.org/2012/11/data-humans-and-the-new-oil>. Acesso em: 20 nov. 2016). Tradução livre: "'Os dados são o novo óleo!' É uma coisa excitante para os tipos de marketing, e é uma equação fácil: big data equivale ao petróleo, igual a grandes lucros."

167 "A dignidade da pessoa humana, como valor e princípio, compõe-se dos princípios da liberdade privada, da integridade psicofísica, da igualdade substancial (art. 3.º, III, CF) e da solidariedade social (art. 3.º, I, CF). Tais princípios conferem fundamento de legitimidade ao valor social da livre iniciativa (art. 1.º, IV, CF), moldam a atividade econômica privada (art. 170, CF) e, em última análise, os próprios princípios fundamentais do regime contratual regulados pelo Código Civil." (TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.14).

sejam tratados e garantidos com status superior pelo ordenamento, cujo desrespeito deve ser sempre combatido:

> *This seems to be an oxymoron when applied to big data and privacy: personal data retain their value as long as they are perceived (and they are) a scarce and difficult to obtain resource, which does effectively and differently impact each individual's life. It is not necessarily in the interest of the big data industry and of the individuals to dilute this value*.[168]

[168] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*: an overview of privacy enhancing technologies in the era of big data analytics. Disponível em: <www.enisa.europa.eu>. Acesso em: 20 nov. 2016. Tradução livre: "Isso parece ser um oxímoro quando aplicado ao big data e privacidade: dados pessoais retem seu valor, enquanto eles são percebidos (e eles são) um recurso escasso e difícil de obter, o que efetivamente e de forma diferente impactam vida de cada indivíduo. Não é necessariamente do interesse da grande indústria de dados e dos indivíduos diluir esse valor. European Union Agency For Network And Information Security."

2 *BIG DATA* E A PROTEÇÃO DOS DADOS PESSOAIS

2.1 Da privacidade aos dados pessoais – evolução histórica

2.1.1 Privacidade como isolamento

A privacidade é algo intimamente ligado à evolução da espécie humana, diretamente relacionada com o instinto animal de territorialidade e de sobrevivência.[169] Suas primeiras referências são encontradas, dentre outros, desde 1.772 A.C. no Código de Hammurabi, na Bíblia, no Alcorão, na Grécia Antiga.

Já os primeiros contornos[170] embrionários da concepção mais atual de privacidade são oriundos da queda do sistema feudal, aliadas às transformações sociais, econômicas e políticas vindas da Revolução Industrial, que teve início no século XVIII. Aqueles que dispunham de bens materiais para construir suas próprias casas, isolando-se dos demais, mesmo nos centros urbanos, passaram também a desfrutar de certa privacidade, privilégio até antes restrito aos que viviam longe da comunidade, como, por exemplo, os senhores feudais e membros da igreja.

O nascimento da privacidade, portanto, não se apresenta como a realização de um valor existencial, ligado aos direitos da personalidade, de caráter fundamental, mas como a aquisição de um privilégio por parte de um grupo com maior poder aquisitivo.[171]

O século XIX foi considerado a época de ouro da privacidade[172], diante dos interesses em sua proteção manifestados pela ascendente classe burguesa. Identifica-se,

---

169 RENGEL, Alexandra. *Privacy in the 21st Century*. Leiden: Martinus Nijhoff Publishers, 2013. p.29.

170 DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000. p.2.

171 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.26.

172 Ibid., p.93.

assim, uma das razões pelas quais o conceito clássico da privacidade apresentava caráter eminentemente individualista, entendido como *right to be let alone,* ou seja, o direito de ser deixado só. Nas palavras de Danilo Doneda: “tomado como garante de isolamento e da solidão”.[173]

Em 1890, nos Estados Unidos, matéria jornalística divulgou fotos de uma festa de casamento da filha de Samuel D. Warren, advogado, sem o consentimento dos envolvidos na reportagem. Warren, em conjunto com Luis D. Brandeis, publicou, no mesmo ano, o artigo[174] *“The right to privacy”*, propondo uma reflexão sobre o tema e sugerindo a tutela da privacidade no direito americano.

O sistema jurídico americano, à época, garantia a tutela de direitos autorais, entendido como bem jurídico passível de controle por seu titular, primordialmente quando houvesse interesse financeiro envolvido. Utilizando-se dessa premissa – controle dos direitos autorais pelo titular – Warren e Brandeis propuseram que, por analogia, o controle das informações pessoais ligadas à esfera íntima deveriam ser vistos como aspectos do direito à privacidade, por sua vez merecedor de tutela[175] pelo ordenamento.

---

[173] DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000. p.2.

[174] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Civilistica.com*, Rio de Janeiro, v.2, n.3, jul./set. 2013. Disponível em: <http://civilistica.com/the-right-to-privacy>. Acesso em: 20 abr. 2015. Warren foi nomeado para a Suprema Corte Americana.

[175] *"The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality. If we are correct in this conclusion, the existing law affords a principle from which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds."* (WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Civilistica.com*, Rio de Janeiro, v.2, n.3, jul./set. 2013. Disponível em: <http://civilistica.com/the-right-to-privacy>. Acesso em: 20 abr. 2015). Tradução livre: "O princípio que protege os escritos pessoais e todas as outras produções pessoais, não contra o roubo e a apropriação física, mas contra a publicação sob qualquer forma, não é, na realidade, o princípio da propriedade privada, mas o de uma personalidade inviolável. A lei existente oferece um princípio a partir do qual pode ser invocado para proteger a privacidade do indivíduo de invasão, seja pela imprensa muito empreendedora, o fotógrafo ou o possuidor de qualquer outro dispositivo moderno para reformular ou reproduzir cenas ou sons."

Como verdadeiros pais fundadores da privacidade no terreno jurídico[176], Warren e Brandeis inauguraram um amplo debate, que persiste até hoje, acerca da tutela efetiva do direito à privacidade.

Neste momento embrionário, a sua proteção, portanto, não passava de impor aos outros um verdadeiro dever geral de abstenção, de não fazer, no afã de impedir a invasão de um espaço reservado exclusivamente ao titular do direito, na esteira da tutela da propriedade privada.[177]

Ilustra esta fase a Declaração Universal dos Direitos Humanos, aprovada através da resolução 217 A (III) da Assembleia Geral das Nações Unidas, de 10 de dezembro de 1948, surgida logo após a Segunda Guerra Mundial, com o objetivo de unir os Estados Europeus no respeito à Lei, democracia, direitos humanos e desenvolvimento social[178], instituindo em seu artigo 12, a seguinte previsão:

> Artigo 12. Ninguém será sujeito à interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

No mesmo turno, a Convenção Europeia dos Direitos do Homem[179], realizada em Roma no ano de 1950, também garantia o respeito pela vida privada e familiar:

> Artigo 8.º (Direito ao respeito pela vida privada e familiar)
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

---

176 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.28.

177 SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011. p.129.

178 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Handbook on European data protection law*. 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Acesso em: 08 out. 2015.

179 EUROPEAN COURT OF HUMAN RIGHTS. *Convenção Europeia dos Direitos do Homem*. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 08 out. 2015.

As disposições constantes dos dispositivos alhures demonstram que a previsão legal de privacidade dos indivíduos, neste primeiro momento, era destinada exclusivamente à garantia de isolamento, estabelecendo ainda um dever negativo ao Estado, para que não houvesse interferência indevida na esfera particular dos cidadãos, diante do clamor popular da época em razão das constantes violações.

2.1.2 Tutela dos dados pessoais

Na década de 1960, observa-se grande avanço nas tecnologias de informação e comunicação e um fluxo cada vez maior de informações pessoais dos cidadãos sendo coletadas por grandes corporações e governos. Estes começaram a armazenar, analisar e processar um volume cada vez maior de dados pessoais para satisfazer seus interesses, sejam comerciais, sejam ideológicos, muitas vezes em prejuízo à dignidade e aos direitos da personalíssimos daqueles que tinham suas informações expostas.[180]

Diante das novas tecnologias, da chamada sociedade da informação[181], percebe-se que a privacidade deixou de se restringir unicamente à garantia do anonimato, do sigilo, do direito de ser deixado só, havendo uma verdadeira *modificação do quadro geral*[182] do escopo de abrangência da privacidade, para se compreender também o controle dos dados pessoais.

A privacidade passa então a ser vista em sua definição funcional[183], de forma mais ampla e abrangente, como o direito conferido à pessoa de controle das informações pessoais que lhe dizem respeito, ou nas palavras de Rodotà, "o direito de manter o

---

180 SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011. p.129.

181 *"A expressão sociedade da informação define uma nova forma de organização social, política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações."* (VIEIRA, Tatiana Malta. *O direito à privacidade na socidedade da informação*: efetividade desse direito fundamental diante dos avanços na tecnologia da informação. 2007. Dissertação (Mestrado em Direito, Estado e Sociedade) - UNB, Brasíia, 2007. p.156.

182 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.44.

183 Ibid., p.92.

controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[184]

Identifica-se, neste turno, um clamor social para que o Estado garanta mecanismos efetivos mínimos de proteção da privacidade, através de sua função promocional[185], com o fito de permitir o exercício da autonomia individual, da liberdade, ou seja, da busca pelo livre desenvolvimento da personalidade humana.[186]

A esfera privada, com efeito, passa a ser definida como o conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo[187], sendo razoável concluir que não se liga, necessariamente, ao secreto, mas substancialmente ao pessoal.

Nesta seara, o direito à privacidade não se coloca mais como um mero privilégio, restrito a determinada casta social com poder para garanti-la, mas radiando-se para toda a coletividade, e entendida, inclusive, como direito fundamental.[188]

Cumpre salientar que, diante da ausência de definição legal do conceito de privacidade, parece mais acertado entendê-la de forma ampla[189], seja nos aspectos

---

184 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.15.

185 BOBBIO, Norberto. *A função promocional do direito*: da estrutura à função: novos estudos da teoria do direito. Rio de Janeiro: Manole, 2007.

186 BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*, Rio de Janeiro, v.3, n.2, jul./dez. 2014. Disponível em: <http://civilistica.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-dadignidade-da-pessoa-humana>. Acesso em: 23 abr. 2015.

187 RODOTÀ, op cit., p.92.

188 Constituição Federal de 1988: “Art. 5.º. X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.”
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) [...] A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

189 SILVA, José Afonso da. *Curso de direito constitucional positivo*. 22.ed. São Paulo: Revista dos Tribunais, 2003. p.205.

atinentes à intimidade e ao sigilo, seja naquilo que concerne ao controle efetivo, pelo titular do direito, das informações pessoais que o identificam, que lhe caracterizam como indivíduo e lhe dizem respeito[190], acrescentando ainda que “um dos conceitos mais influentes a respeito da privacidade é a idéia de controle sobre informações e dados pessoais”.[191]

Deve-se destacar que a privacidade, como direito da personalidade, é irrenunciável, porém seu exercício pode sofrer limitação voluntária pelo titular se assim o desejar, com vistas a satisfazer e permitir o protagonismo do indivíduo em sua livre formação e identificação pessoal e social, valendo destacar o Enunciado 4 da I Jornada de Direito Civil: "Art.11: o exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral".

2.2 **Modelos de proteção dos dados pessoais**[192]

É certo que não há, no mundo, unanimidade naquilo que se refere à forma de proteção privacidade com ênfase na tutela dos dados pessoais. O assunto é tratado de maneira esparsa por razões políticas, econômicas, de territorialidade e soberania,

---

[190] Vozes na doutrina advogam pelo descolamento da proteção de dados como um direito da personalidade, autônomo, diverso da privacidade. Apesar do profundo respeito a esta tese, nesta dissertação, a tutela de dados pessoais será entendida como desdobramento do atual conceito do direito à privacidade. "Por isso, advoga-se para a alocação do direito à proteção dos dados pessoais como uma nova espécie do rol aberto dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana. A proteção dos dados pessoais deve se desprender de amarras conceituais e da dinâmica de proteção própria de proteção do direito à privacidade. A proteção dos dados pessoais reclama uma normatização própria a regular o fluxo informacional como fator promocional da tutela da pessoa humana, cujo livre desenvolvimento da personalidade está, cada vez mais, a ele atrelado." (BIONI, Bruno R. *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. p.128-129).

[191] LEONARDI, Marcel. Marco civil da internet e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.518.

[192] Neste tópico, não se pretende esgotar o tema, tampouco fornecer uma análise da tutela jurídica dos dados pessoais em todos os ordenamentos jurídicos. Na verdade, o estudo pretende se concentrar em breve análise dissertativa da regulamentação da privacidade em alguns países do continente Europeu, bem como nos Estados Unidos da América.

as quais não se pretende esgotar, sendo salutar, no entanto, o estudo de alguns dos modelos de proteção dos dados pessoais atualmente existentes, como se verá nos itens a seguir.

2.2.1 O cenário europeu de proteção de dados

O clamor social pela proteção da privacidade, inicialmente concebida como o direito de ser deixado só, até sua moderna concepção, entendida como direito à autodeterminação informativa, trouxe consigo, ao longo do século XIX, inúmeras leis[193] e constituições nacionais, sobretudo no continente europeu.

Na década de 1960, as chamadas leis de primeira geração tutelavam a privacidade em resposta direta às violações dos espaços de intimidade que o avanço da tecnologia impunha. Eram concebidas através de uma lógica de troca, garantindo de maneira individual e isolada o acesso aos bancos de dados contendo informações pessoais, geralmente mantidos pelo Poder Público, em razão do fornecimento destes dados pelos indivíduos.[194]

Nesta esteira, a Alemanha é considerada a pioneira[195] em legislação específica sobre proteção de dados pessoais, tendo editado norma sobre o assunto em 1970, conhecida como *The Hesse Data Protection Act*.[196]

---

193 "Mas não é apenas o cenário tecnológico que se transforma: também muda profundamente o ambiente jurídico-institucional." (RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.44).

194 Ibid., p.49. Ainda neste sentido: CERVASIO, Daniel Bucar. *Privacidade e banco de dados da administração pública*. Dissertação (Mestrado em Direito Civil) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

195 “Como resultado de diferentes processos históricos e culturais, a Alemanha desenvolveu arcabouço legal no campo da proteção de dados pessoais reconhecido como pioneiro e entre os mais robustos do mundo. Vale notar, por exemplo, que a Lei de Proteção de Dados do estado federal de Hesse, que entrou em vigor em 1970, é considerada a primeira lei formal de proteção de dados do mundo.” (ALEMANHA. *Divisão da Sociedade da Informação*. Disponível em: <http://participacao.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/23-Alemanha.pdf>. Acesso em: 21 abr. 2015).

196 *“To cite a few examples, the Hesse Parliament adopted the Data Protection Act in September 1970. The Swedish government responded to the Computers and Privacy report by passing the Data Act, the first national data protection legislation, and creating the Data Inspection Board in 1973. In the Netherlands, legislation was proposed in 1981, leading to the Act on Personal Data*

Nesta época, o Governo Federal Alemão iniciava a aquisição de grandes computadores com larga capacidade de armazenamento e processamento de dados pessoais, o que gerou grande preocupação da população local, sobretudo em razão de seu passado sombrio.

Esta Lei, portanto, demonstrava um caráter vertical, tutelando a relação entre cidadãos e Estado, e deixava claro, pela primeira vez, que a pessoa que tivesse seus dados coletados teria assegurado o direito de ter acesso a eles, além de direito de corrigir informações imprecisas e impedir ou interromper eventual coleta ou tratamento ilícito de seus dados. Além disso, ela criou uma autoridade externa e independente para receber e direcionar as reclamações em caso de coleta, violação ou tratamento ilícito de dados pessoais.

Registrations and the creation of the data protection authority in 1988. The U.S. Freedom of Information Act was enacted in 1966, the Fair Credit Reporting Act was enacted in 1970, and the Privacy Act was passed in 1974. The French (Tricot) Commission led to the Law on Informatics and Freedom in 1978, and the creation of La Commission nationale de l'informatique et des libertés (CNIL), the French data protection agency. New Zealand set up its first Privacy Commissioner in 1976 to oversee a national law enforcement database and gave the new Human Rights Commission a broad policy remit the following year. The Canadian Human Rights Act of 1977 contained a set of fair information practices for the federal public sector. The Federal Republic of Germany, Norway, Denmark, Austria and Luxembourg also passed legislation before the end of the decade. As a result, more than a third of the then 24 OECD member countries had adopted national legislation by 1980." (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016). Tradução livre: "Para citar alguns exemplos, o Parlamento de Hesse aprovou a Lei de Proteção de Dados em Setembro de 1970. O Governo sueco respondeu ao relatório sobre Informática e Privacidade através da adoção da Lei de Dados, a primeira legislação nacional de proteção de dados. Nos Países Baixos, foi proposta legislação em 1981, que conduziu à Lei sobre Registo de Dados Pessoais e à criação da autoridade de proteção de dados em 1988. A Lei de Liberdade de Informação foi promulgada em 1966, a Fair Credit Reporting Act foi promulgada em 1970, e a Lei de Privacidade foi aprovada em 1974. A Comissão Francesa (Tricot) levou à Lei da Informática e da Liberdade em 1978, e à criação da Comissão Nacional de Informática e Liberdade (CNIL). A Nova Zelândia criou seu primeiro Comissário de Privacidade em 1976 para supervisionar um banco de dados nacional de aplicação da lei e deu à nova Comissão de Direitos Humanos uma ampla política de remissão no ano seguinte. A Lei Canadense de Direitos Humanos de 1977 continha um conjunto de práticas justas de informação para o setor público federal. A República Federal da Alemanha, a Noruega, a Dinamarca, a Áustria eo Luxemburgo também aprovaram legislação antes do final da década. Consequentemente, mais de um terço dos então 24 países membros da OCDE tinha adotado legislação nacional até 1980."

Na França, a primeira Lei de proteção de dados pessoais foi promulgada em 1978, criando a autoridade garante denominada CNIL – Comissão Nacional de Processamento de Dados e Liberdades.[197]

É possível observar que estas primeiras leis sobre proteção de dados tinham como escopo de tutela o processamento automatizado das informações dos indivíduos, ou seja, os grandes bancos de dados sobre a população que começavam a ser construídos em razão da disponibilização de computadores com esta finalidade específica, uma novidade à época, como afirmou relatório da OECD[198] em 1976:

> *A Synthesis Report was prepared by the OECD Secretariat in 1976. The Report succinctly stated the policy problem that the seminar was attempting to address and offered some possible solutions: Innovations in modern information technology, especially computers and telecommunications, bring new dimensions to traditional methods of record-keeping. They have also sharpened public awareness of the human value, "privacy", which may face major changes as the use of automated information and transmission systems expands. What is at stake is the societal control of modern information*

---

197 *"Created in 1978, the CNIL is an independent administrative authority that exercises its functions with accordance to the French Data Protection Act of the 6th of January 1978, amended the 6th of August 2004."* (CNIL. *Status & Composition*. Disponível em: <https://www.cnil.fr/en/node/287>. Acesso em: 25 nov. 2016). Tradução livre: "Criada em 1978, a CNIL é uma autoridade administrativa independente que exerce as suas funções em conformidade com a Lei Francesa de Proteção de Dados de 6 de Janeiro de 1978, alterada em 6 de Agosto de 2004."

198 *"The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies. The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD."* (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016). Tradução livre: "A OCDE é um fórum único onde os governos trabalham em conjunto para enfrentar os desafios econômicos, sociais e ambientais da globalização. A OCDE também está na vanguarda dos esforços para entender e ajudar os governos a responder a novos desenvolvimentos e preocupações, como governança corporativa, a economia da informação e os desafios do envelhecimento da população. A Organização oferece um cenário onde os governos podem comparar experiências políticas, buscar respostas para problemas comuns, identificar boas práticas e trabalhar para coordenar as políticas nacionais e internacionais. Os países membros da OCDE são: Austrália Alemanha, Áustria, Bélgica, Canadá, Estados Unidos, Estónia, Finlândia, França, Grécia, Hungria, Islândia, Irlanda, Israel, Itália, Japão, Coréia, Luxemburgo, México, Países Baixos, Nova Zelândia, Noruega, República Checa, Polónia, Portugal, República Eslovaca, Eslovénia, Espanha, Suécia, Suíça, Turquia, o Reino Unido e os Estados Unidos."

> *technology, and while the past decade has seen a "literature of alarm", the 1970s will be dedicated to the development of "social software" in the form of laws, regulations, codes of ethics, etc., necessary to control information technology and ensure that its development will be, on balance, of a positive dimension to humanity.*[199]

Luxemburgo seguiu caminho similar em 1979, Holanda em 1988, Portugal em 1991, Bélgica e Espanha em 1992. Em 1997, Itália e Grécia aprovaram leis específicas neste mesmo sentido.[200]

A Constituição de Portugal, promulgada em 1979 e alterada em 2005, em seu artigo 35, estabelece regras para controle dos dados pessoais informatizados[201], fixando como um dos nortes o respeito à privacidade dos indivíduos.

---

[199] Tradução livre: "Um relatório de síntese foi preparado pelo Secretariado da OCDE em 1976. O Relatório resumiu sucintamente o problema político que o seminário estava tentando abordar e ofereceu algumas soluções possíveis: As inovações nas modernas tecnologias da informação, especialmente computadores e telecomunicações, trazem novas dimensões aos métodos tradicionais de manutenção de registros. Eles também têm aumentado a consciência pública do valor humano, "privacidade", que pode enfrentar grandes mudanças à medida que o uso de sistemas automatizados de informação e transmissão se expande. O que está em jogo é o controle social da tecnologia da informação moderna, e enquanto a década passada tem visto uma "literatura de alarme", a década de 1970 será dedicada ao desenvolvimento de "software social" sob a forma de leis, regulamentos, códigos de Ética, etc., necessárias para controlar a tecnologia da informação e assegurar que o seu desenvolvimento seja, de forma equilibrada, uma dimensão positiva para a humanidade."

[200] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p.17.

[201] Artigo 35.º "Utilização da informática 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

Em 19 de junho de 1992, a Suíça editou Lei denominada *Federal Act on Data Protection*, onde em seu artigo 12 cujo título é *breaches of privacy*, criando regras[202] para proteção da privacidade dos dados pessoais.

Em 1981, o Conselho da Europa[203] aprovou a Convenção 108, que trata da proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, sendo ratificada por todos os Estados Membros da União Europeia. Esta convenção constitui documento legal vinculante na União Europeia no campo da proteção de dados pessoais, aplicando em qualquer situação de captação, armazenamento e tratamento de dados pessoais ocorridos dentro do território comunitário, seja com entes públicos ou privados.

A Diretiva n.º 95/46/CE do Parlamento Europeu de 24/10/1995, estabelece que os sistemas de tratamento de dados devem respeitar as liberdades e os direitos fundamentais do homem, especialmente a vida privada. Em seu artigo 23 institui[204] e reconhece que qualquer pessoa que tiver sofrido prejuízo em razão de tratamento ilícito de dados tem o direito de obter do responsável a reparação pelo dano sofrido.

---

202 *"Section 3: Processing of Personal Data by Private Persons Art. 12 Breaches of privacy 1 Anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so. 2 In particular, he must not: a. process personal data in contravention of the principles of Articles 4, 5 paragraph 1 and 7 paragraph 1; b. process data pertaining to a person against that person's express wish without justification; c. disclose sensitive personal data or personality profiles to third parties without justification.1 3 Normally there is no breach of privacy if the data subject has made the data generally accessible and has not expressly prohibited its processing."* Tradução livre: "Secção 3: Tratamento de Dados Pessoais por Particulares Art. 12 Violações da privacidade 1 Qualquer um que processe dados pessoais não deve violar ilegalmente a privacidade das pessoas em causa ao fazê-lo. 2 Em particular, não deve: a. Processar dados pessoais em violação dos princípios dos artigos 4.º, 5.º, n.º 1, e 7.º, n.º 1; B. Processar dados relativos a uma pessoa contra o desejo expresso dessa pessoa sem justificação; C. Divulgar dados pessoais sensíveis ou perfis de personalidade a terceiros sem justificação.1 3 Normalmente, não há violação de privacidade se a pessoa em causa tiver tornado os dados geralmente acessíveis e não tenha expressamente proibido o seu processamento."

203 COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>. Acesso em: 10 dez. 2016.

204 Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido.

Na Italia em dezembro de 1996 foi criada a Lei de Proteção de Dados, Lei n.º 675[205], que criou a autoridade Garante Italiana, composta por 4 membros, sendo 2 eleitos pela Câmara dos Deputados e 2 pelo Senado. Estes 4 membros então elegem um presidente, que terá voto decisivo quando houver empate entre os 4 membros eleitos.

Esta Lei foi depois substituída pelo Código Italiano de Proteção de Dados, através do Decreto Legislativo 196[206] de 30 de junho 2003, que consolidou e reuniu toda a tutela dos dados pessoais[207] naquele país em um único documento.[208] A iniciativa teve origem no Poder Executivo, em razão da autorização prevista nos artigos 76 e 87 da Constituição Italiana, bem como inúmeras Leis que o autorizam a regulamentar e legislar a proteção de dados pessoais.

O Código Italiano de Proteção de Dados se divide em três partes. A primeira delas define os princípios gerais de tutela dos dados, que se aplicam a todas as organizações. A segunda parte traz medidas adicionais específicas, que devem ser tomadas por organizações em determinadas áreas, como por exemplo, saúde, telecomunicações, bancos e recursos humanos. Já a terceira parte se refere às sanções e medidas corretivas.

O Código se coloca aplicável a qualquer evento de coleta, processamento e armazenamento de dados pessoais dentro do território Italiano, bem como às organizações externas que se utilizam de equipamentos localizados na Itália.

---

205 Atualizada pelos decretos legislativos: n.º 123 de 09.05.1997, n.º 255 de 28.07.1997, n.º 135 de 08.05.1998, n.º 171 de 13.05.1998, n.º 389 de 6.11.1998, n.º 51 de 26.02.1999, no. 135 de 11.05.1999, n.º 281 de 30.07.1999, n.º 282 de 30.07.1999 and n.º 467 de 28.12.2001. (ITALIA. Protection of individuals and other subjects with regard to the processing of personal data. ACT no. 675 of 31.12.1996. Disponível em: <http://www.privacy.it/legge675encoord.html>. Acesso em: 1.º nov. 2015).

206 ITALIA. Garante per la protezione dei dati personali. Disponível em: <http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf>. Acesso em: 20 nov. 2015.

207 “Seção 1 (Direito à proteção dos dados pessoais) - Art 1 - Toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito. Seção 2 (Propósitos) - Art. 1 - Este estatuto consolidado, a seguir denominado "Código", deve assegurar que os dados pessoais serão tratados respeitando os direitos das pessoas (data subject), as liberdades fundamentais e a dignidade, em particular no que diz respeito à confidencialidade, à identidade pessoal e o direito à proteção de dados pessoais.”

208 ITALIA. Data Protection Code - Legislative Decree n.º 196/2003. Disponível em: <http://www.garanteprivacy.it/home_en/italian-legislation#1>. Acesso em: 1.º dez. 2015.

Além disso, caso uma pessoa física ou jurídica, localizada fora da Comunidade Europeia estiver processando dados dentro do território italiano, deverá necessariamente nomear um representante legal na Itália, de forma a garantir aplicação das regras previstas na legislação.

Estabelece direito de petição, para que o interessado tenha conhecimento de eventual existência de coleta, armazenamento ou tratamento de seus dados pessoais para qualquer pessoa, inclusive garantido pedido de retificação ou bloqueio, sem qualquer formalidade, prevendo a possibilidade de reclamações verbais, que devem ser aceitas e reduzidas a termo pelo reclamado.[209]

Prevê ainda o princípio da finalidade[210], informação e consentimento[211] expresso para coleta e tratamento de dados, traz regras de responsabilidade civil para reparação[212] de danos em caso de tratamento ilícito dos dados pessoais, e determina[213] que a autoridade garante funcione de maneira totalmente autônoma e independente nas suas decisões e avaliações, bem como estabelece que os membros não podem exercer

---

[209] Artigo 9. 1 - O pedido dirigido ao controlador ou processante dos dados também pode ser transmitido por meio de carta registrada, fax ou e-mail. O Garante pode especificar outras disposições adequadas no que diz respeito a novas soluções tecnológicas. Se o pedido for relacionado ao exercício dos direitos referidos na secção 7 (1) e (2), ele também pode ser feita verbalmente; neste caso, será escrito de forma sumária ou por uma pessoa designada pelo processante de dados." Título II do Decreto Legislativo n.º 196.

[210] Título III, Capítulo I, Artigo 11. "exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas." (MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014. p.70-71).

[211] Título III, Capítulo I, Artigo 13/Capítulo III, Artigo 23.

[212] Artigo 15 - 2. "Compensação por danos não-patrimoniais devem ser também devidos em razão de violação do artigo 11.
Artigo 11 –
1. Os dados pessoais objeto de tratamento serão:
a) processado legalmente e de forma justa;
b) coletados e gravados para finalidades determinadas, explícitas e legítimas, e utilizado em outras operações de processamento de uma maneira que não seja incompatível com os referidos fins;
c) exatos e, quando necessário, mantidos atualizados;
d) relevantes, completos e não excessivos em relação aos fins para os quais foram recolhidos ou posteriormente tratados;
e) conservados de forma a permitir a identificação da pessoa apenas durante o período necessário para os fins para os quais os dados foram recolhidos ou posteriormente tratados.
2. Quaisquer dados pessoais que forem processados em violação das disposições pertinentes sobre o tratamento de dados pessoais não poderão ser utilizados."

[213] Título II, Capítulo I, Artigo 153.

qualquer atividade profissional, inclusive não podem dar aulas em Universidades. A remuneração máxima será a equiparada aos Juizes da *Corte di Cassazione*.

Na Europa, em julho de 2002, o Parlamento Europeu editou a Diretiva n.º 2002/58/CE, que versa exclusivamente de tratamento de dados pessoais e à proteção da privacidade das comunicações eletrônicas[214], protegendo, neste âmbito, a privacidade em seu artigo 13[215], na medida em que determina a necessidade de consentimento expresso do indivíduo para que este possa receber qualquer "chamada automatizada sem intervenção humana".[216]

Esta diretiva tem como objetivo garantir que haja harmonização da tutela dos dados pessoais em toda comunidade Europeia, bem como impedir que os Estados promulguem leis que fragilizem as garantias mínimas previstas na regulamentação.[217] Veio também para dar força aos princípios estabelecidos pela Convenção 108 e fortalecer a sua aplicação, se aplicando a todos os 28 Estados Europeus, além de Islândia, Liechtenstein e Noruega, conforme acordo sobre o Espaço Económico Europeu[218] de 1994.

Interpretando o arcabouço jurídico de tutela de dados pessoais na Europa, durante o julgamento Processo C-131/12, a Corte de Justiça Europeia, na análise do caso *Google Spain SL e Google Inc*. contra *Agencia Española de Protección de*

---

214 Em seu preâmbulo, o Parlamento Europeu pondera que "A internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infra-estrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações electrónicas. Os serviços de comunicações electrónicas publicamente disponíveis através da internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade." Íntegra: UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:pt:PDF>. Acesso em: 10 dez. 2016.

215 Artigo 13. "Comunicações não solicitadas 1. A utilização de sistemas de chamada automatizados sem intervenção humana (aparelhos de chamada automáticos), de aparelhos de fax ou de correio electrónico para fins de comercialização directa apenas poderá ser autorizada em relação a assinantes que tenham dado o seu consentimento prévio."

216 Trata-se do mecanismo de *opt-in*. Para maiores detalhes: MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na internet*. São Paulo: Revista dos Tribunais, 2008. p.212-214.

217 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Handbook on European data protection law*. 2014. p.18. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Acesso em: 08 out. 2015.

Datos (AEPD) entendeu que as diretivas europeias são aplicáveis mesmo se os servidores que processam os dados estão localizados fora do território comum europeu, desde que haja representação da entidade no país-membro.[219]

Em 26 de outubro de 2012, o Parlamento Europeu, o Conselho e a Comissão proclamaram a Carta dos Direitos Fundamentais da União Europeia, contendo em seu preâmbulo a seguinte passagem: “Para o efeito, é necessário, conferindo-lhes maior visibilidade por meio de uma Carta, reforçar a proteção dos direitos fundamentais, à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica”.

Além de estabelecer o princípio da dignidade humana em seu primeiro artigo[220], pondo a pessoa no centro do ordenamento, a Carta de 2012 traz ainda o respeito à privacidade[221] e a proteção dos dados pessoais[222], com a exigência do consentimento, o princípio da finalidade e lealdade no tratamento das informações que dizem respeito aos indivíduos. Reitera ainda a necessidade de fiscalização do cumprimento de tais regras, através das autoridades garantes nacionais, como é de praxe na Europa.

---

218 EUROPA. Acordo sobre o Espaço Económico Europeu. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:21994A0103(01)&from=EN>. Acesso em: 08 out. 2015.

219 "Nos termos do artigo 4.º, n.º 1, um Estado Membro aplicará as suas disposições nacionais adotadas por força da diretiva ao tratamento de dados pessoais quando houver um estabelecimento do responsável pelo tratamento situado no território desse Estado Membro ou, nos casos em que o responsável pelo tratamento não estiver estabelecido na União, se recorrer, para tratamento de dados pessoais, a meios situados no território desse Estado Membro." Íntegra do julgamento: THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). C-131/12. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>. Acesso em: 20 nov. 2016.

220 “TÍTULO I - DIGNIDADE. Artigo 1.º Dignidade do ser humano A dignidade do ser humano é inviolável. Deve ser respeitada e protegida.”

221 “Artigo 7.º Respeito pela vida privada e familiar Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.”

222 “Artigo 8.º Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

Note-se ainda que, recentemente, a Diretiva n.º 95/46/CE foi revogada[223] pelo Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, em 27 de abril de 2016.

Este novo regulamento já se encontra em vigor, porém será aplicável a partir de 25 de maio de 2018 e traz em seu preâmbulo a seguinte consideração:

> A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.o, n.o 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.o, n.o 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Em razão do Regulamento n.º 679 e da constante evolução tecnológica, a Comissão Europeia lançou uma proposta[224], em 10 de janeiro de 2017, para revogação da Diretiva n.º 2002/58/CE, propondo um regulamento diretamente aplicável a todos os Estados membros, na tentativa de ampliar ainda mais a tutela da privacidade nas comunicação eletrônicas, bem como harmonizar e atualizar[225] a sua proteção.

A análise destas singelas considerações revela que a comunidade europeia adota uma significativa regulamentação da questão concernente à privacidade dentro do bloco comum, motivado, em grande parte pelo passado recheado de regimes autoritários, que perseguiam parcela da população: *"Europe's past history with fascist and totalitarian*

---

223 "CAPÍTULO XI. Disposições finais Artigo 94.o Revogação da Diretiva 95/46/CE 1. A Diretiva 95/46/CE é revogada com efeitos a partir de 25 de maio de 2018".

224 COMISSÃO EUROPEIA. Comunicado de imprensa. Comissão propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrónicas e atualiza as regras de proteção de dados para as instituições da EU. Bruxelas, 10 de janeiro de 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017.

225 *"Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services."* (EUROPEAN COMMISSION. *Proposal for a Regulation of the European Parliament and of the Council*. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017). Tradução livre: "Consequentemente, a diretiva não acompanhou o ritmo da evolução tecnológica, resultando num vazio de proteção das comunicações transmitidas através de novos serviços."

regimes clearly informs its views on data protection and contributes to the demands from European politicians and publics for strict data privacy controls".[226]

[226] WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016. Tradução livre: " A história passada da Europa com regimes fascistas e totalitários informa claramente as suas visões sobre a proteção de dados e contribui para as exigências dos políticos e público europeus para controles rigorosos do controle de dados pessoais."

2.2.2 A proteção dos dados pessoais nos EUA

Ao contrário dos países Europeus que contam com vasta proteção da privacidade em textos constitucionais, tratados internacionais, diretivas e regulamentos, não há no sistema americano previsão expressa[227] na Constituição acerca deste instituto como um direito fundamental, uma cláusula geral, horizontalmente aplicável:

> *U.S. and EU privacy law diverge greatly. At the foundational level, they differ in their underlying philosophy: In the United States, privacy law focuses on redressing consumer harm and balancing privacy with efficient commercial transactions. In the European Union, privacy is hailed as a fundamental right that can trump other interests*.[228]

Frise-se que a quarta emenda[229] à Constituição Americana tem sido aplicada pela Suprema Corte como norma tuteladora da privacidade[230] para determinados casos específicos.[231]

---

227 *"While the US Constitution nowhere expressly establishes a general right to privacy, certain of the amendments to the Constitution explicitly of inferentially confer specific privacy rights."* (BRENNER, Susan W. Constitutional rights and the new technologies in the United States. In: LEENES, Ronald; KOOPS, Bert-Jaap; HERT, Paul de. *Constitutional rights and new technologies*: a comparative study. New York: Cambridge University Press, 2008. p.230). Tradução livre: "Embora a Constituição dos Estados Unidos em nenhum lugar estabeleça expressamente um direito geral à privacidade, algumas das emendas à Constituição explicitamente de inferencialmente conferem direitos específicos de privacidade."

228 SCHWARTZ, Paul M.; SOLOVE, Daniel J. Reconciling Personal Information in the United States and the European Union. *California Law Review*, v.102, n.4, 2014. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4252&context=californialawreview>. Acesso em: 25 nov. 2016. Tradução livre: "A lei de privacidade dos EUA e da UE divergem muito. No nível fundacional, eles diferem em sua filosofia subjacente: Nos Estados Unidos, a lei de privacidade se concentra em corrigir os danos ao consumidor e equilibrar a privacidade com transações comerciais eficientes. Na União Europeia, a privacidade é saudada como um direito fundamental que pode ultrapassar outros interesses."

229 *"Amendment IV. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."* Tradução livre: "Emenda IV O direito do povo de estar seguro em suas pessoas, casas, papéis e efeitos, contra buscas e apreensões não razoáveis, não será violado, e nenhum mandado emitirá, senão por causa provável, apoiado por juramento ou afirmação, e descrevendo particularmente o lugar a ser pesquisado, e as pessoas ou coisas a serem apreendidas."

Faz-se possível afirmar que a regulamentação dos dados pessoais nos Estados Unidos da América se mostra visivelmente menos enfática e garantista quando confrontada com a Europa:

> *Many U.S. officials and industry representatives maintain that the U.S. approach to data privacy is more nimble than what they view as the EU's "one-size-fits-all" approach. They also contend that the U.S. approach helps to promote and sustain U.S. technological innovation*.[232]

Diante deste quadro, o caminho norte-americano aduz que a regulamentação da privacidade acaba sendo direcionada do cidadão para o Estado[233], similar aos primórdios legislativos verificados na Europa em meados do século XX.

A tutela dos dados pessoais entre particulares é vista, tão somente, para questões específicas, a depender do tipo de atividade e do local onde ela se desenvolva, opondo-se à regulamentação abrangente que se vê no velho continente, aplicável a toda e qualquer atividade envolvendo dados pessoais: *"These sector-specific laws create privacy safeguards that apply only to specific types of entities*

---

230 *"This sections immediately below explain how the Fourth Amendment – wich is the most important guarantor of privacy for US citizens – constrains official efforts at data-gathering."* (BRENNER, Susan W. Constitutional rights and the new technologies in the United States. In: LEENES, Ronald; KOOPS, Bert-Jaap; HERT, Paul de. *Constitutional rights and new technologies*: a comparative study. New York: Cambridge University Press, 2008. p.231). Tradução livre: "Estas seções imediatamente abaixo explicam como a Quarta Emenda – que é o garante mais importante da privacidade para os cidadãos dos EUA – restringe os esforços oficiais na coleta de dados"

231 *Boyd v United States; Olmstead v United States; United States v Miller; United States V Knotts; Kyllo v United States.*

232 WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016. Tradução livre: "Muitos funcionários dos EUA e representantes da indústria sustentam que a abordagem dos EUA à privacidade dos dados é mais ágil do que o que eles consideram a abordagem da UE 'one-size-fits-all'. Eles também afirmam que a abordagem americana ajuda a promover e sustentar a inovação tecnológica dos EUA."

233 "*Unlike the situation in Europe, therefore, privacy in the U.S. (as a constitutional right) has been tailored to be exclusively asserted against the State – even though specific statutory laws have subsequently endorsed a legal right to privacy enforceable also against the private sector by means of a 'sectoral approach'."* (DE FILIPPI, Primavera; BELLI, Luca. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal for Law and Technology*, v.3, n.2, p.3, 2012). Tradução livre: "Ao contrário da situação na Europa, portanto, a privacidade nos EUA (como um direito constitucional) foi adaptada para ser exclusivamente afirmado contra o Estado – apesar de leis estatutárias específicas subscreveram posteriormente um direito legal à privacidade também aplicável ao setor privado por meio de uma 'abordagem setorial'."

and data. With a few exceptions, individual states and the federal government have predominantly enacted privacy laws on a sectoral basis".[234]

Ademais, a própria abordagem da tutela dos dados pessoais acaba de mostrando distinta entre Europa e EUA, como se vê da seguinte constatação:

> *For instance, in the United States, what the European Commission (the EU's executive) refers to as the "collecting and processing of personal data" is allowed unless it causes harm or is expressly limited by U.S. law. In Europe, by contrast, processing of personal data is prohibited unless there is an explicit legal basis that allows it*.[235]

Dentre as atividades cuja regulação de dados pessoais atinge de maneira específica, vale destacar a *"Fair Credit Reporting Act"* de 1970, com vistas a promover regras aptas a garantir a privacidade e normas de conduta adequadas diante das informações pessoais nas agências de avaliação de crédito. Deve ser mencionado ainda a *"Health Insurance Portability and Accountability Act"* de 1996, que trouxe o direito à privacidade das informações para as empresas do sector da saúde.

A chamada *"Children's Online Privacy Protection Act (COPPA)"* no ano 2000 – foi criada para proteger especificamente a privacidade das crianças abaixo de 13 anos, onde deverá ser solicitando o consentimento dos pais para a coleta ou uso de qualquer informação pessoal.

---

[234] WHITE HOUSE. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 ago. 2015. Tradução livre: "Essas leis específicas de setor criam salvaguardas de privacidade que se aplicam apenas a tipos específicos de entidades e dados. Com algumas exceções, os estados individuais e o governo federal predominantemente promulgaram leis de privacidade em uma base setorial."

[235] WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016. Tradução livre: "Por exemplo, nos Estados Unidos, o que a Comissão Européia (o executivo da UE) designa como "coleta e processamento de dados pessoais" é permitido, a menos que cause danos ou seja expressamente limitado pelo direito dos Estados Unidos. Na Europa, pelo contrário, o tratamento de dados pessoais é proibido, a menos que exista uma base jurídica explícita que o permita."

Destaca-se ainda os acordos de transferência de dados entre Europa e Estados Unidos, dentre eles o *Safe Harbour*, criado em 2000[236] e declarado inválido[237] pela Corte de Justiça da União Europeia em 06 de outubro de 2015, após julgamento do caso C-362/14 – Maximillian Schrems contra Data Protection Commissioner[238], além do recentíssimo Privacy Shield[239], anunciado[240] em fevereiro de 2016, porém pendente

---

236 *"In 2000, the U.S. Department of Commerce issued the Safe Harbor Privacy Principles, which were subsequently recognized by the European Commission."* (WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016). Tradução livre: "Em 2000, o Departamento de Comércio dos EUA emitiu os Princípios de Privacidade de Safe Harbor, que foram posteriormente reconhecidos pela Comissão Europeia."

237 *"Finally, the Court finds that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Court holds that the Commission did not have competence to restrict the national supervisory authorities powers in that way. For all those reasons, the Court declares the Safe Harbour Decision invalid."* (THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Judgment in Case C-362/14 - Maximillian Schrems v Data Protection Commissioner. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>. Acesso em: 27 ago. 2016.). Tradução livre: "Por último, o Tribunal considera que a decisão Safe Harbor nega às autoridades nacionais de supervisão as suas competências quando uma pessoa põe em causa a compatibilidade da decisão com a proteção da vida privada e dos direitos e liberdades fundamentais dos particulares. O Tribunal de Justiça considera que a Comissão não tinha competência para restringir dessa forma as competências das autoridades nacionais de supervisão. Por todas estas razões, o Tribunal declara a Decisão Safe Harbor inválida."

238 "Reenvio prejudicial – Dados pessoais – Proteção das pessoas singulares relativamente ao tratamento desses dados – Carta dos Direitos Fundamentais da União Europeia – Artigos 7.°, 8.° e 47.° – Diretiva 95/46/CE – Artigos 25.° e 28.° – Transferência de dados pessoais para países terceiros – Decisão 2000/520/CE – Transferência de dados pessoais para os Estados Unidos – Nível de proteção inadequado – Validade – Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos – Poderes das autoridades nacionais de controlo". Íntegra do julgamento: THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Processo C-362/14. Disponível em: <http://curia.europa.eu/juris/documents.jsf?num=C-362/14>. Acesso em: 27 ago. 2016.

239 "*The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. On July 12, the European Commission deemed the Privacy Shield Framework adequate to enable data transfers under EU law."* (PRIVACY SHIELD. *Privacy Shield Program Overview*. Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em: 25 nov. 2016). Tradução livre: "A plamaforma EU-U.S. Privacy Shield foi concebida pelo Departamento de Comércio dos EUA e pela Comissão Europeia para fornecer às empresas de ambos os lados do Atlântico um mecanismo para cumprir os requisitos da UE de proteção de dados ao transferir dados pessoais da União Europeia para os Estados Unidos em apoio ao comércio transatlântico. Em 12 de julho, a Comissão Européia considerou o Privacy Shield Framework adequado para permitir transferências de dados sob a legislação da UE."

de aprovação pelas autoridades europeias para que suas previsões passem a ser válidas e eficazes.

Tais regras entre EUA e Europa são vitais para a transferência de dados entre os entes, especialmente por que a grande maioria das empresas de tecnologia que utilizam dados pessoais como principal ativo se encontram em solo norte-americano, porém seus usuários não encontram fronteiras, se espalhando por todo mundo. Além disso, o volume de negócios entre os blocos é um dos mais relevantes para o comércio mundial.[241]

Com base naquilo que foi acima exposto, conclui-se que enquanto no Velho Continente se enxerga com clareza uma profunda e eficaz regulação da privacidade, especificamente dos dados pessoais, nos EUA o tema é tratado de maneira rasa[242], inexistindo direito fundamental à privacidade ou sequer autoridades legalmente constituídas para fiscalizar e forçar o cumprimento das Lei.

---

[240] UNITED STATES DEPARTMENT OF COMMERCE. Disponível em: <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf>. Acesso em: 27 ago. 2016.

[241] *"The transatlantic flow of data is a form of international trade and is of critical importance for the U.S. and European economies. The United States and the EU remain each other's largest trade and investment partners. In 2013, total U.S.-EU trade in goods and services amounted to $1 trillion and U.S. FDI in EU totaled $2.4 trillion (or about 56%) of total U.S. direct investment abroad. Conversely, EU companies accounted for $1.7 trillion (or about 62%) of direct investment in the United States. According to a 2014 study, cross-border data flows between the United States and Europe are the highest in the world—almost double the data flows between the United States and Latin America and 50% higher than data flows between the United States and Asia."* (WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016). Tradução livre: "O fluxo transatlântico de dados é uma forma de comércio internacional e é de importância crítica para as economias dos EUA e da Europa. Os Estados Unidos e a UE continuam a ser os maiores parceiros comerciais e de investimento de cada um dos países. Os serviços totalizaram US $ 1 trilhão e o IDE dos EUA na UE totalizou US $ 2,4 trilhões (ou cerca de 56%) do total de investimento direto dos EUA no exterior, enquanto as empresas da UE representavam US $ 1,7 trilhão (ou cerca de 62%) de investimento direto nos Estados Unidos. Um estudo de 2014, os fluxos de dados transfronteiriços entre os Estados Unidos e a Europa são os mais altos do mundo - quase o dobro dos fluxos de dados entre os Estados Unidos e a América Latina e 50% mais elevados que os fluxos de dados entre os Estados Unidos e a Ásia."

[242] BAMBERGER, Kenneth; MULLIGAN, Deirdre. *Privay on the Ground*: Drivign corporate behavior in the United States and Europe. Cambridge: MIT Press, 2015. p.185.

2.3 **Aplicação dos diferentes modelos de proteção**

2.3.1 Consentimento e *big data*

Com razão se afirmou que “o consentimento é o pilar regulatório adotado para a proteção de dados pessoais”[243], funcionando, desde a década de 1990 na Europa[244] como ponto de partida a legitimar e justificar a licitude da coleta, tratamento e análise de dados do titular.

O Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho reacende esta chama em diversas passagens[245], trazendo o instituto do consentimento como a chave mestra do cofre que dá acesso aos dados pessoais, porém contemplando novas formas, além dele, que conferem licitude ao tratamento de dados.

---

243 INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?*: relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 27 ago. 2016.

244 *“At EU level, reliance on consent as a criterion for legitimising personal data processing operations was foreseen from the very beginning of the legislative process that ended with the adoption of Directive 95/46/EC.”* (EUROPEAN COMMISSION. *Opinion 15/2011 on the definition of consent.* Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016). Tradução livre: "A nível da UE, a confiança no consentimento como critério para legitimar as operações de tratamento de dados pessoais estava prevista desde o início do processo legislativo que terminou com a adopção da Diretiva 95/46/CE."

245 “O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.”

Considerando a efetiva tutela dos dados pessoais no velho continente, através das chamadas quarta geração de leis[246], que estabelecem limitações e regras rígidas sobre o consentimento[247], instituindo procedimentos estritos de coleta, tratamento, compartilhamento e armazenamento dos dados pessoais, tem-se a ideia de que seria árdua a tarefa conciliá-las[248] com o universo trazido pelo *big data*, tornando o instituto até mesmo obsoleto.[249]

No Brasil, o texto da Lei n.º 12.965/2014 – Marco Civil da Internet, notadamente em seu artigo 7.º, menciona a privacidade[250] como direito essencial ao

---

246 Sobre as gerações de leis de tutela dos pessoais: BIONI, Bruno R. *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. p.145-148.

247 "A disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais, bem como proposições normativas, que não deixaram mais ao reino do indivíduo a escolha conquanto ao processamento de certos tipos de dados pessoais (sensíveis), relativizaram, de certa maneira, a referenciada centralidade do consentimento." (Ibid., p.147).

248 *"Big data and mass surveillance are difficult to reconcile with the mandate of the European Union under Article 16 TFEU in the area of privacy and data protection."* (HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.81). Tradução livre: "Big data e vigilância em massa são difíceis de conciliar com o mandato da União Europeia nos termos do artigo 16.º TFUE na área da privacidade e da protecção de dados."

249 *"The continuous repurposing and making use of already processed or inherent data sets, has made the traditional consent models insufficient and obsolete in big data."* (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.). Tradução livre: "O reaproveitamento contínuo e o uso de conjuntos de dados já processados ou inerentes, tornaram os modelos de consentimento tradicionais insuficientes e obsoletos no big data."

250 "Art. 7.º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
[...] VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

acesso à rede mundial de computadores, trazendo ainda vários incisos quem tratam da privacidade dos usuários.

Estabelece, dentre outros, a obrigação de prestar "informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet", o "não fornecimento a terceiros de seus dados pessoais", garante a proteção dos dados e vedam a sua utilização para outros fins além daqueles expressamente autorizados, determinando ainda a necessidade de *"consentimento expresso"* na coleta e tratamento dos dados, "que deverá ocorrer de forma destacada das demais cláusulas contratuais".[251]

Em igual turno, o Anteprojeto de Lei de proteção dados pessoais traz diversas previsões contemplando a necessidade de consentimento livre e inequívoc[252], através de cláusula apartada, considerando nulo[253] quando for obtido de maneira diversa

---

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - 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;"

[251] Vale mencionar também os artigos 3, 8 e 11 do Marco Civil da Internet que também abordam a tutela da privacidade no mundo virtual.

[252] "Art 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento pelo titular de consentimento livre e inequívoco; Art. 9.º O consentimento previsto no art. 7.º, I deverá ser livre e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique.§ 1.º Caso o consentimento seja fornecido por escrito, este deverá ser fornecido em cláusula destacada das demais cláusulas contratuais.§ 2.º Cabe ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.§ 3.º É vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.§ 4.º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.§ 5.º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular.§ 6.º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 8.º, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.§ 7.º O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos."

[253] "Art. 8.º [...]
§ 1.º Na hipótese em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva."

da legislação, e ainda estabelecendo que, quando se tratar de coleta de dados de forma continuada, o titular das informações deverá ser informado com regularidade.[254]

Inobstante, a legislação mencionada informa que quando a finalidade inicial for alcançada, deve-se por fim ao tratamento de dados pessoais, o que também pode, em tese, obstaculizar muitas práticas típicas do *big data*, onde, por exemplo, em determinados casos os benefícios e resultados satisfatórios são obtidos por tratamentos secundários, distantes da finalidade inicial para a qual os dados foram coletados, diversas vezes sequer possível ou conhecida no momento da coleta dos dados.

Quando se impõe amarras expressas no tratamento, especialmente se reportando ao princípio da finalidade[255], coloca-se em cheque muitas práticas atualmente frequentes que extrem valor e benefícios diante de uma utilização secundária, muitas vezes inimaginável no momento da coleta daquele banco de dados que está sendo objeto de análise:

> *In the EU context there is a further consequence: purpose limitation is a substantive principle of EU data protection law, included in Article 8 Charter, which means, in essence, that collection of data should take place for a specific purpose.*
> *[...] However in a big data context, personal data collection takes place for unspecified purposes and on a massive scale.*[256]

---

254 "Art. 8.º [...]
§ 3.º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente."

255 REGULAMENTO (UE) 2016/679": Artigo 5.º Princípios relativos ao tratamento de dados pessoais 1. Os dados pessoais são: [...] b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);"

256 HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016. p.99. Tradução livre: "No contexto da UE, há uma outra consequência: a limitação da finalidade é um princípio substantivo da legislação da UE em matéria de proteção de dados, incluída no artigo 8.º da Carta, o que significa, essencialmente, que a coleta de dados deve ter um fim específico. [...] No entanto, num contexto do big data, a captação de dados pessoais tem lugar para fins não especificados e em grande escala."

Em que pese ser o consentimento instituto relevante a garantir ao indivíduo o protagonismo do controle de seus dados pessoais, esta assertiva tem causado relevantes impasses ao avanço tecnológico[257], diante de práticas já presentes e difundidas, a justificar a lúcida constatação: “Fato é, contudo, que a própria emergência do consentimento como vetor central para a proteção dos dados pessoais carregou consigo seus complicadores”.[258]

Na sociedade da informação, onde já se afirmou que a privacidade morreu[259], não é raro se deparar com autores defendendo uma revisitação da tutela da privacidade[260], de forma que o consentimento não seria suficiente[261] a suprir integralmente os anseios desta nova realidade trazida pela tecnologia, especialmente com o *big data*.[262]

Em extenso relatório divulgado pela Comissão Europeia em janeiro de 2017, concluiu-se que o instituto do consentimento tem se tornado um pesado fardo a ser

---

257 "Por vezes, aliás, tem-se a sensação de que cresce a distância entre o velocíssimo mundo da inovação tecnológica e aquele lentíssimo do planejamento sócio-institucional." (RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.42).

258 BIONI, Bruno R. *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. p.147.

259 MORGAN, Jacob. Privacy Is Completely And Utterly Dead, And We Killed It. *Forbes*, Aug. 2014. Disponível em: <http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#46c9c18fdfbd>. Acesso em: 1.º dez. 2016.

260 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.173.

261 *“In this chapter I have been arguing that consent-based privacy models are inadequate in the face of contemporary information practices and the emerging corporate–state nexus that has created such a striking surveillance infrastructure on the internet.”* (AUSTIN, Lisa M. Enough About Me: Why Privacy is About Power, not Consent (or Harm). In: SARAT, Austin (Ed.). *A World without Privacy*: What Law Can and Should Do? Cambridge: Cambridge University Press, 2014. p.189). Tradução livre: "Neste capítulo tenho argumentado que os modelos de privacidade baseados no consentimento são inadequados em face das práticas contemporâneas de informação e do nexo emergente entre empresas e Estados que criou uma infra-estrutura de vigilância tão impressionante na internet."

262 *“In the context of Big Data, there is growing skepticism regarding the effectiveness of informed consent in the context of personal data processing [...]”*. (CUSTERS, Bart. Click here to consent forever: expiry dates for informed consent. *Big Data & Society*, 2016. p.2). Tradução livre: "No contexto da Big Data, cresce o ceticismo em relação à eficácia do consentimento informado no contexto do processamento de dados pessoais [...]."

carregado pelas empresas e não necessariamente é capaz de prover a proteção almeijada à privacidade dos cidadãos.[263]

Stefano Rodotà já teceu critícas ao consentimento, quando asseverou, por exemplo, que para se ter acesso a determinado bem ou serviço é necessário fornecer os seus dados pessoais[264], o que revela uma faceta imprópria da utilização do instituto, posto que, em razão da assimetria de poder entre o fornecedor do bem ou serviço e o aderente, não haverá escolha[265] ao aderente senão por "consentir". Em outras palavras:

---

263 *"Based on these issues relating to the scope, the consent mechanism and enforcement, competent authorities interviewed by Deloitte pointed out that this provision causes an unnecessarily high burden for businesses, while the usefulness for citizens is not optimal."* Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector. (EUROPEAN COMMISSION. *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*: Final Report - A study prepared for the European CommissionDG Communications Networks, Content & Technology. 2017. Disponível em: http://ec.europa.eu/newsroom/document.cfm?doc_id=41232>. Acesso em: 11 jan. 2017). Tradução livre: "Com base nessas questões relacionadas ao escopo, ao mecanismo de consentimento e ao cumprimento, as autoridades competentes entrevistadas pela Deloitte ressaltaram que esta disposição causa uma carga desnecessariamente alta para as empresas, enquanto a utilidade para os cidadãos não é o ideal."

264 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.76. Ver ainda: 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). Artigo 7.º Condições aplicáveis ao consentimento [...] 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

265 *"There is also the issue of the extent to which individuals have meaningful choices about what information they disclose. Typically, individuals cannot use a service unless they agree to the terms of use, which, in addition to being complex or legalistic, frequently present a "take it or leave it" approach. Under such an approach the user must agree to provide personal data for all of the purposes the organisation represents – even if some are not directly related to the service – in order to access the service. This substantially limits the ability of the individual to protect their personal data by giving meaningful consent. Generally, the emphasis on consent based on overly complex privacy policies that provide few real options and few limitations on collection and use diminish the effectiveness of privacy protections that are intended to support the individual's role in controlling his or her own personal data."* (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016). Tradução livre: "Há também a questão de até que ponto os indivíduos têm escolhas significativas sobre quais informações eles revelam. Normalmente, os indivíduos não podem usar um serviço a menos que concordem com os termos de uso, que, além de serem complexos ou legalistas, freqüentemente apresentam uma abordagem "ou tudo ou nada". De acordo com essa abordagem, o usuário deve concordar em fornecer dados pessoais para todos os fins que a organização representa – mesmo que alguns não estejam diretamente relacionados ao serviço – para acessar o serviço. Isto limita substancialmente a capacidade do indivíduo de proteger os seus dados pessoais dando um consentimento significativo. Geralmente, a ênfase no consentimento baseado em políticas de privacidade excessivamente complexas que oferecem poucas opções reais e poucas limitações na coleta e no uso diminuem a eficácia das proteções de privacidade que são destinadas a apoiar o papel do indivíduo no controle de seus próprios dados pessoais."

> Pode-se acrescentar, de modo mais geral, que o usuário de serviços informáticos e telemáticos se encontra em tal situação de disparidade de poder em relação aos fornecedores de tais serviços que, a rigor, não se pode falar em consentimento livremente manifestado para transações referentes à privacidade.[266]

Acrescenta Rodotà que, quando se coloca o consentimento exclusivamente nas mãos do titular, acaba-se por estabelecer uma lógica exclusivamente proprietária da privacidade, que deixa a cargo exclusivo do indivíduo a escolha e as consequências do fornecimento, tratamento e armazenamento de suas informações, pondo de lado os reflexos sociais de determinada atitude de circulação dos dados pessoais.[267]

Há que se mencionar ainda a possibilidade de se transferir toda a responsabilidade pelas consequências danosas do tratamento de dados para o indivíduo que teria consentido com aqueles riscos previstos nos termos do serviço.[268]

A dificuldade de conciliação do *modus operandi* das tecnologias inovadoras às regras existentes tem, inclusive, levado as empresas do Vale do Silício a praticarem *lobby*[269] junto ao Executivo e Legislativo americanos, com o intuito de passar leis

---

[266] RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.52-53.

[267] Ibid., p.76.

[268] "*Consent is related to the concept of informational self-determination. The autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data. However, as explored in the next chapter, this principle has limits, and there are cases where the data subject is not in a position to take a real decision. The data controller may want to use the data subject's consent as a means of transferring his liability to the individual."* (EUROPEAN COMMISSION. *Opinion 15/2011 on the definition of consent.* Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016.). Tradução livre: "O consentimento está relacionado com o conceito de auto-determinação informacional. A autonomia da pessoa em causa é simultaneamente uma condição prévia e uma consequência do consentimento: confere ao sujeito de dados a influência sobre o tratamento dos dados. Contudo, tal como analisado no capítulo seguinte, este princípio tem limites e há casos em que a pessoa em causa não está em posição de tomar uma decisão real. O responsável pelo tratamento dos dados pode querer utilizar o consentimento da pessoa em causa como meio de transferir a sua responsabilidade para o indivíduo."

[269] *"Across the country, well-funded armies of technology lobbyists are mobilizing as part of a coordinated national effort to water down common-sense privacy protections for kids and parents. As tech executives wage private battles to keep their own information private, they are employing hordes of lobbyists to work state legislatures across the country and in the halls of Congress to water down privacy rules for everyone else. Wherever they go, their rallying cry is the same: That simple protections to ensure the privacy of sensitive information will somehow stifle innovation."* (STEYER, James. High-Tech Hypocrisy. *Recode*, May 2015. Disponível em: <http://recode.net/2015/05/18/high-tech-hypocrisy/> Acesso em: 25 jun. 2015). Tradução livre: "Em todo o país,

que flexibilizem a proteção da privacidade e barrar projetos que de alguma forma possam tolher a inovação, garantindo assim menor interferência das autoridades na coleta, circulação e tratamento dos dados coletados dos usuários, componente essencial do funcionamento dos objetos dotados de sensores e conectados à internet no cenário do *big data*.

Em derteminadas situações, certamente, o consentimento livre, informado, expresso, em cláusula apartada e destacada, renovado quando em contratos de longa duração, com finalidades estritas e restritas, se mostra impróprio para tratar de toda e qualquer atividade que envolva o tratamento de dados pessoais, especialmente na sociedade da informação, mostrando-se um instituto, certas vezes, "*anêmico*".[270]

Aliás, a própria regulamentação europeia, que trata dos dados pessoais, reconhece que o consentimento, apesar de protagonista, não é o único fundamento a iluminar com licitude o tratamento dos dados pessoais, a saber:

> *Therefore, consent is recognised as an essential aspect of the fundamental right to the protection of personal data. At the same time, consent under the Charter is not the only legal ground enabling the processing of personal data; the Charter explicitly recognises that the law may lay down other legitimate grounds, as is the case with Directive 95/46/EC*.[271]

---

exércitos de lobistas tecnológicos bem remunerados estão se mobilizando como parte de um esforço nacional coordenado para diluir as proteções de privacidade de senso comum para crianças e pais. Como executivos da tecnologia realizam batalhas privadas para manter sua própria informação privada, eles estão empregando hordas de lobistas para trabalhar legislaturas estaduais em todo o país e nos salões do Congresso para diluir as regras de privacidade para todos os outros. Onde quer que eles vão, seu discurso é o mesmo: Que as proteções simples para garantir a privacidade de informações sensíveis de alguma forma sufocar a inovação."

[270] AUSTIN, Lisa M. Enough About Me: Why Privacy is About Power, not Consent (or Harm). In: SARAT, Austin (Ed.). *A World without Privacy*: What Law Can and Should Do? Cambridge: Cambridge University Press, 2014. p.131-189.

[271] EUROPEAN COMMISSION. *Opinion 15/2011 on the definition of consent.* Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016. Tradução livre: "Por conseguinte, o consentimento é reconhecido como um aspecto essencial do direito fundamental à proteção dos dados pessoais. Ao mesmo tempo, o consentimento ao abrigo da Carta não é o único fundamento jurídico que permite o tratamento de dados pessoais; A Carta reconhece explicitamente que a lei pode estabelecer outros fundamentos legítimos, como é o caso da Diretiva 95/46/CE."

O novo Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho, que revogou a Diretiva n.º 95/46/EC, traz a mesma ressalva[272], entendendo pela possibilidade de que outros institutos ou circunstâncias específicas[273] legitimem a coleta e análise de dados pessoais sem, necessariamente, existir consentimento do titular.

Note-se que o mencionado regulamento de 2016 não trata, em seu texto, diretamente do termo *big data*, no entanto, faz referência a práticas e situações as quais se pode inferir que esta modalidade de tratamento de dados está sendo abordada:

> (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. [...]

Percebe-se, neste turno, que o Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho, apesar de reforçar o consentimento com regra geral, traz casos específicos, como o acima destacado, onde outras questões em jogo justificariam a licitude do tratamento dos dados.[274]

---

272 "Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar."

273 *"Moreover, taking into account the sensors and smart devices in big data, other types of usable and practical user positive actions, which could constitute consent (e.g. gesture, spatial patterns, behavioral patterns, motions), need to be analyzed."* (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016). Tradução livre: "Além disso, tendo em conta os sensores e dispositivos inteligentes no big data, outros tipos de ações positivas do usuário usáveis e práticas, que poderiam constituir consentimento (por exemplo, gesto, padrões espaciais, padrões comportamentais, movimentos), precisam ser analisados."

274 "Nessa conjuntura, uma abordagem normativa mais flexível seria necessária, o que foi endereçado, mesmo que não voluntariamente para tais desafios mais contemporâneos, por algumas legislações ao redor do mundo através de exceções à regra do consentimento. Previsões legais para o tratamento adicional dos dados pessoais sem qualquer tipo de consentimento ulterior do titular, como do interesses legítimos na Diretiva da União Europeia, são um bom exemplo disso." (BIONI, Bruno. *XEQUE-MATE*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016. p.39).

Na esteira da novel regulamentação sobre dados pessoais na europa, a Comissão Europeia elaborou, em janeiro de 2017, proposta de revogação da Diretiva n.º 2002/58 que versa exclusivamente sobre comunicações eletrônicas, onde, em seu turno, reconhece que as regras atualmente existentes não acompanharam[275] as inovações tecnológicas dos últimos anos, colocando o consentimento como um dos exemplos[276] neste sentido, propondo novas formas de tutela da privacidade e controle dos dados pessoais.

Este novo esboço de regulamentação na Europa, que trata exclusivamente sobre comunicações eletrônicas, em que pese ampliar a tutela dos dados pessoais, flexibiliza[277] a regra geral do consentimento em casos específicos, como, por exemplo, quando o usuário de um navegador de internet define as sua regras básicas de privacidade para utilização de cookies, entendendo que tal configuração definiria as suas preferências gerais de navegação na rede, sendo então desnecessário que,

---

275 *"Accordingly, the Directive has not kept pace with technological developments, resulting in a void of protection of communications conveyed through new services."* (EUROPEAN COMMISSION. *Proposal for a Regulation of the European Parliament and of the Council*. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017). Tradução livre: "Consequentemente, a diretiva não acompanhou o ritmo da evolução tecnológica, resultando num vazio de proteção das comunicações transmitidas através de novos serviços."

276 "*The evaluation further showed that some provisions have created an unnecessary burden on businesses and consumers. For example, the consent rule to protect the confidentiality of terminal equipment failed to reach its objectives as end-users face requests to accept tracking cookies without understanding their meaning and, in some cases, are even exposed to cookies being set without their consent."* (EUROPEAN COMMISSION. *Proposal for a Regulation of the European Parliament and of the Council*. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017). Tradução livre: "A avaliação mostrou ainda que algumas disposições criaram um encargo desnecessário para as empresas e os consumidores. Por exemplo, a regra de consentimento para proteger a confidencialidade dos equipamentos não conseguiu atingir seus objetivos como usuários finais enfrentam pedidos de aceitar cookies de rastreamento sem entender o seu significado e, em alguns casos, são expostos a cookies que são definidos sem o seu consentimento."

277 "A 'disposição sobre cookies', que obriga os utilizadores da Internet a responder incessantemente a pedidos de consentimento, será racionalizada. As novas regras permitirão aos utilizadores controlar melhor os seus parâmetros, proporcionando uma maneira fácil de aceitar ou recusar os cookies e outros identificadores de rastreio das suas atividades em caso de risco para a privacidade. A proposta esclarece que não é necessário consentimento relativamente a cookies não invasivos da privacidade utilizados para melhorar as pesquisas na Internet (memorização do histórico de compras, por exemplo). A introdução de cookies por um determinado sítio para contagem do número de visitantes do sítio deixará de necessitar de consentimento." (COMISSÃO EUROPEIA. Comunicado de imprensa. Comissão propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrónicas e atualiza as regras de proteção de dados para as instituições da EU. Bruxelas, 10 de janeiro de 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017).

em todos os sítios visitados, houvesse uma nova e incômoda mensagem requerendo o consentimento do usuário[278], como ocorre atualmente.

Importante ressaltar ainda uma tímida passagem constante do Anteprojeto de Lei de Proteção de Dados Pessoais, que em seu artigo 9.º, § 7.º assevera que "O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos." Ou seja, *"consent is not the only ground for lawfulness"*.[279]

Há que se considerar a especificidade do contexto no qual o *big data* se insere, não se revelando, à primeira vista, razoável que o pano de fundo regulatório a legitimar o tratamento de dados pessoais seja inteiramente homogêneo, horizontal, fulcrado quase que integralmente na regra do consentimento[280], sem que haja

---

278 *"Article 9 Consent. 1.The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply. 2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet. 3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues."* (EUROPEAN COMMISSION. *Proposal for a Regulation of the European Parliament and of the Council*. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017). Tradução livre: "Artigo 9.º Consentimento. 1. É aplicável a definição e as condições de consentimento previstas no artigo 4.º, n.º 11, e no artigo 7.º do Regulamento (UE) n.º 2016/679/UE. 2. Sem prejuízo do disposto no n.º 1, sempre que tal seja tecnicamente possível e exequível, para efeitos do n.º 1, alínea b), do artigo 8.º, o consentimento pode ser expresso utilizando as definições técnicas adequadas de um programa informático que permita o acesso à Internet. 3. Os utilizadores finais que tenham dado o seu consentimento para o tratamento de dados de comunicações eletrónicas nos termos da alínea c) do n.º 2 do artigo 6.º e das alíneas a) e b) do n.º 3 do artigo 6.º devem ter a possibilidade de: Retirar o seu consentimento em qualquer momento, nos termos do n.º 3 do artigo 7.º do Regulamento (UE) n.º 2016/679, devendo ser lembrada dessa possibilidade em intervalos periódicos de 6 meses, desde que o processamento continue."

279 EUROPEAN COMMISSION. *Opinion 15/2011 on the definition of consent.* Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016. Tradução livre: "Consentimento não é o único fundamento para a licitude."

280 *"Given this, common approaches to notification and consent may not be providing the privacy protection originally intended. As data usage has become more complex, so too have the privacy policies that describe them. Many organisations tend to rely on these as a basis for consent, but given the implications about how individuals make decisions, questions can be asked about whether this focus on privacy notices and consent can continue to bear the weight they are often assigned in the process of affording protection. Do they allocate too much risk to the consenting individual, who rarely reads the information or understands it if they do? Alternatively, we may also need to consider whether an overly rigid interpretation of the concept of consent, in other words, one which assumes that explicit and specific consent is required for each and every transfer of information necessary to fulfil the original purpose of the transaction, runs the risk of being used to weaken the control which many privacy laws specifically aim to give individuals."* (ORGANISATION FOR

previsão de estados de fato específicos e que podem fugir à regra geral, como é nitidamente o caso do *big data*[281], onde os resultados úteis da análise dos dados surge, muitas vezes, distante da finalidade inicial para as quais foram coletados.[282] Nas palavras de Rodotà:

> Foi o próprio tratamento automático de dados a demonstrar, à evidência, que nenhuma informação tem valor por si mesma, mas em virtude do contexto no qual está inserida, ou pelas finalidades para as quais é utilizada, ou pelas informações às quais tem sido associada. As regras sobre a circulação dos dados então tendem a ser cada vez mais orientadas para a consideração de contextos, funções, associações.[283]

ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016). Tradução livre: "Dado isto, abordagens comuns de notificação e consentimento podem não estar fornecendo a proteção de privacidade originalmente pretendida. Como o uso de dados tornou-se mais complexo, também se tornaram as políticas de privacidade que as descrevem. Muitas organizações tendem a confiar nisso como base para o consentimento, mas tendo em conta as implicações sobre a forma como as pessoas tomam decisões, pode-se perguntar se este foco em avisos de privacidade e consentimento pode continuar a suportar o peso que muitas vezes são atribuídos no processo de proteção. Alternativamente, talvez também precisemos considerar se uma interpretação muito rígida do conceito de consentimento, ou seja, uma que supõe que o consentimento explícito e específico é necessário para cada um e dada transferência de informações necessárias para cumprir o propósito original da transação, corre o risco de ser usado para enfraquecer o controle que muitas leis de privacidade especificamente visam dar aos indivíduos."

281 *"The opaquenes of data processing in AmI due of the ability of the sistem to capture and process data in an automated and hidden fashions one of the reasons for its sucess. What happens if this anawareness extends also to the same kind of unrevealed and unfair practices that are today used on the Internet (such as behavional targeting, stereotyping)? Can a legal requirement such as the consent be deemed appropriate and usefull in such kind of situations? Therefore, it seems that recognizing the concerns deriving from the use of AmI mechanisms in different contexts could enable us to find different and differentiated data protections rules."* (MONTELEONE, Shara. Ambient Intelligence: Legal Challenges and Possible Directions for Privacy Protection. In: AKRIVOPOULOU, Christina. *Personal data privacy and protection in a surveillance era*: technologies and practices. Hershey, PA: Information Science Reference, 2011. p.212-213). Tradução livre: "A opacidade do processamento de dados em AmI devido à capacidade do sistema para capturar e processar dados de forma automatizada e oculta uma das razões de seu sucesso. O que acontecerá se a falta de ciência se estender também ao mesmo tipo de práticas não reveladas e injustas que são hoje usadas na Internet (como a segmentação comportamental, os estereótipos)? Um requisito legal como o consentimento pode ser considerado apropriado e útil em tais situações? Portanto, parece que reconhecer as preocupações derivadas do uso de mecanismos AmI em diferentes contextos poderia permitir-nos encontrar regras diferentes e diferenciadas de proteção de dados."

282 *"In the era of big data, however, when much of data's value is in secondary uses that may have been unimagined when the data was collected, such a mechanism to ensure privacy is no longer suitable."* (MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.173). Tradução livre: "Na era do big data, entretanto, quando grande parte do valor dos dados está em usos secundários que podem ter sido inimaginados quando os dados foram coletados, tal mecanismo para garantir a privacidade não é mais adequado."

283 RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.77.

Esse contexto revela uma clara hipótese onde os institutos jurídicos clássicos se mostram obsoletos diante da evolução informática e do contexto social do século XXI, devendo ser revisitados e reconstruídos à luz dos valores cardeais do sistema, promovendo a livre iniciativa, o progresso social e tecnológico, sem esvaziar a proteção da dignidade humana, conforme lição de Gustavo Tepedino:

> As categorias do direito privado devem ser reconstruídas, a partir do surgimento de situações jurídicas inteiramente novas, advindas com a revolução tecnológica dos últimos cinquenta anos. Basta pensar na engenharia genética, na procriação in vitro, na extraordinária massa de informações pessoais colhidas mediante exame de DNA e na circulação de dados propiciados pelas redes de informática. Cabe à doutrina do direito civil estabelecer parâmetros para tutelar a pessoa humana diante dos novos bens jurídicos que se tornam objeto de situações existenciais suscitadas pelo avanço da cibernética e da tecnologia.[284]

Com base neste cenário, constanta-se vozes ganhando força na tentativa de revisitar o instituto do consentimento, especialmente quando se tratar de *big data*, de forma a flexibilizá-lo em determinadas situações, garantindo licitude ao tratamento com base em outras hipóteses igualmente legítimas.

Destas novas formas propostas para licitude, como acima demonstrado, temos ainda como exemplos a maior ênfase à transparência e responsabilização[285] efetiva dos agentes por eventual ilicitude e/ou abusividade na coleta, armazenagem e tratamento dos dados[286], quando diante do *big data*, que são os temas do próximo item.

---

284 TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.15.

285 *"Accountability implies an obligation to report and justify algorithmic decision-making, and to mitigate any negative social impacts or potential harms. We'll consider accountability through the lens of five core principles: responsibility, explainability, accuracy, auditability, and fairness."* (DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How to Hold Algorithms Accountable. *MIT Technology Review*, Nov. 2016. Disponível em: <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/>. Acesso em: 26 nov. 2016). Tradução livre: "A responsabilização implica a obrigação de relatar e justificar a tomada de decisões algorítmicas e de mitigar os impactos sociais negativos ou os danos potenciais. Nós vamos considerar a responsabilidade através da lente de cinco princípios fundamentais: responsabilidade, explicabilidade, precisão, auditabilidade e justiça."

286 *"we envision a very diferent privacy framework for the big-data age, one focused less on individual consente at the time of collection and more on holding data users accountable for hat they do."* (MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.173). Tradução livre: "Imaginamos uma estrutura de privacidade muito diferente para a era do big data, uma focada menos no consentimento individual no momento da coleta e mais em responsabilizar os usuários de dados pelo que fazem."

2.3.2 Responsabilidade e transparência

Viktor Mayer-Schönberger advoga de maneira contundente a necessidade de mudança no sistema de responsabilidade em caso de tratamento ilícito ou abusivo de dados pessoas no *big data*[287], de forma a enfatizar menos o consentimento e propondo a valorização de um sistema que imponha severa[288] responsabilização dos agentes que tratam dados, quando estes agirem de maneira contrária aos regramentos especificamente criados neste sentido.

Estudo publicado em 2016 demonstrou que o estabelecimento de penalidades e multas elevadas para casos de violação de dados pessoais surtiu efeitos positivos no Reino Unido.[289]

Durante encontro internacional realizado em Paris no ano 2010, autoridades, acadêmicos e membros da sociedade civil ligados à proteção de dados[290], debateram e ressaltaram, em documento publicado ao final do evento, a importância de práticas

---

287 MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013. p.171-184.

288 *"Data-user accountability only works when it has teeth."* (Ibid., p.173). Tradução livre: "A responsabilidade do usuário de dados só funciona quando tem dentes."

289 *"This notwithstanding, our analysis does suggest that fines play a valuable role in enhancing the business case for privacy compliance and raising awareness of data protection law, both amongst data subjects and within controller organisations."* (GRANT, Hazel; CROWTHER, Hannah. How Effective Are Fines in Enforcing Privacy? In: WRIGHT, David; DE HERT, Paul. *Enforcing Privacy*: Regulatory, Legal and Technological Approaches. Springer International Publishing, 2016. p.304). Tradução livre: "Não obstante, nossa análise sugere que as multas têm um papel valioso no aprimoramento dos argumentos comerciais para o cumprimento da privacidade e no aumento da conscientização da lei de proteção de dados, tanto entre os indivíduos quanto entre as organizações de controladores."

290 *"This paper has benefited from the insights and perspectives of all sectors – industry, civil society, academia, and government. The Centre is particularly encouraged by the participation of data protection commissioners and privacy regulators from Canada, France, Germany, Hungary, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain, the United Kingdom and the United States, as well as the European Data Protection Supervisor."* (HUNTON & WILLIAMS LLP. The Centre for Information Policy Leadership. *Demonstrating and Measuring Accountability*: A Discussion Document, Accountability Phase II – The Paris Project, October 2010. Disponível em: <https://iapp.org/media/pdf/knowledge_center/Accountability_Phase_II.pdf>. Acesso em: 1.º dez. 2016). Tradução livre: "Este artigo se beneficiou das idéias e perspectivas de todos os setores – indústria, sociedade civil, academia e governo. O Centro é particularmente encorajado pela participação de comissários de proteção de dados e reguladores de privacidade do Canadá, da França, da Alemanha, da Hungria, da Irlanda e dos Estados Unidos da América, Israel, Itália, Países Baixos, Nova Zelândia, Espanha, Reino Unido e Estados Unidos, bem como a Autoridade Europeia para a Protecção de Dados."

específicas para o setor, concernentes à responsabilização e transparência, como se vê da conclusão abaixo:

> *For purposes of this project, accountability can be described as a demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection for data*.[291]

Ou seja, considerando os elevados riscos[292] envolvidos no tratamento ilícito de dados, é imperiosa a fixação clara de deveres e responsabilidades daqueles responsáveis, com normas específicas para tais práticas cujo potencial danoso é evidente.[293]

Note-se que o Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho, cujas regras serão obrigatórias para todos os Estados-Membros da União Europeia a

---

[291] HUNTON & WILLIAMS LLP. The Centre for Information Policy Leadership. *Demonstrating and Measuring Accountability*: A Discussion Document, Accountability Phase II – The Paris Project, October 2010. Disponível em: <https://iapp.org/media/pdf/knowledge_center/Accountability_Phase_II.pdf>. Acesso em: 1.º dez. 2016. Tradução livre: "Para fins deste projeto, a responsabilização pode ser descrita como um reconhecimento demonstrável e assumição de responsabilidade de ter políticas e procedimentos adequados e promoção de boas práticas que incluem correção e remediação de falhas e má conduta. É um conceito que tem governança e dimensões éticas. Prevê uma infra-estrutura que promova a tomada de decisões responsáveis, gera responsabilidade, aumenta a transparência e considera a responsabilidade. Ele engloba as expectativas de que as organizações relatam, explicam e respondem pelas conseqüências das decisões sobre a proteção dos dados. A prestação de contas promove a implementação de mecanismos práticos através dos quais os requisitos legais e as orientações são traduzidos em proteção efetiva para os dados."

[292] Ver Capítulo 1, Item 1.3. "O outro lado da moeda: os riscos do big data."

[293] *"Given the literally life-altering nature of these algorithmic decisions, they should receive careful attention and be held accountable for negative consequences."* (DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How to Hold Algorithms Accountable. *MIT Technology Review*, Nov. 2016. Disponível em: <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/>. Acesso em: 26 nov. 2016). Tradução livre: "Dada a natureza, que literalmente altera a vida, dessas decisões algorítmicas, elas devem receber atenção cuidadosa e ser responsabilizadas por conseqüências negativas."

contar de 2018[294], estabeleceu o chamado “direito à explicação”[295], quando a pessoa se vê diante de decisões automatizadas com base em um algorítimo que analisa dados e extrai resultados, justamente a forma com a qual o *big data* opera.

Segundo análise doutrinária de acadêmicos da Universidade de Oxford, diante do aludido regulamento[296], Bryce Goodman e Seth Flaxman entendem que nascerá um direito à explicação garantido aos indivíduos abrangidos pela incidência da regra, oponível aos agentes que tratam os dados de maneira automatizada, em que pese não haver qualquer forma clara de como esse direito será exercido.[297]

Tal direito se liga diretamente ao anseio pela transparência[298], diante da verdadeira caixa preta[299] que se tornaram os algorítimos automatizados que norteiam

---

294 *“The GDPR, on the other hand, requires no enabling legislation to take effect. It does not direct the law of EU member states, it simply is the law for member states (or will be, when it takes effect).”* (GOODMAN, Bryce; FLAXMAN, Seth. *European Union regulations on algorithmic decision-making and a “right to explanation”*. Disponível em: <https://arxiv.org/pdf/1606.08813v3.pdf>. Acesso em: 30 nov. 2016). Tradução livre: "O GDPR, por outro lado, não requer nenhuma legislação habilitante para entrar em vigor. Não direciona a lei dos Estados membros da UE, é simplesmente a lei para os Estados membros (ou será, quando ela entrar em vigor)."

295 “*Citizens of EU member states might soon have a way to demand explanations of the decisions algorithms about them.”* (CHIEL, Ethan. EU citizens might get a ‘right to explanation’ about the decisions algorithms make. *Fusion*, July 2016. Disponível em: <http://fusion.net/story/321178/european-union-right-to-algorithmic-explanation/>. Acesso em: 30 nov. 2016). Tradução livre: "Os cidadãos dos Estados-Membros da UE poderão em breve ter uma maneira de exigir explicações dos algoritmos acerca das decisões sobre eles."

296 “Artigo 13.º Informações a facultar quando os dados pessoais são recolhidos junto do titular. 1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações: [...] f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.”

297 *“[...] Articles 13 and 14 state that, when profiling takes place, a data subject has the right to “meaningful information about the logic involved.” This requirement prompts the question: what does it mean, and what is required, to explain an algorithm’s decision?”* (GOODMAN, Bryce; FLAXMAN, Seth. *European Union regulations on algorithmic decision-making and a “right to explanation”*. Disponível em: <https://arxiv.org/pdf/1606.08813v3.pdf>. Acesso em: 30 nov. 2016). Tradução livre: "[...] Os artigos 13.º e 14.º afirmam que, quando se procede à elaboração de um perfil, a pessoa em causa tem o direito a "informações significativas sobre a lógica envolvida". Esta exigência suscita a pergunta: o que significa e o que é necessário, para explicar a decisão de um algoritmo?”

298 *“The use of algorithmic decisions in an increasingly wider range of applications has led some to caution against the rise of a “black box” society and demand increased transparency in algorithmic decision-making.”* (GOODMAN, Bryce; FLAXMAN, Seth. *European Union regulations on algorithmic decision-making and a “right to explanation”*. Disponível em: <https://arxiv.org/pdf/1606.08813v3.pdf>. Acesso em: 30 nov. 2016). Tradução livre: "O uso de decisões algorítmicas em uma gama cada vez mais ampla de aplicações levou alguns a cautela contra o surgimento de uma sociedade da "caixa preta" e exigem maior transparência na tomada de decisão algorítmica."

a atuação das grandes empresas de tecnologia e governos, notadamente pela enorme quantidade de dados pessoais, muitas vezes sensíveis, objeto de análise.

Sem qualquer pretensão de resolver o problema, é possível, no entanto, mencionar que os exemplos ora destacados demonstram a possibilidade de criação de regras específicas[300], para determinados casos – como o *big data* – que se aplicam tão somente quando verificado o fato previsto na norma, sem que se utilize uma regulamentação genérica e estrutural, insensível aos pormenores tão corriqueiros da complexa e múltipla sociedade da informação.

2.3.3 Um exemplo de mudança do paradigma

O Marco Civil da Internet conseguiu promover uma verdadeira mudança de paradigma no Direito Brasileiro, especificamente em matéria de responsabilidade civil, quando tratou de uma questão pontual, como a responsabilidade civil do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, prevendo regras claras e moldadas especificamente para a situação, diante de suas peculiaridades.

Neste turno, opções específicas se mostraram possíveis, especialmente em território pátrio, com a recente mudança no paradigma da responsabilização para casos específicos na internet, valendo mencionar os artigos 19 e 21 do Marco Civil da Internet.[301] Em análise do tema, Anderson Schreiber assevera que: “[...] de modo

---

299 PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.46-48.

300 *“In order to answer to the need of safeguards arising from the emergence of AmI, one approach could be to adopt a system of ‘micro-policies’ instead of domain policies that could better fit with the specific circumstances.”* (MONTELEONE, Shara. Ambient Intelligence: Legal Challenges and Possible Directions for Privacy Protection. In: AKRIVOPOULOU, Christina. *Personal data privacy and protection in a surveillance era*: technologies and practices. Hershey, PA: Information Science Reference, 2011. p.214). Tradução livre: "A fim de responder à necessidade de salvaguardas decorrentes do surgimento do AmI, uma abordagem poderia ser a de adotar um sistema de ‘micro-políticas’ em vez de políticas de domínio que poderia melhor se ajustar às circunstâncias específicas.”

301 “Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para,

geral, nossas cortes vinham entendendo que as sociedades empresarias que criam e exploram de algum modo redes sociais devem ser consideradas responsáveis pelos danos causados às vítimas de conteúdo lesivo".[302]

Em que pese esta constatação, a verdade é que o assunto vinha sendo decidido de maneira quase casuística[303] pelos magistrados brasileiros, diante da ausência de norma específica, o que levou, inclusive, a matéria a alcançar repercução geral no Supremo Tribunal Federal.[304]

---

no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. [...]
Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário. [...]
Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo".

302 SCHREIBER, Anderson. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.285.

303 "Defendia-se desde uma total isenção de responsabilidade até a responsabilidade objetiva do provedor independentemente de sua notificação prévia. Correntes intermediárias apontavam ora para uma responsabilidade objetiva do provedor (com base no Código de Defesa do Consumidor ou no Código Civil) se, após notificado extrajudicialmente, ele não retirasse o conteúdo lesivo, ora para uma responsabilidade subjetiva, caso ele se mantivesse inerte após a sua notificação extrajudicial, sendo esta última corrente adotada majoritariamente pelo STJ. Por fim, parte da doutrina defendia como regra a responsabilidade subjetiva do provedor se, após a ordem judicial impondo a retirada do conteúdo lesivo, este restasse omisso e não tornasse indisponível o material, entendimento que acabou sendo adotado no MCI." (TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o marco civil da internet. *Revista Fórum de Direito Civil – RFDC*, Belo Horizonte, v.4, n.10, set./dez. 2015. Disponível em: <http://www.bidforum.com.br/bid/PDI0006.aspx?pdiCntd=238166>. Acesso em: 17 dez. 2015).

304 BRASIL. Superior Tribunal de Justiça. *ARE 660861* - RECURSO EXTRAORDINÁRIO COM AGRAVO-MG. Relator: Min. Luiz Fux. Ainda pendente de julgamento, conforme acompanhamento processual. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4155926>. Acesso em: 27 dez. 2106.

O Marco Civil da internet alterou, de maneira clara, a orientação majoritária vigente à época de sua edição, inclusive presente no Superior Tribunal de Justiça[305], onde a Corte entendia ser suficiente a mera notificação extrajudicial do provedor de aplicações para que, diante de sua posterior omissão, fosse responsabilizado civilmente pelo conteúdo indevido gerado por terceiro.

Tratava-se, como se afirmou, de uma responsabilidade *"condicionada"*[306], ou responsabilidade civil *ex post*[307], que surgiria a contar do momento em que a empresa gestora ou propietária do espaço virtual – provedor de aplicações de internet – quedava-se inerte após ser comunicada pela pessoa que se dizia vítima de um dano perpetrado por terceiro.[308] Trata-se da figura conhecida como *notice and take down*[309], cuja inspiração vem dos Estados Unidos, através do *Digital Millennium Copyriright Act*.

Ocorre que, de acordo com os artigos acima destacados no Marco Civil da Internet, estabeleceu-se que caberia, exclusivamente, ao Poder Judiciário a ordem pela remoção ou não do conteúdo alegadamente ilítico, alterando substancialmente a orientação jurisprudencial desde então, conforme se lê de recente decisão emanada pelo STJ:

> Contudo, não se pode impor ao provedor de internet que monitore o conteúdo produzido pelos usuários da rede de modo a impedir a divulgação de futuras manifestações ofensivas contra determinado indivíduo. Não se pode exigir dos provedores que determinem o que é ou não apropriado para divulgação pública. Cabe ao Poder Judiciário, quando instigado, aferir se determinada manifestação deve ou não ser extirpada da rede mundial de computadores e, se for o caso, fixar a reparação civil cabível contra o real responsável pelo

---

305 "Haverá responsabilidade subjetiva do provedor de busca, quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide." (BRASIL. Superior Tribunal de Justiça. *REsp 1.193.764/SP*. Relator: Min. Nancy Andrighi. Órgão Julgador: Terceira Turma. Publicação: DJe 8/8/2011).

306 SCHREIBER, Anderson. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.286.

307 Ibid., p.287.

308 "[...] considero razoável que, uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, o provedor retire o material do ar no prazo de 24 (vinte e quatro) horas, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada." (BRASIL. Superior Tribunal de Justiça. *REsp 1.323.754*. Relator: Min. Nancy Andrigui. Julgamento: 19/06/2012. Órgão Julgador: Terceira Turma. Publicação: DJe 28/08/2012).

309 SCHREIBER, op. cit., p.286.

> ato ilícito. Ao provedor não compete avaliar eventuais ofensas, em virtude da inescapável subjetividade envolvida na análise de cada caso. Somente o descumprimento de uma ordem judicial, determinando a retirada específica do material ofensivo, pode ensejar a reparação civil. Para emitir ordem do gênero, o Judiciário avalia a ilicitude e a repercussão na vida do ofendido no caso concreto. Ademais, observa-se que o Marco Civil da Internet (Lei n.º 12.965/2014) disciplinou, em seu artigo 19, o tema no sentido acima exposto. [...][310]

Na lição de Carlos Affonso Pereira de Souza, dentre os vários fundamentos que levaram até esta regulamentação específica contida no Marco Civil da Internet, destacou-se que a retirada de conteúdos do ar, de forma subjetiva e mediante mera notificação, poderia prejudicar a inovação no âmbito da internet, implicando em sério entrave para o desenvolvimento de novas alternativas de exploração e comunicação na rede, as quais poderiam não ser desenvolvidas em razão do receio de futuras ações indenizatórias, bem como tal medida colocaria nas mãos do Poder Judiciário a apreciação do conteúdo, garantiria maior segurança jurídica e previsibilidade para os negócios desenvolvidos na internet.[311]

Deve ser salientado ainda que, apesar da existência da norma, nada impede que o provedor de aplicações de internet crie mecanismos internos, através de seus respectivos termos de uso, de forma a permitir reclamações e denúncias, com a posterior remoção do conteúdo sem qualquer necessidade de intervenção do Poder Judiciário.[312]

---

[310] BRASIL. Superior Tribunal de Justiça. *AgREsp 917.162-SP*. Relator: Min. Ricardo Villas Bôas Cueva. Disponível em: <http://www.jusbrasil.com.br/diarios/documentos/386875692/andamento-do-processo-n-2016-0122040-3-agravo-recurso-especial-21-09-2016-do-stj>. Acesso em: 1.º dez. 2016.

[311] SOUZA, Carlos Affonso Pereira de. Responsabilidade civil dos provedores de acesso e de aplicações de Internet: evolução jurisprudencial e os impactos da Lei 12.695/2014 (Marco Civil da Internet). In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.803-804.

[312] TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o marco civil da internet. *Revista Fórum de Direito Civil – RFDC*, Belo Horizonte, v.4, n.10, set./dez. 2015. Disponível em: <http://www.bidforum.com.br/bid/PDI0006.aspx?pdiCntd=238166>. Acesso em: 17 dez. 2015.

Apesar da existência de críticas[313] ao disposto no Artigo 19 do Marco Civil da Internet, este singelo exemplo demonstra cabalmente ser possível o estabelecimento de novas regras[314], eventualmente até contrárias ao atual posicionamento doutrinário, legislativo e jurisprudencial, tendo em vista uma atividade que contenha especificidades e resultados particulares, criando-se um sistema que, diante de uma ponderação dos interesses em jogo, viabilize a inovação tecnológica e a atividade econômica, garanta a privacidade e a liberdade de expressão, porém ao mesmo observe os valores nortedores do sistema jurídico, qual seja, a dignidade da pessoa humana.[315]

---

313 "Os direitos fundamentais da pessoa humana (honra, privacidade, imagem, entre outros) também são tutelados pela Constituição brasileira, em patamar axiológico não inferior à liberdade de expressão, de modo que recorder apenas "um lado da moeda" já no art. 19 representa má técnica legislativa e uma preocupante advertência sobre o que está por vir." (SCHREIBER, Anderson. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.290).

314 TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o marco civil da internet. *Revista Fórum de Direito Civil – RFDC*, Belo Horizonte, v.4, n.10, set./dez. 2015. Disponível em: <http://www.bidforum.com.br/bid/PDI0006.aspx?pdiCntd=238166>. Acesso em: 17 dez. 2015.

315 "O Marco Civil estabeleceu, como regra, que o provedor de aplicações de internet deverá retirar o conteúdo danoso, após ordem judicial específica, sob pena de responder subjetivamente pela omissão. Todavia, caso se trate de conteúdo que viole frontalmente a privacidade de uma pessoa – imagens, vídeos ou outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado – este provedor terá o dever de retirar o material após a notificação extrajudicial da vítima ou de seu representante legal." (TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o marco civil da internet. *Revista Fórum de Direito Civil – RFDC*, Belo Horizonte, v.4, n.10, set./dez. 2015. Disponível em: <http://www.bidforum.com.br/bid/PDI0006.aspx?pdiCntd=238166>. Acesso em: 17 dez. 2015).

3 A REGULAÇÃO DO *BIG DATA* NO BRASIL

Há, no sistema jurídico brasileiro, normas que podem incidir sobre a atividade preponderante no *big data*, qual seja, análise de grande quantidade de dados, para se extrair resultados.

Sem qualquer pretensão de esgotamento do tema, neste capítulo serão abordados alguns dos dispositivos legais brasileiros que tratam sobre proteção de dados pessoais à luz do *big data*, destacando também exemplos que os desafiam.

3.1 O cenário legislativo nacional sobre proteção de dados

Considerando o conceito jurídico amplo de privacidade que, conforme mencionado no Capítulo 2, alberga a proteção de dados pessoais, pode-se verificar que a Constituição Brasileira de 1988, em seu artigo 5.º, reconhece como inviolável a intimidade e a vida privada, mencionando ainda o direito à indenização pelos danos decorrentes de sua violação.[316]. Destaca-se ainda previsão genérica de inviolabilidade de dados[317] e o instrumento do Habeas Data[318].

---

316 "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

317 "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; "

318 "LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

O Código de Proteção e Defesa do Consumidor, de 1990, regula a privacidade[319] e controle de dados pessoais do interessado de maneira bastante tímida, embora pioneira[320] em nosso ordenamento, pois, dentre outros, conferiu ao consumidor direito de acesso livre aos seus dados pessoais.[321]

A Lei Complementar n.º 105 de 2001 instituiu o sigilo das operações de instituições financeiras[322], diante do caráter sensível de tais dados que se encontram em poder de bancos e demais instituições públicas e privadas abrangidas pela norma.

No Código Civil de 2002, foi dedicado tão somente um único artigo[323] ao tema da privacidade, sem qualquer inovação, praticamente repetindo o que já havia se afirmado pelo constituinte de 1988 e ainda incidindo em verdadeira indiferença ao novel significado da privacidade nos tempos modernos.[324]

---

319 "Dessa forma, não é possível, no Direito brasileiro, que informações pessoais sejam coletadas sem o consentimento do consumidor." (LEMOS, Ronaldo; DONEDA, Danilo; SOUZA, Carlos Affonso Pereira de; ROSSINI, Carolina Almeida A. *Estudo sobre a regulamentação jurídica do spam no Brasil*. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS),da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas. p.15. Disponível em: <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 18 jul. 2015.

320 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p.18.

321 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1.º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2.º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3.º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4.º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5.º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

322 "Art. 1.º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados."

323 "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

324 SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011. p.128. Sobre a crítica ao legislador do Código Civil de 2002, o autor prossegue afirmando ainda que "não é exagero dizer que o Código Civil ignorou a vasta amplitude do tema, cuja compreensão é essencial para perceber o importante papel reservado à tutela da privacidade no século XXI."

Em 2011 foi promulgada a Lei n.º 12.414 que tratou de disciplinar o cadastro positivo[325] e certos aspectos sobre proteção de dados pessoais no ambiente de crédito[326], que inclusive acabou por constar como referência da Súmula n.º 550 do Superior Tribubal de Justiça[327]. Destaca-se ainda a Lei n.º 12.527/2011, chamada Lei de acesso a informação, que em seus artigos 4.º, inciso IV[328] e 31[329] tratam sobre o tratamento de dados pessoais.

Os diplomas legais acima garantem tutela da privacidade, através do controle de dados pessoais pelo titular, constituindo evidente ato ilícito a sua violação. Passa-se

---

325 Segundo leciona Leonardo Bessa: "Os bancos de dados de proteção ao crédito são entidades que têm por principal objeto a coleta, o armazenamento e transferência a terceiros (credor potencial) de informações dos pretendentes (consumidores) à obtenção de crédito." (BESSA, Leonardo Roscoe. *Responsabilidade civil dos bancos de dados de proteção ao crédito*: diálogo entre o Código de Defesa do Consumidor e a Lei do Cadastro Positivo. Disponível em: <http://www.mpcon.org.br/Revista_mpcon/n01/artigos/ARTIGO_2014-RESPONSABILIDADE_CIVIL_DOS_BANCOS_DOS_DADOS_DE_PROTECAO_AO_CREDITO-DIALOGO_ENTRE_O_CDC_E_A_LEI_DO_CADASTRO_POSITIVO-LEONARDO_ROSCOE_BESSA.pdf>. Acesso em: 10 nov. 2015).

326 "Art. 1.º Esta Lei disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, sem prejuízo do disposto na Lei n.º 8.078, de 11 de setembro de 1990 - Código de Proteção e Defesa do Consumidor."

327 "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo." (Súmula 550, SEGUNDA SEÇÃO, julgado em 14/10/2015, DJe 19/10/2015).

328 "Art. 4.º Para os efeitos desta Lei, considera-se: [...] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;"

329 "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1.º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2.º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3.º O consentimento referido no inciso II do § 1.º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4.º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5.º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal."

à análise do Marco Civil da Internet e a sua regulamentação, cuja tutela dos dados pessoais se dá de maneira ainda mais enfática.

3.1.1 O Marco Civil da Internet e sua regulamentação

Sem dúvida as revelações de espionagem de chefes de Estado e empresas brasileiras lançaram o país no cenário mundial, gerando uma resolução[330] da Assembleia Geral da ONU, na qual, por votação unânime, declarou a privacidade na internet como um direito humando fundamental, culminando[331] ainda na promulgação da Lei n.º 12.965/2014, legislação pioneira[332] em todo o mundo e que tem servido de base e inspiração[333] para outros sistemas jurídicos.

Apesar da Lei datar de 2014, Ronaldo Lemos, um dos idealizadores do projeto ao lado de Carlos Affonso Pereira de Souza e Sérgio Branco, revela[334] que a ideia da criação do Marco Civil teve seus primeiros contornos em 2007, em resposta ao Projeto de Lei n.º 84/1999 de autoria do Senador Eduardo Azeredo.

Acrescenta Lemos que o mencionado projeto estabeleceria um verdadeiro marco criminal da rede, pois previa inúmeros fatos típicos e ainda equiparava os

---

330 GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.250.

331 "Quando o escândalo provocado pelas revelações de Edward Snowden repercutiu no Brasil, o tema tornou-se rapidamente uma questão de governo. [...] Naquele momento, a resposta mais séria e completa de reação do Estado brasileiro consistia no Marco Civil da Internet, projeto de lei que se encontrava então pendente de análise – para não dizer meramente engavetado – na Câmara dos Deputados havia quase dois anos." (LEMOS, Ronaldo. O marco civil como símbiolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.3).

332 "Vale mencionar que o Marco Civil funcionou como uma iniciativa pioneira na ideia de uma democracia expandida." (Ibid., p.5).

333 "Países que vão do Chile à Jordânia seguiram vários dos passos do Marco Civil brasileiro, transformando em leis internas dispositivos do projeto concebido no Brasil." (Ibid., p.7).

334 LEMOS, Ronaldo. Internet brasileira precisa de Marco Regulatório Civil. *UOL Tecnologia*, 22 maio 2007. Disponível em <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm>. Acesso em 29 dez. 2016.

dados pessoais à figura jurídica de coisa[335], urgindo por uma resposta eficaz capaz de evitar a promulgação deste projeto retrógado.

A ideia à época, com base na experiência internacional, era que uma lei criminal para a internet constituiria o último passo para a regulamentação da rede. O ideal, inicialmente, seria que a internet recebesse um tratamento na base civil, para posteriormente, diante de um maior amadurecimento do sistema jurídico, regular a eventual tipicidade de condutas no meio virtual.[336]

Em 23 de abril de 2014, a mencionada Lei n.º 12.965, conhecida como Marco Civil da Internet, inaugurou como princípio da disciplina do uso da internet no Brasil a proteção da privacidade e dos dados pessoais[337], instituindo ainda, em vários artigos[338], direito e garantia dos usuários à inviolabilidade da intimidade e da vida privada.

---

335 "O projeto, em seu artigo 183-A, equipara à 'coisa', para efeitos penais, o dado, informação ou unidade de informação em meio eletrônico. Essa equiparação gera efeitos imprevisíveis no ordenamento jurídico brasileiro." (LEMOS, Ronaldo. Internet brasileira precisa de Marco Regulatório Civil. *UOL Tecnologia*, 22 maio 2007. Disponível em <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm>. Acesso em 29 dez. 2016).

336 "[...] o ponto defendido pelo autor era de que a Lei Azeredo invertia indevidamente o caminho da regulamentação da internet no Brasil." (LEMOS, Ronaldo. Uma breve história da criação do marco civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.83).

337 "Art. 3.º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;"

338 São exemplos da proteção da intimidade e vida privada dos usuários na internet os seguintes artigos:
Art. 7.º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Apesar de promulgada em 2014, o nome inicialmente proposto para Lei foi *"Marco Regulatório Civil da Internet"*[339], sendo oriundo do Projeto de Lei n.º 2.126/11 de autoria e iniciativa do Poder Executivo junto à Câmara dos Deputados.[340] Traz princípios e direitos para o uso da internet, tutelando, dentre outros direitos da personalidade, a privacidade, estabelcendo regras gerais de consentimento para coleta, tratamento e armazenamento de dados pessoais.

Como afirmou Carlos Affonso Pereira de Souza, o Marco Civil da Internet é "essencialmente uma afirmação de direitos"[341], criado sob uma perspectiva de "tutela de direitos fundamentais".

Diante do disposto nos parágrafos 3.º e 4.º de seu artigo 11[342] ve-se que os provedores de conexão e de aplicações de internet devem sempre respeitar a legislação pátria, especialmente no tocante ao direito à privacidade, à proteção dos dados pessoais, naquilo que se refere à coleta, à guarda, ao armazenamento ou tratamento de dados.

Há ainda regra do consentimento expresso[343] e do princípio da finalidade[344], não havendo qualquer dúvida, portanto, que as normas acima mencionadas se aplicam

---

339 LEMOS, Ronaldo. Uma breve história da criação do marco civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.82.

340 CÂMARA DOS DEPUTADOS. PL 2126/2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 29 dez. 2016.

341 SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p. 377.

342 "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...] § 3.º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4.º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo."

343 "Art. 7.º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;"

à grande maioria das hipóteses de aplicação do *big data*, quando presentes os requisitos de incidência da norma brasileira.

Na esteira do Marco Civil da Internet, o Ministério da Justiça lançou um Anteprojeto de Lei para a proteção de dados pessoais[345], cujo texto proposto ficou aberto à população para críticas e contribuições pela internet[346], prevê igualmente a proteção da privacidade em inúmeros dispositivos, inclusive nos artigos 1.º e 2.º[347], e maneira ainda mais clara no artigo 17.[348]

O referido APL, que culminou no Projeto n.º 5.276/2016, de autoria do Poder Executivo, traz ainda os legítimos interesses[349] como um de nove formas de requisito lícito de tratamento de dados pessoais, além de não adjetivar o consentimento como expresso, mas tão somente como livre e inequívoco.[350]

---

344 "Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: [...] II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular."

345 "Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural."

346 BRASIL. Anteprojeto de Lei para a Proteção de Dados Pessoais. Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 15 ago. 2015.

347 "Art. 1.º Esta Lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Art. 2.º A disciplina da proteção de dados pessoais no Brasil tem como fundamento o respeito à privacidade, bem como: I - a autodeterminação informativa; II - a liberdade de expressão, comunicação e opinião; III - a inviolabilidade da intimidade, vida privada, honra e imagem;"

348 "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei." Versão final do APL Disponível em: <http://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf>. Acesso em: 20 fev. 2016.

349 "Art. 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: IX – quando necessário para atender aos interesses legítimos do responsável, respeitados os interesses ou os direitos e liberdades fundamentais do titular."

350 "Art. 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento pelo titular de consentimento livre e inequívoco;"

O recente Decreto n.º 8.771[351], de 11 de maio de 2016, regulamenta o Marco Civil da Internet, trazendo, em igual turno, regras atinentes à privacidade, dentre elas reiterando a previsão do princípio da finalidade[352] e ainda definindo o conceito de dados pessoais[353] e de tratamento[354] destes. Note-se que o Decreto e o APL contêm redação idêntica no tocante às definições de dado pessoal[355] e de tratamento[356].

Na análise do Marco Civil da Internet e do Decreto n.º 8.771, conclui-se que a privacidade das pessoas naturais, especificamento no tocante aos seus dados pessoais, encontra ampla proteção no direito positivo brasileiro.

Tais regras incidem sobre todas as operações de coleta, tratamento e armazenamento de dados pessoais, especialmente na internet, o que as faz, sem dúvida, abranger as práticas presentes no *big data*, diante de seu corriqueiro escopo

---

351 "Regulamenta a Lei n.º 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações."

352 "Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: [...] § 2.º Tendo em vista o disposto nos incisos VII a X do caput do art. 7.º da Lei n.º 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I - tão logo atingida a finalidade de seu uso; ou II - se encerrado o prazo determinado por obrigação legal."

353 "Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal – dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; "

354 "Art. 14. Para os fins do disposto neste Decreto, considera-se: [...] II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."

355 APL: Art. 5.º Para os fins desta Lei, considera-se: I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

356 APL: "Art. 5.º Para os fins desta Lei, considera-se: II - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"

de atuação, que se dá, na grande maioria das vezes, por algorítimos e com transmissão de dados pela internet.

Há ainda, na legislação destacada, possibilidade inequívoca de se buscar a responsabilidade civil daquele que tiver a sua privacidade violada, especialmente na coleta, tratamento e armazenagem de dados pessoais, exigindo que seja impedida[357] a circulação não autorizada de informações atinentes aos dados pessoais.

Este novo panorama leva à afirmação de que o titular do direito à privacidade pode, atualmente, exigir não só que seja impedida ou interrompida[358] a coleta, circulação e armazenagem de suas informações pessoais, mas sobretudo que a circulação esteja sempre sobre seu controle e supervisão.[359]

3.1.2 Projetos de Lei sobre proteção de dados

Há no parlamento brasileiro diversos Projetos de Lei que versam sobre dados pessoais, merecendo especial ênfase os Projetos n.º 330/2013[360] do Senado

---

[357] Código Civil. “Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.”

[358] Como mundialmente famoso exemplo de interrupção da circulação de video viola a privacidade, vale mencionar o caso Cicarelli: "Ação inibitória fundada em violação do direito à imagem, privacidade e intimidade de pessoas fotografadas e filmadas em posições amorosas em areia e mar espanhóis – Esfera íntima que goza de proteção absoluta, ainda que um dos personagens tenha alguma notoriedade, por não se tolerar invasão de intimidades [cenas de sexo] de artista ou apresentadora de tv – Inexistência de interesse público para se manter a ofensa aos direitos individuais fundamentais [artigos 1.º, III e 5.º, V e X, da CF] – Manutenção da tutela antecipada expedida no agravo de instrumento n.º 472.738-4 e confirmada no julgamento do agravo de instrumento n.º 488.184-4/3 – Provimento para fazer cessar a divulgação dos filmes e fotografias em websites, por não ter ocorrido consentimento para a publicação – Interpretação do art. 461, do CPC e 12 e 21, do CC, preservada a multa diária de R$ 250.000,00, para inibir transgressão ao comando de abstenção." (SÃO PAULO. Tribunal de Justiça de São Paulo. APELAÇÃO CÍVEL 556.090.4/4-00. Relator: Enio Zuliani. Julgamento: 12/06/2008. Orgão Julgador: 4.ª Câmara de Direito Privado. Publicação: 17/07/2008).

[359] RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.93.

[360] “Art. 1.º Esta Lei estabelece princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados de pessoas naturais, tendo como fundamento o princípio da dignidade da pessoa humana, a proteção da privacidade, a garantia da liberdade e a inviolabilidade da honra e da imagem das pessoas.”

Federal, n.º 4.060/2012[361] da Câmara dos Deputados e o Projeto n.º 5.276/2016, este de autoria do Poder Executivo, oriundo do Anteprojeto de Lei de Proteção de Dados Pessoais, com pedido de urgência na tramitação, este que tramita apensado ao PL 4.060/2012.

A primeira questão que se nota é que cada um dos PLs estabelece uma noção e definição própria para aquilo que seria um dado pessoal. O 5.276 reproduz o já disposto no artigo 14, I do Decreto n.º 8.771/16 quando aduz ser "Dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;", o 330 menciona "Qualquer informação sobre pessoa natural identificável ou identificada;" e o 4.060 estabelece como "Qualquer informação que permita a identificação exata e precisa de uma pessoa determinada."

Percebe-se, diante desta análise, que os PLs n.ºs 5.276 e 330 trazem uma visão expansionista acerca da proteção dos dados pessoais, ao passo que o PL 4.060 se mostra reducionista.[362]

No tocante ao consentimento, o PL n.º 5.276 estabelece que o consentimento passa a ser apenas uma das nove maneiras a autorizar a coleta, uso e tratamento dos dados pessoais, incluindo a figura dos legítimos interesses.[363] O consentimento livre e inequívoco para a funcionar como regra geral, e o expresso apenas em determinadas situações específicas, como quando se tratar de informações sensíveis – Art. 11.

---

361 "Art. 1.º Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem."

362 "A orientação reducionista baseia-se em uma lógica restritiva pela qual dado pessoal é uma informação que deve estar associada a uma pessoa específica. Ele deve ser um signo que permita estabelecer de forma imediata ou direta um vínculo com o seu titular, individualizando-o de forma precisa. [...] Enquanto que a expansionista aposta em uma lógica mais flexível, que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta." (BIONI, Bruno. *XEQUE-MATE*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016. p.14).

363 "Art. 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses. [...] IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberadades fundamentais do titular que exigam a proteção dos dados pessoais, em especial se o titula for menor de idade."

Menciona ainda no parágrafo 7.º do artigo 9.º que o "órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos", o que pode ser de grande valia no contexto do *big data*, cotejando com os legítimos interesses envolvidos, diante de suas especificidades, especialmente no caso de tratamentos secundários, distante da finalidade inicial, sempre respeitando os direitos e liberdades fundamentais do titular.

Cria ainda um órgão competente para zelar pela implementação e fiscalização da Lei e zelar, dentre outros, pela proteção dos dados pessoais, além do Conselho Nacional de Proteção de Dados e da Privacidade – artigos 53-55.

No tocante ao PL 4.060, este também estabelece que os legítimos interesses permitem o tratamento de dados pessoais: "Art. 9.º Os dados pessoais serão tratados com lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares", flexibilizando, de certa forma, a regra do consentimento em algumas outras passagens.[364]

Já o PL 330 veda expressamento o tratamento secundário ao estabelecer regras estritas para o princípio da finalidade em seu artigo 4, inciso I[365], trazendo ainda a

---

364 "Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal.
Art. 13. O tratamento de dados pessoais ou a sua interconexão respeitará a lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares, lhes devendo ser garantido sempre o direito ao bloqueio do registro, salvo se necessário para cumprimento de obrigação legal ou contratual.
Art. 14. Respeitado o disposto no artigo anterior, os responsáveis pelo tratamento de dados poderão compartilhá-los, inclusive para fins de comunicação comercial, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais."

365 "Art. 4.º Ao tratamento de dados pessoais aplicam-se os seguintes princípios: I - coleta, armazenamento e processamento de forma lícita, com observância do princípio da boa-fé e adstritos a finalidades determinadas, vedada a utilização posterior incompatível com essas finalidades; VI - transparência no tratamento de dados, por meio inclusive da comunicação ao titular de todas as informações relevantes ao tratamento dos seus dados, tais como finalidade, forma de coleta e período de conservação, dentre outras; VII - proporcionalidade no tratamento dos dados, sendo vedado o tratamento de dados que não seja adequado, necessário e proporcional à finalidade desejada ou que tenha fundamentado sua coleta; XI - o tratamento de dados pessoais deve ser compatível com as finalidades a que se destinam e com as legítimas expectativas do titular, respeitado o contexto do tratamento;
Art. 16. O tratamento de dados pessoais será encerrado: II - quando o tratamento não se mostrar mais adequado, necessário ou proporcional à finalidade a que se propõe ou que fundamentou sua coleta;"

necessidade de consentimento livre, específico, inequívoco e informado com princípio para o tratamento de dados pessoias.[366]

Apesar disso, em redação que guarda similaredidades com o PL n.º 5.276, o PL 330 traz oito hipóteses as quais autorizam o tratamento de dados pessoais, sendo somente uma delas o consentimento, estabelecendo a possibilidade dos legítimos interesses do titular como forma de tratamento de dados.[367]

Comparando-se os três projetos, especificamente no tocante à hipótese dos legítimos interesses a permitir o tratamento de dados pessoais, nota-se que o PL n.º 5.276 estabelece freios e contrapesos de maneira bastante rígida e evidente, tais como a transparência e direito de oposição do titular[368], solicitação de relatório de impacto à privacidade[369], dentre outros, ao passo que o PL 330 é brando nestas amarras, sendo tais contrapesos inexistentes[370] no PL 4.060.

Em que pese não haver menção expressa sobre o *big data* em nenhum dos textos, em 15 de dezembro de 2016 foi realizado requerimento[371] pelo deputado André Figueiredo no bojo do Projeto de Lei n.º 4.060, com vistas à realização de Seminário Internacional sobre Tratamento de Dados Pessoais, onde um dos tópicos tem como título *"Novas fronteiras e big data"*, o que demonstra estar o tema na ordem do dia, revelando-se crucial ao aprimoramento e evolução legislativa.

---

366 "Art. 4.º Ao tratamento de dados pessoais aplicam-se os seguintes princípios: V – consentimento livre, específico, inequívoco e informado do titular de dados como requisito à coleta de dados pessoais e, ainda, prévio e expresso, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado;"

367 "Art. 12. O tratamento de dados pessoais somente pode ser realizado nas seguintes hipóteses: VIII – quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados."

368 "Art. 10 § 2.º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais."

369 "Art. 10 § 4.º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo."

370 "Art. 9.º caput: Os dados pessoais serão tratados com lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares."

371 CÂMARA DOS DEPUTADOS. Requerimento n.º 11/2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1517227&filename=Tramitacao-PL+4060/2012>. Acesso em: 18 dez. 2016.

Considerando o acima exposto, parece ser o PL n.º 5.276 o mais completo e ponderado, até porque oriundo do Anteprojeto de Lei de Proteção de Dados Pessoais, especialmente quando considerado o atual panorama acerca da necessidade de regulamentação da tutela dos dados pessoais, posto que traz diversas formas de tratamento lícito de dados pessoais, tais como os legítimos interesses, sem ouvidar da autodeterminação informativa e dos valores cardeais do sistema, garantido o exercício e a proteção da privacidade às pessoais naturiais, ao mesmo tempo que não marginaliza por completo a inovação tecnológica, visivelmente presentes nas práticas do *big data*.

3.2 **O Brasil na encruzilhada: para onde caminha a proteção de dados no País?**

Conforme já delineado neste capítulo, há no Brasil proteção no tocante aos dados pessoais, atrelado à privacidade, com tutela constitucional e previsão específica em diversas Leis, dentre elas se destacam o Marco Civil da Internet de 2014 e o Decreto n.º 8.771/2016, porém sem esgotar[372] o tema e inexistindo previsão para casos específicos, como o *big data*.

O relator do Marco Civil da Internet, afirma ainda que:

> O Marco Civil garante a proteção dos dados pessoais e disciplina seu uso pelas empresas de Internet. A proteção à privacidade é reforçada no artigo 8.º: "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet". Além disto, o parágrafo 3.º do artigo 9.º deixa claro que é "vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados". Ou seja, o Marco Civil cria todos os mecanismos para proteger a privacidade do internauta brasileiro.[373]

---

[372] "Com o objetivo de endereçar as questões relacionadas à proteção de dados pessoais e privacidade dos usuários da rede mundial de computadores, o Marco Civil da Internet trouxe algumas previsões, imprecisas e incompletas, a respeito desse tema, que está diretamente relacionado à inviolabilidade da vida privada e da intimidade." (GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.388).

[373] MOLON, Alessandro. *Entenda o Marco Civil da Internet*. 28 abr. 2014. Disponível em: <http://molon.com.br/entenda-o-marco-civil-da-internet/>. Acesso em: 27 dez. 2016.

Note-se que a legislação pátria vigente se mostrou, até o presente momento, garantista[374] e principiológica[375], contendo regras gerais atinentes à coleta, tratamento e guarda de dados pessoais, tais como a finalidade[376], necessidade[377], colocando ainda o consentimento[378] como o pilar regulatório a legitimiar tal prática, aproximando-se, de certa forma ao modelo Europeu, que igualmente trata a privacidade com um direito fundamental.[379]

Porém, ao contrário do que ocorre em diversos países do velho continente, inexiste uma autoridade garante no Brasil, em que pese haver registro de vontade

---

374 "O desenvolvimento do capítulo parte da análise da Lei n.º 12.965/2014, mormente o Capítulo II, artigos 7.º e 8.º, que tratam especialmente da proteção dos direitos de liberdade de expressão e de privacidade, os quais encontram respaldo no artigo 5.º e incisos da Constituição Federal Brasileira de 1988, enquanto teoricamente adota-se o modelo jurídico garantista, a partir da vasta obra do jurista italiano Luigi Ferrajoli." (COPETTI NETO, Alfredo; FISCHER, Ricardo Santi. A natureza dos direitos e das garantias dos usuários de internet: uma abordagem a partir do modelo jurídico garantista. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). *Marco civil da internet*. São Paulo: Atlas, 2014. p.350).

375 "O Marco Civil deveria promover a liberdade de expressão, a privacidade, a neutralidade da rede, o direito de acesso à internet, os limites à responsabilidade dos intermediários e a defesa da abertura (openness) da rede, crucial para a inovação. Uma vez estabelecidos esses princípios, foi então construíudo o texto legal que dava concretude a eles. Cada princípio ganhou um capítulo ou, ao menos, artigos específicos no Marco Civil." (LEMOS, Ronaldo. O marco civil como símbiolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.5).

376 Decreto n.º 8.771. "Art. 13, § 2.º [...] dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I - tão logo atingida a finalidade de seu uso."

377 Decreto n.º 8.771. "Art. 13, § 2.º Tendo em vista o disposto nos incisos VII a X do caput do art. 7.º da Lei n.º 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações."

378 Lei n.º 12.965. "CAPÍTULO II - DOS DIREITOS E GARANTIAS DOS USUÁRIOS. Art. 7.º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;"

379 O regulamento 2016/679 do Parlamento Europeu e do Conselho, aplicável a partir de 25 de maio de 2018, traz em seu preâmbulo: "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito."

política[380] para se criar o denominado Orgão competente[381] e o Conselho Nacional de Proteção de Dados e da Privacidade[382], através do Projeto de Lei n.º 5.276.

Importante ressaltar ainda que no relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais, que originou o Projeto de Lei n.º 5.276, o tema *"Como deve ser o órgão responsável pela aplicação da lei de proteção de dados pessoais?"* ganhou destaque e foi objeto de grande discussão[383], recebendo inúmeras sugestões e contribuições.

Da análise da conjuntura jurídica e legislativa em torno do tema, salta aos olhos que o sistema jurídico brasileiro busca inspiração nos regramentos que tratam das autoridades garantes existentes na Europa[384], local onde se vê tratar de medida

---

380 "Segundo o deputado federal Orlando Silva (PCdoB-SP), as discussões na câmara envolvem inclusive a possibilidade de se criar uma agência reguladora a fim de fiscalizar o uso de dados pessoais." (CANALTECH. *Agência reguladora de dados de usuários na web é possibilidade, diz deputado*. 21 dez. 2016. Disponível em: <https://canaltech.com.br/noticia/protecao-de-dados/agencia-reguladora-de-dados-de-usuarios-na-web-e-possibilidade-diz-deputado-86294>. Acesso em: 23 dez. 2016).

381 "Art. 53. O órgão competente designado para zelar pela implementação e pela fiscalização desta Lei terá as seguintes atribuições: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua confirmidade aos princípios e regras desta Lei; VII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; XII - editar normas sobre proteção de dados pessoais e privacidade."

382 "Art. 55. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugeror ações a serem realizadas pelo órgão competente; IV - realizar estudos e debates sobre a proteção de dados pessoais e privacidade; e V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população."

383 "Uma análise abrangente dos comentários dos participantes revela certa coesão quanto às características gerais que devem pautar a criação do órgão. Tais características têm proximidade com o formato de autoridades de garantia de dados pessoais europeias." (INTERNETLAB. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 dez. 2016).

384 "Os trabalhos de Danilo Doneda (2006) e de Laura Schertel Mendes (2009), pelo que sei, foram os primeiros a tentar traçar um panorama de legislação brasileira e a defender a ideia da adoção do "modelo europeu" (declaração de direitos e criação de órgãos reguladores independentes)." (ZANATA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.455).

indispensável à efetiva proteção dos dados pessoais, especialmente pela necessidade de fiscalização dos agentes envolvidos.[385]

Ocorre que o sistema jurídico pátrio não dispõe de uma legislação específica que verse exclusivamente sobre os dados pessoais, estando o assunto regulado de maneira aberta, principiológica[386], sem adentrar nos meandros da miríade de situações específicas que versam sobre a coleta, tratamento e guarda de dados, como é o caso do *big data*.

Ademais, da leitura dos dispositivos legais que tratam do consentimento no Marco Civil da Internet sobre dados pessoais demonstra que a lei brasileira, ao que parece, tem como foco as modalidades de contratação nas quais haverá, na grande maioria das vezes, aderência do usuário ao contrato cujo consentimento será condicionado à utilização do serviço ou bem oferecido, tais como redes sociais, contas de *e-mail* e aplicativos de celular. Nesta hipótese, portanto, haverá uma tela onde ao contratante será franqueada a leitura dos termos do serviço, devendo consentir com eles.

Esta constatação é possível através das informações sobre a concepção da própria Lei n.º 12.965/2014, cujo esboço que foi preparado em julho de 2009[387], época em que a tecnologia disponível e existente em muito se distancia da atual, e muitas das práticas atualmente existentes e largamente difundidas sequer eram exequíveis.

---

385 *"However, there seems to be a consensus that the process must involve being called 'to account' by some authority for one's actions. The involvement of an external body is, therefore, indispensable."* (GUAGNIN, Daniel; HEMPEL, Leon; ILTEN, Carla; KROENER, Inga; NEYLAND, Daniel; POSTIGO, Hector. *Managing Privacy through Accountability*. London: Palgrave Macmillan, 2016. p.33). Tradução livre: "No entanto, parece haver um consenso de que o processo deve envolver ser chamado 'para prestar contas' por alguma autoridade em razão das suas ações. O envolvimento de um organismo externo é, portanto, indispensável."

386 "O Marco Civil da Internet é uma legislação baseada em princípios. Foi propositalmente concebida para esse fim: definer os valores básicos que a sociedade pretende proteger no uso da internet no Brasil. É ilusório pensar que a solução para os vários problemas jurídicos do uso da internet está na Lei 12.965/2014. A proteção de dados pessoais, por exemplo, está apenas definida como direito. Não há, por enquanto, garantia suficiente para uma adequação da tutela dos dados pessoais no Brasil." (ZANATA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.462-463).

387 "Como se verá, o Marco Civil finalmente aprovado pelo Congresso Nacional em abril de 2014 muito se assemelha à arquitetura que foi definida e articulada naquele momento de julho de 2009." (LEMOS, Ronaldo. Uma breve história da criação do marco civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.93).

No entanto, diante da análise do *modus operandi*[388] da grande maioria dos agentes que utilizam o *big data* como modelo de atuação, revela que será tortuoso e questionável o atendimento integral das previsões legislativas atualmente escritas no ordenamento jurídico pátrio.[389] Com razão já se alerta:

> O big data, junto com outras inovações como as relacionadas com a Internet das Coisas (Internet of Things – IoT), estão mudando sobremaneira o cenário referente aos dados pessoais e exigirão que as agências regulatórias se adaptem a essas novas circunstâncias, seja adequando as ferramentas e os princípios existentes, seja criando novos meios para a aplicação das leis.[390]

Tome-se como exemplo os sensores e câmeras inteligentes: esses objetos são capazes de captar, analisar e armazenar dados pessoais como imagem, sinais vitais, localização[391] por GPS, e transmitir dados em tempo real pela internet, por vezes sendo impossível a leitura ou identificação do contrato e dos termos de uso, e mesmo

---

388 *"By their very nature, IoT and wearable technologies are always on, always sensing, always collecting and always communicating."* (THIERER, Adam. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. p.60. Disponível em: <http://jolt.richmond.edu/v21i2/article6.pdf>. Acesso em: 04 ago. 2015). Tradução livre: "Pela sua própria natureza, o IOT e tecnologias wearable estão sempre ligadas, sempre sentindo, sempre coletando e sempre comunicando."

389 Nos autos da ação civil pública, em trêmite na 2.ª Vara da Justiça Federal no Piauí, Processo n.º 25463-45.2016.4.01.4000, constam, dentre outros, os seguintes pedidos: "d) o DEFERIMENTO DE TUTELA DE URGÊNCIA ou EVIDÊNCIA, para que o réu suspenda a análise (scaneamento) do conteúdo dos e-mails dos usuários do Gmail, em todo o território nacional, enquanto não for colhido o consentimento prévio, expresso e destacado do titular da conta de e-mail, inclusive para o envio de publicidade comportamental, sob pena de multa diária no valor de R$ 100.000,00 (cem mil reais); e) que o Google seja CONDENADO em obrigação de fazer, consistente em obter dos usuários do Gmail, em todo o território nacional, consentimento prévio, expresso e destacado para analisar/scanear o conteúdo de e-mails, na forma do art. 7.º, incisos IX da lei n. 12.965/14, assegurando ainda que a qualquer momento o usuário possa revogar a autorização;"

390 INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. *Big data no projeto Sul Global*: relatório sobre estudos de caso. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

391 *"Whenever you use the Services, Waze will collect: detailed location and route information, for example in the form of GPS signals and other information sent by your mobile device on which the Application is installed and activated. Waze uses this location and route information to create a detailed location history of all of the journeys you have made while using the Application"* (WAZE. *Privacy Policy*. Disponível em: <https://www.waze.com/pt-BR/legal/privacy>. Acesso em: 15 ago. 2015). Tradução livre: "Sempre que usar os Serviços, o Waze irá coletar: informações detalhadas de localização e rota, por exemplo, sob a forma de sinais GPS e outras informações enviadas pelo dispositivo móvel no qual o Aplicativo está instalado e ativado. O Waze usa essa localização e informações de rota para criar um histórico de localização detalhado de todas as viagens que você fez ao usar o aplicativo."

quando disponível, em sua grande maioria, são redigidos por advogados, expondo texto de inúmeras laudas[392] com linguagem técnica, não raro com termos ambíguos.

Diante da evidente constatação de que na era do *big data*, inúmeros itens que hoje representam a Internet das Coisas não possuem sequer telas ou botões, para ter acesso à política de privacidade, o usuário se vê obrigado acessar o *website* do vendedor ou fabricante de forma a consentir ou não com os termos de uso.

Na maioria das vezes, tais informações não são facilmente localizadas[393], em alguns casos, inexistentes. Em certas situações, os indivíduos cujos dados estão sendo analisados sequer tomam conhecimento disso[394], valendo acrescentar a coerente constatação:

> *Enforcing privacy best practices in a age of increasing device miniaturization means that, in many cases, it also will not be possible for consumers to read an organization's privacy policy because many of these Technologies will be too small to even have a display*.[395]

---

392 *"Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days"* (MADRIGAL, Alexis C. Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. *The Atlantic*, Mar. 2012. Disponível em: <http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/>. Acesso em: 03 jan. 2017). Tradução livre: "Ler as políticas de privacidade que você se depara em um ano levaria 76 dias de trabalho."

393 *"Internet of Things devices, however, are currently betwixt and between. A device most likely has no means to display a privacy notice. As a result, such information must be conveyed to consumers elsewhere: in the box with the device, on the manufacturer's website, or in an associated mobile application."* (PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.140, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015. Tradução livre: "Dispositivos da Internet de coisas, entretanto, estão atualmente entre tudo. Um dispositivo provavelmente não tem meios para exibir um aviso de privacidade. Como resultado, essas informações devem ser transmitidas aos consumidores em outros lugares: na caixa com o dispositivo, no site do fabricante ou em uma aplicação móvel associada."

394 *"Many of these technologies and capabilities will eventually operate in the background of consumers lives and be almost invisible do them"* (THIERER, Adam. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. p.9. Disponível em: <http://jolt.richmond.edu/v21i2/article6.pdf>. Acesso em: 04 ago. 2015). Tradução livre: "Muitas dessas tecnologias e capacidades eventualmente operarão no fundo da vida dos consumidores e serão quase invisíveis."

395 Ibid., p.62. Tradução livre: "Aplicar as melhores práticas de privacidade em uma era de crescente miniaturização de dispositivos significa que, em muitos casos, também não será possível aos consumidores lerem a política de privacidade de uma organização, porque muitas dessas tecnologias serão muito pequenas para sequer ter uma tela."

É necessário atentar ainda que a grande maioria das empresas de tecnologia com presença global são oriundas dos Estados Unidos, que criam e desenvolvem seus produtos sob a égide da legislação local, na maioria das vezes ignorando[396] o verdadeiro cipoal de regramentos existentes nas dezenas, as vezes centenas, de países nos quais pretende distribuir seus produtos e serviços, como o Brasil. Em lúcida e acertada dissertação, Eli Pariser afirma:

> *As billions come online in India and Brazil and Africa, the Internet is transforming into a truly global place. Increasingly, it will be the place where we live our lives. But in the end, a small group of American companies may unilaterally dictate how billions of people work, play, comunicate and understand the world. Protecting the early vision of radical connectedness and user control should be an urgente priority for all of us*.[397]

As novas tecnologias na era do *big data*, face a esta realidade de constante coleta e tratamento de dados pessoais, muitas vezes distante da finalidade inicial, desafia os regramentos inscritos no Marco Civil da Internet e no Decreto que o regulamentou, atinentes à privacidade e proteção de dados pessoais, notadamente

---

396 *"Special Note to International Users: The WhatsApp Site and Service are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy Policy, and our Terms of Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes."* (WHATSAPP. *Informação legal do WhatsApp*. Disponível em: <https://www.whatsapp.com/legal/?l=pt_br>. Acesso em: 15 ago. 2015). Tradução livre: "Nota Especial para Usuários Internacionais: O Site e o Serviço da WhatsApp são hospedados nos Estados Unidos e são destinados e dirigidos a usuários nos Estados Unidos. Se você é um usuário que acessa o Site e o Serviço da WhatsApp da União Européia, Ásia ou qualquer outra região com leis ou regulamentos que regem a coleta, uso e divulgação de dados pessoais, que diferem das leis dos Estados Unidos, O uso do Site e do Serviço da WhatsApp, que são regidos pela lei da Califórnia, esta Política de Privacidade e nossos Termos de Serviço, você está transferindo suas informações pessoais para os Estados Unidos e você expressamente consente com essa transferência e consente em ser regido pela lei da Califórnia para esses fins."

397 PARISER, Eli. *The filter bubble*: how the new personalized web is changing what we read and how we think. New York: Penguin Books, 2012. p.243. Tradução livre: "À medida que bilhões de pessoas ficam online na Índia e Brasil e África, a Internet está se transformando em um lugar verdadeiramente global. Cada vez mais, será o lugar onde vivemos nossas vidas. Mas no final, um pequeno grupo de empresas americanas pode unilateralmente ditar como bilhões de pessoas trabalham, brincam, comunicam e entendem o mundo. Proteger a visão inicial de conexão radical e controle de usuários deve ser uma prioridade urgente para todos nós."

diante da necessidade das atuais regras concernentes ao consentimento, como já analisado anteriormente neste capítulo.

Na sociedade da informação, na qual o Brasil se insere, não se mostra plenamente viável, ao menos em termos práticos[398], por exemplo, a todo momento se obter o consentimento expresso e informado, através de cláusula contratual apartada, como determina a Lei brasileira, pois "caso contrário, o consentimento do titular dos dados pessoais será apenas uma falácia a legitimar um resultado totalmente contrário àquele que deve ser extraído da norma: a (des)proteção dos dados pessoais".[399]

Os benefícios sociais oriundos da inovação tecnológica e a difusão de novos serviços e aplicativos constam de igual maneira escritos[400] na Lei n.º 12.965, porém o próprio inciso VIII do artigo 3.º, ao garantir proteção jurídica aos novos modelos de negócios na internet, contem ressalva ao final, estabelecendo que as inovações "não conflitem com os demais princípios estabelecidos nesta Lei".

Vale mencionar, por conseguinte, que a privacidade e proteção dos dados pessoais foram inseridos nos incisos II e III do artigo 3.º, como um dos princípios da disciplina do uso da internet em território nacional.

Saliente-se que é possível avançar na regulamentação brasileira, especialmente no tocante ao disposto no Projeto de Lei n.º 330, o qual estabelece que o consentimento passa a ser apenas uma das oito maneiras a autorizar a coleta, uso e tratamento dos dados pessoais, incluindo a figura dos legítimos interesses.[401]

---

398 "Daí se deduz a impossibilidade de fazer operar o consentimento em todos os casos: e isto significa também a impossibilidade de fundar no consentimento a definição de privacidade." (RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.77).

399 LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do marco civil da internet partir da human computer interaction e da privacy by default. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.287.

400 "Art. 3 A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; [...] VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
Art. 4 A disciplina do uso da internet no Brasil tem por objetivo a promoção: [...] III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso;"

401 "Art. 12. O tratamento de dados pessoais somente pode ser realizado nas seguintes hipóteses: VIII - quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados."

O mesmo pode ser dito com relação ao Projeto de Lei n.º 5.276, que também inaugura a figura dos legítimos interesses[402] e o traz como uma das nove hipóteses de licitude no tratamento de dados.

Neste contexto, o consentimento livre e inequívoco passa a funcionar como regra geral, e o expresso apenas em determinadas situações específicas, como quando se tratar de informações sensíveis, o que permite a ponderação dentro do contexto do *big data*, na medida em que haveria o cotejo com os legítimos interesses envolvidos, porém sem ter como letra morta os direitos fundamentais do titular, garantindo unicidade e coerência normativa ao ordenamento.[403]

Cumpre destacar que este caminho tem sido traçado pelo sistema jurídico Europeu desde a Diretiva n.º 95/46/CE[404], e mais recentemente através de seu novo regulamento n.º 2016/679, já destacado alhures, quando faz referência a práticas e situações as quais se pode inferir que esta o *big data* está sendo retratado.[405]

Novas formas a legitimar o tratamento de dados pessoais parece ser o caminho seguido na Europa[406], onde a sua regulamentação está na vanguarda[407], sem, no

---

402 "Art 7.º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso que prevalecerem os interesses ou direitos e liberdades fundamentais do titular, que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade."

403 TEPEDINO, Gustavo. O direito civil-constitucional e suas perspectivas atuais. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.21-40.

404 "Artigo 7.º Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se [...] ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º 1 do artigo 1.º."

405 "(50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. [...]"

406 "Previsões legais para o tratamento adicional dos dados pessoais sem qualquer tipo de consentimento ulterior do titular, como do interesses legítimos na Diretiva da União Europeia, são um bom exemplo disso." (BIONI, Bruno. *XEQUE-MATE*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016. p.39).

407 Nas palavras do vice-presidente da Comissão Européia: "As nossas propostas assegurarão a confiança no mercado único digital que as pessoas esperam. Pretendo garantir a confidencialidade das comunicações eletrónicas e a proteção da vida privada. O nosso projeto de regulamento

entanto, passar ao largo dos direitos e garantias fundamentais dos indivíduos, especialmente a privacidade.

No Brasil, há registro de esfoço neste sentido, como se vê no tocante ao Anteprojeto de Lei de Proteção de Dados Pessoais que eclodiu no Projeto de Lei n.º 5.276, onde se realirazam consultas públicas através Secretaria Nacional do Consumidor (SENACON) em conjunto com a Secretaria de Assuntos Legislativos (SAL) dentro do escopo do projeto "Pensando o Direito" do Ministério da Justiça.

Buscou-se criar normas mais efetivas e conectadas com a realidade atual e as demandas dos cidadãos, onde foram coletadas inúmeras contribuições para o Anteprojeto, todas minuciosamente organizadas pelo Internetlab[408], em memorável documento publicado na internet.

Nesta consulta pública, no bojo do debate sobre a regulamentação do consentimento como requisito para o tratamento de dados pessoais, perguntou-se se a adjetivação imposta ao consentimento deveria ser restringida ou ampliada.

Nas diversas sugestões, vale destacar as seguintes, que trataram especificamente sobre o *big data* neste contexto:

> Seria impossível prever todas as variações e possibilidades de tratamento de dados pessoais. Esse é, exatamente, o estado atual da arte da tecnologia que, com o advento do Big Data, mostra-se incompatível com relação à exigência de um consentimento específico (Maria Cunha e Melo). Nesses casos, o responsável pelo tratamento não pode definir – ou até mesmo ter uma compreensão clara – da finalidade do processamento dos dados no momento ou antes da coleta inicial e (CTS-FGV, Centre for Information Policy Leadership). Logo, essa exigência seria, extremamente, inviável e prejudicial para as inúmeras atividades comerciais que estão sendo conduzidas por essa potencialidade imprevisível da inovação lastreada no tratamento dos dados pessoais.
> Seguindo a lógica do argumento de que o consentimento do titular dos dados pessoais não deve ser sempre expresso, deve haver a previsão da hipótese de dispensa do consentimento para interesses legítimos para abrir caminho à hipótese de consentimento tácito/implícito [ITI]. Tal como ocorre na diretiva da União Europeia (Diretiva 95\46\CE, em seu artigo 7.º, alínea

---

«Privacidade e Comunicações Eletrónicas» estabelece um justo equilíbrio entre um elevado nível de proteção dos consumidores e, simultaneamente, perspetivas de inovação para as empresas." (COMISSÃO EUROPEIA. Comunicado de imprensa. Comissão propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrónicas e atualiza as regras de proteção de dados para as instituições da EU. Bruxelas, 10 de janeiro de 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017).

408 INTERNETLAB. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 dez. 2016.

> f), essa nova exceção à regra do consentimento assegurará a possibilidade da realização de tratamento de dados de forma facilitada em situações nas quais não haveriam impactos indevidos sobre o indivíduo e seus direitos. Ao final, os titulares dos dados pessoais não seriam onerados com a necessidade de manifestação de seu consentimento a cada instante [IAB]. Isso otimizaria o controle dos dados pessoais, evitando-se a fadiga do consumidor.[409]

As diversas contribuições da sociedade civil e empresas levaram à alteração completa do texto final constante do Anteprojeto de Lei de Proteção de Dados Pessoais, especialmente naquilo que se refere ao consentimento, tornando a redação mais avançada e consentânea com o atual composição sócio-jurídica sobre o tema, resultando na redação do Projeto de Lei n.º 5.276, atualmente em trâmite no Congresso Nacional.

Nesta ceara, observa-se que no *"CAPÍTULO II"*, ao tratar sobre *"REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS"*, o título da *"Seção I"* foi alterado de *"Consentimento"* para *"Requisitos para o tratamento"*. O artigo 7.º, que inicia a Seção I, teve texto originalmente proposto, que consistia em "O tratamento de dados pessoais somente é permitido após: I - consentimento livre, expresso, específico e informado do titular, salvo o disposto no art.", após o amplo debate e contribuições diversas, a ser concebido como "O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento pelo titular de consentimento livre e inequívoco".

Além desta substancial alteração do texto original, o APL trouxe novas hipóteses de requisitos líticos de tratamento, não previstas na redação inicialmente ofertada para debate público, dentre elas o inciso IX que trata dos legítimos interesses[410] do responsável.

Destacou-se o debate acerca das hipóteses de dispensa do consentimento, que seria uma exceção à regra geral, aparecendo novamente o *big data* como sugestão de inclusão no texto do Anteprojeto, *verbis*:

---

[409] INTERNETLAB. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 dez. 2016.

[410] "IX - quando necessário para atender aos interesses legítimos do responsável, respeitados os interesses ou os direitos e liberdades fundamentais do titular."

> Tal como já acontece com pesquisas científicas, jornalísticas e históricas no APL, também deve haver uma exceção para uso de Big Data. Isso porque, tal tecnologia vale-se da técnica da anonimização dos dados, o que reduz, significativamente, eventuais danos da atividade. O APL deve, portanto, fomentar o uso da anonimização e para isso a própria tecnologia do Big data.[411]

Vê-se, portanto, a sociedade civil, as empresas e o governo estão atentos à necessidade de criação de uma Lei geral de proteção de dados pessoais, registrando-se diversas iniciativas das várias esferas dos Poderes para tratar do tema de forma mais refletida com a realidade. Neste sentido, destaca-se:

> A correta interpretação da garantia à intimidade e à vida privada deve ser consentânea do próprio conceito contemporâneo de privacidade, daquilo que qualquer usuário pode esperar, legitimamente, de acordo com os valores sociais e morais, da sua não exposição.[412]

O *big data* urge por abordagem lúcida no debate democrático contemporâneo, especialmente no aprimoramento da legislação brasileira, esta que, sem dúvidas, tem se espelhado[413] no sistema europeu, notadamente quando se percebe ter a privacidade status constitucional no ordenamento pátrio.

A presença dos legítimos interesses, como uma das formas de conferir licitude ao tratamento de dados pessoais se revela um caminho possível, pois constitui uma verdadeira cláusula geral, dispondo de conteúdo flúido, mutável e adaptável com às mais varias situações, muitas delas que, diante da constante e infreável evolução da tecnologia, surgirão no futuro e sequer são possíveis de imaginar neste momento.

Gustavo Tepedino, tratando dos desafios impostos pelas novas tecnologias, defende a utilização das cláusulas abertas para solucionar questões difíceis, senão vejamos:

---

411 INTERNETLAB. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 dez. 2016.

412 GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.381.

413 "Ao mesmo tempo, a Diretiva Europeia 95/46/EC, que já está em vigor há mais de 15 anos e serviu de ponto de partida do Anteprojeto apresentado pelo Ministério da Justiça [...]." (Ibid., p.388).

> Diante da multiplicação de situações trazidas pelas novas tecnologias, muda-se radicalmente a técnica legislativa, valendo-se o legislador de inúmeras cláusulas gerais – às quais permitem ao intérprete amoldar as previsões normativas às peculiaridades do caso concreto –, e os princípios, dotados de força normativa, tornam-se fundamentais para determinação dos ordenamentos aplicáveis aos casos concretos, cada vez mais inusitados.[414]

Neste mesmo sentido, o professor italiano Pietro Perlingieri sustenta de maneira contundente a necessidade de utilização de cláusulas gerais quando se tratar da tutela das sutiações subjetivas existenciais, advogando que deve haver a *"elasticidade da tutela"* e que nenhuma forma de tutela dos direitos da personalidade deveria ser exaustiva, posto que "deixaria de fora algumas manifestações e exigências da pessoa que, em razão do progresso da sociedade".[415]

Cumpre salientar que os legítimos interesses aparecem em diversas passagens dos mais relevantes projetos de lei em trâmite no parlamento, sendo crucial, no entanto, que existam sistemas de "freios e contrapesos"[416], evitando-se um cheque em branco e o esvaziamento do consentimento com regra geral, sendo garantinda a privacidade[417], através do controle dos dados pessoais nas mãos de seu titular.

Ou seja, sob o pretexto dos legítimos interesses a dar licitude ao tratamento de dados, não se pode olvidar da dignidade da pessoa humana como fundamento da república, da direta aplicação das normas constitucionais e da necessidade imperiosa

---

414 TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.17.

415 PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p.765.

416 "Do contrário, a regra geral do consentimento tornar-se-ia exceção, tamanha a elasticidade e as diversas facetas que a hipótese camaleão dos interesses legítimos poderia alcançar. Um sistema de freios e contrapesos deve ser arquitetado para tanto." (BIONI, Bruno. *XEQUE-MATE*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016. p.40).

417 "No entanto, apesar da flexibilidade dos seus critérios, em função das peculiaridades e circunstâncias que envolvem cada caso, deverá a privacidade ter pontos de referência implacáveis: a dignidade humana e o respeito à personalidade de cada indivíduo servirem de guia, como valores constitucionais primordiais e unificadores de todo o sistema." (KLEE, Antonia Espínola Longoni; MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei n.º 12.965/2014). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.299).

de garantir unidade ao ordenamento jurídico[418], sob pena de criação de um microssistema[419] incoerente e absolutamente incostitucional.

Com base em tudo que foi exposto, não há dúvidas de que a criação de uma legislação que regulamente a proteção dos dados pessoais no Brasil é fundamental[420], pois, ao contrário doque pode parecer, o vácuo legislativo constitui verdadeiro empecilho à efetiva tutela da privacidade nos tempos modernos[421], além de trazer imensa insegurança jurídica[422], especialmente quando eventuais conflitos forem levados ao Poder Judiciário, que poderá decidir da forma que quiser, com base apenas em verdadeiro vácuo legislativo, que não contempla a possibilidade de novas formas de traramento de dados, como o *big data*.

---

418 TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.19).

419 Id. O Código Civil, os chamados microssistemas e a Constituição: premissas para uma reforma legislativa. In: Problemas de direito civil-constitucional. Rio de Janeiro: Renovar, 2000. p.5.

420 "Por fim, constata-se que o Marco Civil da Internet possui disposições relativas à proteção de dados pessoais e de comunicação de forma imprecisa e incompleta, o que, provavelmente, somente será integralizado quando da promulgação da Lei de Proteção de Dados e Privacidade." (GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.391).

421 GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.390.

422 "Ao contrário do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade e do laissez-faire. Ao contrário, a ausência de uma legislação que trate das questões civis da rede leva, ao contrário, a uma grande insegurança jurídica." (LEMOS, Ronaldo. O marco civil como símbiolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.10).

CONCLUSÃO

A realidade trazida pela era do *big data* ressalta um cristalino exemplo onde os benefícios da inovação tecnológica, que por vezes se mostram lantentes, chocam-se com os seus riscos, estes mais tangíveis, especialmente por que produzem danos e efeitos colaterais.

Estando o controle dos dados pessoais constantemente desafiado pelas novas tecnologias, deve haver uma profunda reflexão pelos juristas acerca do novo contexto social, econômico, político e tecnológico do século XXI[423], especialmente diante da noção de que o ordenamento jurídico não está confinado ao direito positivo, mas se apresenta na forma de uma sistema heterogêneo e aberto.[424]

Notadamente o instituto da privacidade e do controle de dados pessoais, acaba por contemplar a matriz do consentimento, tendo sido concebido em realidade absoluta distinta da atual, onde o fluxo de informações era ínfimo, a velocidade de captação era lenta e o tratamento se dava de maneira rudimentar.

Com bilhões de sensores conectados, sofisticados mecanismos de inteligência artificial, algorítimos que aprendem, se transformam, tomam decisões e fornecem análises de maneira totalmente automatizada e sem qualquer ação humana, a realidade se mostra em constante transformação, deixando o sistema jurídico atônito e urgindo por novas formas de tutela, que compatilize as novas práticas com os valores cardeiais do sistema.[425]

Não se trata de subverter os valores constantes da tábua axiológica, muito menos esvaziar a fundamental proteção da pessoa humana com valor central do ordenamento, mas de reflexão e adaptação dos institutos jurídicos existentes à atual

---

423 “Toda transformação da realidade social interessa à ciência do direito, já que reage sobre a realidade normativa. Crer que o direito seja imodificável, eterno, a-histórico e insensível a qualquer ideologia é atitude formalista que ignora a conexão entre comportamentos e regras.” (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008. p.170).

424 TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p 9.

425 "Ao direito civil apresenta-se o desafio de incentivar os novos horizontes da ciência e tecnologia sem perder de vista, contudo, a promoção da pessoa humana." (Id. O direito civil-constitucional e suas perspectivas atuais. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.23).

conjuntura que transformou a realidade, de forma que o direito não iniba a progresso e sirva como instrumento de promoção da pessoa, pois inegável que a concepção clássica da privacidade se tornou obsoleta para tratar de todos os novos desafios impostos pelo *big data*.

O tratamento de dados pessoais constitui o principal combustível para o motor que conduz o *big data*, sendo necessária a ponderação entre os direitos da personalidade, que deve levar em conta não somente um exegese insensível à realidade, na sociedade da informação onde a internet se tornou o epicentro do mundo[426], mas promover a concreta realização da pessoa com espaço para a autonomia, a liberdade[427] e a difusão de novas tecnologias.

Especialmente no Brasil, onde inexiste uma Lei geral de proteção de dados, o *big data* acaba sendo tutelado, na maioria das oportunidades, pelo Marco Civil da Internet – Lei n.º 12.965/14, incidindo, principalmente suas regras gerais atinetes ao consentimento. Não há dúvidas de que o Marco Civil foi imbuído das mais nobres intenções, e no contexto sócio-político de sua edição, justificava as medidas protetivas contidas no texto promulgado.

Ocorre que, no afã de dar uma resposta rápida a um real problema diante dos recorrentes abusos praticados na internet, o Marco Civil da Internet acabou tornando rígida a tutela da privacidade e do controle dos dados pessoais, eventualmente relegando à ilegalidade a possibilidade da sociedade desfrutar dos inegáveis benefícios trazidos pelo *big data*.

Em que pese ser louvável, em outro turno, o excesso de zelo do legislador poderá culminar em verdadeira marginalização ou desestímulo à inovação. A grande questão que se coloca é saber se as novas tecnologias prevalecerão sobre os datados regramentos jurídicos, nesta constante tensão entre as previsões legais restritivas e

---

426 GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014. p.5-6.

427 "Liberdade significa, hoje, poder realizar, sem interferências de qualquer gênero, as próprias escolhas individuais, exercendo-as como melhor convier." (BODIN DE MORAES, Maria Celina. *Danos à pessoa humana*: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003. p.107).

o cenário tecnológico verdadeiramente disruptivo e inimaginável[428] à época de criação da Lei.

A figura dos legítimos interesses, a justificar o tratamento de dados pessoais sem a necessidade de rígida modalidade de consentimento previsto como uma regra geral, já existe no sistema jurídico europeu, sendo, no Brasil, objeto dos Projetos de Lei n.os 5.276 e 330, em trâmite no Congresso Nacional.

Parece ser um caminho possível a criação de novas formas a justificar o tratamento de dados, como na figura já existente dos legítimos interesses, sendo fundamental ao sistema jurídico pátrio a edição de norma legal que regulamente a proteção dos dados pessoais, terminando com o vácuo legislativo que tem se revelado verdadeiro impasse à efetiva tutela da privacidade nos tempos modernos, além de trazer imensa insegurança jurídica.

No entanto, a tutela jurídica a ser desenvolvida, evidentemente, não pode constituir em cheque em branco e simplesmente esvaziar o consentimento, devendo, sempre, garantir a tutela a privacidade, através do controle dos dados pessoais nas mãos de seu titular, jamais se olvidando que a dignidade da pessoa humana constitui o fundamento da república, da direta aplicação das normas constitucionais e da garantia unidade ao ordenamento jurídico.[429]

Sem qualquer pretensão de trazer uma solução definitiva aos desafios supra mencionados, a presente obra se destina tão somente a alimentar e estimular o debate e reflexão, valendo, neste espeque, parafrasear o Professor Gustavo Tepedino, que nos ensina: “Há que se construir, superando misoneísmos, técnica interpretativa compatível com o tempo das liberdades e das tecnologias”.[430]

---

[428] “A internet trará desafios não imaginados para a aplicação dos termos do Marco Civil. Isso é uma certeza.” (SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.407).

[429] CANARIS, Claus-Wilhem. *Teses*: pensamento sistemático e conceito de sistema na ciência do direito. 2.ed. Lisboa: Fundação Calouste Gulbenkian, 1996.

[430] TEPEDINO, Gustavo. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v.110, n.419, p.70, jan./jun. 2014.

REFERÊNCIAS

ABIRESEARCH. *Sports and Wellness Drive mHealth Device Shipments to Nearly 30 Million in 2012*. New York, Dec. 2012. Disponível em: <https://www.abiresearch.com/press/sports-and-wellness-drive-mhealth-device-shipments/>. Acesso em: 06 ago. 2015.

_____. *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*. London, United Kingdom, 09 May 2013. Disponível em: <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/>. Acesso em: 04 ago. 2015.

ALEMANHA. *Divisão da Sociedade da Informação*. Disponível em: <http://participacao.mj.gov.br/marcocivil/wp-content/uploads/sites/2/2015/04/23-Alemanha.pdf>. Acesso em: 21 abr. 2015.

ALL THINGS D. *Nearly a Decade Later, the Autocomplete Origin Story*: Kevin Gibbs and Google Suggest. Disponível em: <http://allthingsd.com/20130823/nearly-a-decade-later-the-autocomplete-origin-story-kevin-gibbs-and-google-suggest/>. Acesso em: 30 out. 2016.

ANGWIN, Julia; PARRIS JR. Terry. Facebook Lets Advertisers Exclude Users by Race. *ProPublica*, Oct. 2016. Disponível em: <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>. Acesso em: 13 nov. 2016.

ANTISPAM. *O que é spam?* Disponível em: <http://www.antispam.br/conceito/> Acesso em: 23 abr. 2015.

ASHTON, Kevin. That 'Internet of Things' Thing. *RFID Journal Live*, June 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: 25 jun. 2015.

AUSTIN, Lisa M. Enough About Me: Why Privacy is About Power, not Consent (or Harm). In: SARAT, Austin (Ed.). *A World without Privacy*: What Law Can and Should Do? Cambridge: Cambridge University Press, 2014. p.131-189.

AZEVEDO, Fábio de Oliveira. Privacidade e tratamento dos dados pessoais: limites, possibilidade e responsabilidade. In: MARTINS, Guilherme Magalhães (Coord.). *Temas de responsabilidade civil*. Rio de Janeiro: Lumen Juris, 2012.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*, Rio de Janeiro, v.3, n.2, jul./dez. 2014. Disponível em: <http://civilistica.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-dadignidade-da-pessoa-humana>. Acesso em: 23 abr. 2015.

BAMBERGER, Kenneth; MULLIGAN, Deirdre. *Privay on the Ground*: Drivign corporate behavior in the United States and Europe. Cambridge: MIT Press, 2015.

BANCO CENTRAL DO BRASIL. *Conversão de moedas*. Disponível em: <http://www4.bcb.gov.br/pec/conversao/conversao.asp>. Acesso em: 06 out. 2016.

BARROSO, Luís Roberto. Colisão entre liberdade de expressão e direitos da personalidade: critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa. *Revista de Direito Administrativo*, Rio de Janeiro, v.235, p.1-36, jan./mar. 2004.

BESSA, Leonardo Roscoe. *Responsabilidade civil dos bancos de dados de proteção ao crédito*: diálogo entre o Código de Defesa do Consumidor e a Lei do Cadastro Positivo. Disponível em: <http://www.mpcon.org.br/Revista_mpcon/n01/artigos/ARTIGO_2014-RESPONSABILIDADE_CIVIL_DOS_BANCOS_DOS_DADOS_DE_PROTECAO_AO_CREDITO-DIALOGO_ENTRE_O_CDC_E_A_LEI_DO_CADASTRO_POSITIVO-LEONARDO_ROSCOE_BESSA.pdf>. Acesso em: 10 nov. 2015.

BIONI, Bruno R. *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.

_____. *XEQUE-MATE*: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016.

BOBBIO, Norberto. *A era dos direitos*. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

_____. *A função promocional do direito*: da estrutura à função: novos estudos da teoria do direito. Rio de Janeiro: Manole, 2007.

BODIN DE MORAES, Maria Celina. *Danos à pessoa humana*: uma leitura civil-constitucional dos danos morais. Rio de Janeiro: Renovar, 2003.

_____. O conceito de dignidade humana: substrato axiológico e conteúdo normativo. In: SARLET, Ingo Wolfgang (Org.). *Constituição, direitos fundamentais e direito privado*. Porto Alegre: Livraria do Advogado, 2006. p.107-149.

_____. *Na medida da pessoa humana*: estudo de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, v.15, n.5, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878>. Acesso em: 1.º dez. 2016.

BRENNER, Susan W. Constitutional rights and the new technologies in the United States. In: LEENES, Ronald; KOOPS, Bert-Jaap; HERT, Paul de. *Constitutional rights and new technologies*: a comparative study. New York: Cambridge University Press, 2008. p.225-257.

BRONSON, Kelly; KNEZEVIC, Irena. Big Data in food and agriculture. *Big Data & Society*. Jan./June 2016. Disponível em <http://bds.sagepub.com/content/spbds/3/1/2053951716648174.full.pdf>. Acesso em: 1.º dez. 2016.

CANALTECH. *Agência reguladora de dados de usuários na web é possibilidade, diz deputado*. 21 dez. 2016. Disponível em: <https://canaltech.com.br/noticia/protecao-de-dados/agencia-reguladora-de-dados-de-usuarios-na-web-e-possibilidade-diz-deputado-86294>. Acesso em: 23 dez. 2016

CANARIS, Claus-Wilhem. *Teses*: pensamento sistemático e conceito de sistema na ciência do direito. 2.ed. Lisboa: Fundação Calouste Gulbenkian, 1996.

CENTER FOR MEDICARE & MEDICAID SERVICES. *Fraud Prevention Toolkit.* Disponível em: <https://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/FraudPreventionToolkit.html>. Acesso em: 18 ago. 2016.

CERVASIO, Daniel Bucar. *Privacidade e banco de dados da administração pública*. Dissertação (Mestrado em Direito Civil) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2008.

CHIEL, Ethan. EU citizens might get a ‘right to explanation’ about the decisions algorithms make. *Fusion*, July 2016. Disponível em: <http://fusion.net/story/321178/european-union-right-to-algorithmic-explanation/>. Acesso em: 30 nov. 2016.

CLOVER, Charles. China: When big data meets big brother. *Financial Times*, Jan. 2016. Disponível em: <http://www.ft.com/cms/s/2/b5b13a5e-b847-11e5-b151-8e15c9a029fb.html#axzz4Hy8NUVqa>. Acesso em: 21 ago. 2016.

CNIL. *Status & Composition*. Disponível em: <https://www.cnil.fr/en/node/287>. Acesso em: 25 nov. 2016.

COMISSÃO EUROPEIA. Comunicado de imprensa. Comissão propõe normas rigorosas em matéria de privacidade para todas as comunicações eletrónicas e atualiza as regras de proteção de dados para as instituições da EU. Bruxelas, 10 de janeiro de 2017. Disponível em: <http://europa.eu/rapid/press-release_IP-17-16_pt.htm>. Acesso em: 11 jan. 2017.

COOK, Tim. *Apple's commitment to your privacy*. Disponível em: <https://www.apple.com/privacy/>. Acesso em: 06 ago. 2015.

COPETTI NETO, Alfredo; FISCHER, Ricardo Santi. A natureza dos direitos e das garantias dos usuários de internet: uma abordagem a partir do modelo jurídico garantista. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord). *Marco civil da internet*. São Paulo: Atlas, 2014. p.349-364.

CRAWFORD, Kate; SCHULTZ, Jason. Big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, v.55, n.1, 2014. Disponível em: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>. Acesso em: 29 ago. 2016.

CUSTERS, Bart. Click here to consent forever: expiry dates for informed consent. *Big Data & Society*, 2016.

DAVIS, Kord; PATTERSON, Doug. *Ethics of Big Data*. Sebastopol: O'Reilly Media, 2012.

DE FILIPPI, Primavera; BELLI, Luca. Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation. *European Journal for Law and Technology*, v.3, n.2, p.1-17, 2012.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo I-II.

DELGADO, Mário Luiz. Responsabilidade civil na sociedade de informação: novas tendências. In: RODRIGUES JUNIOR, Otavio Luiz; MAMEDE, Gladson; VITAL DA ROCHA, Maria (Coord.). *Responsabilidade civil contemporânea*: em homenagem a Sílvio de Salvo Venosa. São Paulo: Atlas, 2011. p.372-390.

DENYER, Simon. China's plan to organize its society relies on 'big data' to rate everyone. *The Washington Post*, Oct. 2016. Disponível em: <https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html>. Acesso em: 13 nov. 2016.

_____. China wants to give all of its citizens a score: and their rating could affect every area of their lives. *Independent*, Oct. 2016. Disponível em: <http://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html>. Acesso em: 13 nov. 2016.

DIAKOPOULOS, Nicholas; FRIEDLER, Sorelle. How to Hold Algorithms Accountable. *MIT Technology Review*, Nov. 2016. Disponível em: <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/>. Acesso em: 26 nov. 2016.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Coord.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000.

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

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). *Algorithms in the Criminal Justice System*. Disponível em: <https://epic.org/algorithmic-transparency/crim-justice/>. Acesso em: 26 nov. 2016.

EPSTEIN, Robert; ROBERTSON, Ronald. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences*, 2015. Disponível em: <http://www.pnas.org/content/112/33/E4512.full.pdf>. Acesso em: 25 ago. 2016.

ERENBERG, Jean Jaques. Publicidade patológica na internet à luz da legislação brasileira. *Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo*, v.2, n.1-4, p.109-133, jul. 2002.

EUROPEAN COMMISSION. *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*: Final Report - A study prepared for the European CommissionDG Communications Networks, Content & Technology. 2017. Disponível em: http://ec.europa.eu/newsroom/document.cfm?doc_id=41232>. Acesso em: 11 jan. 2017.

_____. *Opinion 15/2011 on the definition of consent.* Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>. Acesso em: 27 nov. 2016.

_____. *Opinion 03/2013 on purpose limitation*. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 12 out. 2016.

_____. *Proposal for a Regulation of the European Parliament and of the Council*. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>. Acesso em: 11 jan. 2017.

_____. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>. Acesso em: 30 out. 2016.

EUROPEAN COURT OF HUMAN RIGHTS. *Convenção Europeia dos Direitos do Homem*. Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 08 out. 2015.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Handbook on European data protection law*. 2014. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf>. Acesso em: 08 out. 2015.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy by design in big data*. Dec. 2015. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: 15 ago. 2016.

_____. *Privacy by design in big data*: an overview of privacy enhancing technologies in the era of big data analytics. Disponível em: <www.enisa.europa.eu>. Acesso em: 20 nov. 2016.

EVANS, Bryce. Using Big Data to Achieve Food Security. In: BUNNIK, Anno; CAWLEY, Anthony; MULQUEEN, Michael; ZWITTER, Andrej. *Big Data Challenges*: Society, Security, Innovation and Ethics. London: Palgrave Macmillan, 2016. p.127-135.

FOOD AND AGRICULTURE ORGANIZATION (FAO). Disponível em: <http://www.fao.org/economic/ess/ess-home/food/en/>. Acesso em: 18 ago. 2016.

GABINETE DE DOCUMENTAÇÃO E DIREITO COMPARADO. Conselho da Europa. *Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina*. Disponível em: <http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhregionais/convbiologiaNOVO.html>. Acesso em: 13 nov. 2016.

GARTNER. *Top Strategic Predictions for 2016 and Beyond*: The Future Is a Digital Thing. Disponível em: <https://www.gartner.com/doc/3142020?refval=&pcp=mpe>. Acesso em: 09 ago. 2016.

GERSHENFELD, Neil; VASSEUR, J. P. *As objects go online*. Foreign Affairs. Disponível em: <http://www.foreignaffairs.com/articles/140745/neil-gershenfeld-and-jp-vasseur/asobjects-go-online>. Acesso em: 26 maio 2015.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.375-391.

GILPIN, Lyndsey. How big data is going to help feed nine billion people by 2050. *Tech Republic*. Disponível em: <http://www.techrepublic.com/article/how-big-data-is-going-to-help-feed-9-billion-people-by-2050/>. Acesso em: 18 ago. 2016

GOODMAN, Bryce; FLAXMAN, Seth. *European Union regulations on algorithmic decision-making and a "right to explanation"*. Disponível em: <https://arxiv.org/pdf/1606.08813v3.pdf>. Acesso em: 30 nov. 2016.

GOOGLE. *Pesquisar usando o preenchimento automático*. Disponível em: <https://support.google.com/websearch/answer/106230?hl=pt-BR>. Acesso em: 21 ago. 2016

GRANT, Hazel; CROWTHER, Hannah. How Effective Are Fines in Enforcing Privacy? In: WRIGHT, David; DE HERT, Paul. *Enforcing Privacy*: Regulatory, Legal and Technological Approaches. Springer International Publishing, 2016. p.287-305.

GREENWALD, Glen. *No place to hide*: Edward snowden, the NSA and the U.S. surveillance state. New York: Metropolitan Book, 2014.

GROVES, Peter; KAYYALI, Basel; KNOTT, David; VAN KUIKEN, Steve. The 'big data' revolution in health care: accelerating value and innovation. New York: McKinsey & Company, 2013.

GUAGNIN, Daniel; HEMPEL, Leon; ILTEN, Carla; KROENER, Inga; NEYLAND, Daniel; POSTIGO, Hector. *Managing Privacy through Accountability*. London: Palgrave Macmillan, 2016.

GUTWIRTH, Serge; POULLET, Yves; HERT, Paul de. *Data protection in a profiled world*. Dordrecht; New York: Springer, 2010.

HARDY, Quentin. Big Data in Your Blood. *Bits*, Sept. 2012. Disponível em: <http://bits.blogs.nytimes.com/2012/09/07/big-data-in-your-blood/?_php=true&_type=blogs&_r=0>. Acesso em: 25 jun. 2015.

HARTZOG, Woodrow; SELINGER, Evan. Big data in small hands. *Stanford Law Revier*, 2013. Disponível em: <http://www.stanfordlawreview.org/online/privacy-and-big-data/big-data-small-hands>. Acesso em: 02 dez. 2016.

HASSELBALCH, Gry; TRANBERG, Pernille. Privacy is still alive and kicking in the digital age. *Tech Crunch*, Dec. 2016. Disponível em: <https://techcrunch.com/2016/12/25/privacy-is-still-alive-and-kicking-in-the-digital-age/>. Acesso em: 27 dez. 2016.

HEISENBERG, Dorothee. *Negotiating Privacy*: The European Union, the United States, and Personal Data Protection. Boulder: Lynne Rienner Publishers, 2005.

HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*: The Story of Art 16 TFEU. Brussels, Belgium: Springer International Publishing, 2016.

HUNTON & WILLIAMS LLP. The Centre for Information Policy Leadership. *Demonstrating and Measuring Accountability*: A Discussion Document, Accountability Phase II – The Paris Project, October 2010. Disponível em: <https://iapp.org/media/pdf/knowledge_center/Accountability_Phase_II.pdf>. Acesso em: 1.º dez. 2016.

INTERNATIONAL BUSINESS MACHINES (IBM). Disponível em: <http://www.ibm.com/smarterplanet/global/files/ca__en_us__healthcare__ca_brochure.pdf>. Acesso em: 18 ago. 2016.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). *Censo 2010*. Disponível em: <http://censo2010.ibge.gov.br/resultados.html>. Acesso em: 11 ago. 2016.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. *Big data no projeto Sul Global*: relatório sobre estudos de caso. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big-Data_PT-BR_v2.pdf>. Acesso em: 09 ago. 2016.

INTERNATIONAL BUSINESS MACHINES (IBM). *Bringing big data to the enterprise*: What is big data? Disponível em: <https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html>. Acesso em: 06 ago. 2016.

_____. Infographics & Animations: The Four V's of Big Data. Disponível em: <http://www.ibmbigdatahub.com/infographic/four-vs-big-data>. Acesso em: 15 ago. 2016.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). *ICT Facts & Figures 2015*: The world in 2015. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>. Acesso em: 28 ago. 2015.

INTERNET LAB. *O que está em jogo no debate sobre dados pessoais no Brasil?*: relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 27 ago. 2016.

_____. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: <http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de-lei-de-protecao-de-dados-pessoais/>. Acesso em: 04 dez. 2016.

INTERNET LIVE STATS. *Google Search Statistics*. Disponível em: <http://www.internetlivestats.com/google-search-statistics/>. Acesso em: 30 out. 2016.

JORDANA, Jacint. *Governing Telecommunications and the New Information Society in Europe*. Cheltenham, UK: Edward Elgar, 2002.

KENYON, Andrew; RICHARDSON, Megan. *New dimensions in privacy law. International and comparative perspectives*. Cambridge: Cambridge University Press, 2006.

KLEE, Antonia Espínola Longoni; MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei n.º 12.965/2014). In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.291-368.

KLEINER; PERKINS; CAUFIELD; BYERS (KPCB). *Internet Trends 2016*: Code Conference. Mary Meeker, june 2016. Disponível em: <http://www.kpcb.com/internet-trends>. Acesso em: 20 jan. 2016.

KLITOU, Demetrius. *Privacy-invading thecnologies and privacy by design. Safeguarding privacy, liberty and security in the 21st century*. Leinden: Asser Press, 2014.

KNIGHT FOUNDATION. *Knight Foundation, Omidyar Network and Linkedin Founder Reid Hoffman Create $27 Million Fund to Research Artificial Intelligence for the Public Interest*. Jan. 2017. Disponível em: <http://www.knightfoundation.org/press/releases/knight-foundation-omidyar-network-and-linkedin-founder-reid-hoffman-create-27-million-fund-to-research-artificial-intelligence-for-the-public-interest>. Acesso em: 11 jan. 2017.

KONDER, Carlos Nelson. Privacidade e corpo: convergências possíveis. *Pensar* (UNIFOR), v.18, p.352-398, 2013. Disponível em: <http://ojs.unifor.br/index.php/rpen/article/view/2696/pdf>. Acesso em: 05 out. 2016.

KRAMER, Samuel Noah. *The Sumerians*: Their History, Culture, and Character. Chicago: University of Chicago Press, 1963.

LANEY, Doug. *3D Data Management*: Controlling Data Volume, Velocity and Variety. Feb. 2001. Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume- Velocity-and-Variety.pdf. Acesso em: 09 ago. 2016.

LARDINOIS, Frederic. *Google Improves Gmail's Spam Filters, Launches New Analytics Tool For Bulk Senders*. *Tech Crunch*, July 2015. Disponível em: <https://techcrunch.com/2015/07/09/google-improves-gmails-spam-filters-launches-new-analytics-tool-for-bulk-senders/>. Acesso em: 30 out. 2016.

LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014.

LEMOS, Ronaldo. A sociedade contra-ataca: O Marco Civil como símbolo do desejo por inovação no Brasil. *Revista Observatório Itaú Cultural*, São Paulo, n.16, p.92-105, 2007.

_____. Internet brasileira precisa de Marco Regulatório Civil. *UOL Tecnologia*, 22 maio 2007. Disponível em <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm>. Acesso em 29 dez. 2016.

_____. O marco civil como símbiolo do desejo por inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.3-11.

_____. Uma breve história da criação do marco civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.79-100.

LEMOS, Ronaldo; DONEDA, Danilo; SOUZA, Carlos Affonso Pereira de; ROSSINI, Carolina Almeida A. *Estudo sobre a regulamentação jurídica do spam no Brasil*. Trabalho comissionado pelo Comitê Gestor da Internet no Brasil ao Centro de Tecnologia e Sociedade (CTS),da Escola de Direito do Rio de Janeiro/Fundação Getúlio Vargas. Disponível em: <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Acesso em: 18 jul. 2015.

LEONARDI, Marcel. Marco civil da internet e proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.517-538.

LEV-RAM, Michal. What John Deere is Doing to Fight Slumping Sales. *Fortune*, Nov. 2016. Disponível em: <http://fortune.com/2015/11/15/john-deere-software-services-agriculture-data/>. Acesso em: 18 ago. 2016.

LEWICKI, Bruno. Realidade refletida: privacidade e imagem na sociedade vigiada. In: TEPEDINO, Gustavo; FACHIN, Luiz Edson. *O ditreito & o tempo*: embates jurídicos e utopias contemporâneas: estudos em homenagem ao professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008. p.103-114.

LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. A proteçãoo dos dados pessoais na fase de coleta: apontamentos sobre a adjetivaçãoo do consentimento implementada pelo artigo 7, incisos VIII e IX do marco civil da internet partir da human computer interaction e da privacy by default. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.263-290.

LOHR, Steve. The Age of Big Data. *The New York Times*, Feb. 2012. Disponível em: <http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0>. Acesso em: 10 ago. 2016.

MARKET WIRED. *Mobile Healthcare and Medical App Downloads to Reach 44 Million Next Year, Rising to 142 Million in 2016, Finds Juniper Research Limited*. Nov. 2011. Disponível em: <http://www.marketwired.com/press-release/mobile-healthcare-medical-app-downloads-reach-44-million-next-year-rising-142-million-1591994.htm>. Acesso em: 06 ago. 2015.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na internet*. São Paulo: Revista dos Tribunais, 2008.

MATTELART, Armand. *História da sociedade da informação*. Tradução de Nicolás Nejimi Campanário. 2.ed. rev. atual. São Paulo: Loyola, 2006.

MAYER-SCHONBERGER, Viktor. *Delete*: the virtue of forgetting in the digital age. Oxford: Princeton University Press, 2011.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. *Big data*: a Revolution That Will Transform How We Live, Work, and Think. New York: Houghton Mifflin Harcourt, 2013.

MEDICARE. *The Affordable Care Act & Medicare*. Disponível em: <https://www.medicare.gov/about-us/affordable-care-act/affordable-care-act.html. Acesso em: 21/08/2016.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.

MERRILL, Jeremy B. Liberal, Moderate or Conservative? See How Facebook Labels You. *The New York Times*, Aug. 2016. Disponível em: <http://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html?_r=0>. Acesso em: 24 ago. 2016.

MICHALSKI, Jerry. Big Data and the Stalker Economy. *Forbes*, Mar. 2012. Disponível em: <http://www.forbes.com/sites/jerrymichalski/2012/03/10/big-data-stalker-economy/#1ec615604636>. Acesso em: 18 nov. 2016.

MIMS, Christopher. To Feed Billions, Farms Are About Data as Much as Dirt. *The Wall Street Journal*, Aug. 2015. Disponível em: <http://www.wsj.com/articles/to-feed-billions-farms-are-about-data-as-much-as-dirt-1439160264>. Acesso em: 18 ago. 2016.

MOLON, Alessandro. *Entenda o Marco Civil da Internet*. 28 abr. 2014. Disponível em: <http://molon.com.br/entenda-o-marco-civil-da-internet/>. Acesso em: 27 dez. 2016.

MONTEIRO FILHO, Carlos Edison do Rêgo. Rumos cruzados do direito civil pós – 1988 e do constitucionalismo de hoje. In: TEPEDINO, Gustavo. *Direito civil contemporâneo*: novos problemas à luz da legalidade constitucional. São Paulo: Atlas, 2008. p.262-281.

_____. O conceito de dano moral nas relações de trabalho. *Civilistica.com*, Rio de Janeiro, v.3, n.1, jan./jun. 2014. Disponível em: <http://civilistica.com/o-conceito-de-dano-moral-nas-relacoes-de-trabalho/>. Acesso em: 1.º nov. 2016.

_____. Subversões hermenêuticas: a Lei da Comissão da Anistia e o direito civil-constitucional. *Civilistica.com*, Rio de Janeiro, v.5, n.1, 2016. Disponível em: <http://civilistica.com/subversoes-hermeneuticas/>. Acesso em: 1.º out. 2016.

MONTEIRO FILHO, Carlos Edison do Rêgo; RITO, Fernanda Paes Leme Peyneuau. Subsídios para o equilíbrio funcional dos contratos. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Coord.). *O direito civil entre o sujeito e a pessoa*: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p.425-442.

MONTELEONE, Shara. Ambient Intelligence: Legal Challenges and Possible Directions for Privacy Protection. In: AKRIVOPOULOU, Christina. *Personal data privacy and protection in a surveillance era*: technologies and practices. Hershey, PA: Information Science Reference, 2011. p.201-213.

MORGAN, Jacob. Privacy Is Completely And Utterly Dead, And We Killed It. *Forbes*, Aug. 2014. Disponível em: <http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#46c9c18fdfbd>. Acesso em: 1.º dez. 2016.

NEWSROOM. *Our History*. Disponível em: <http://newsroom.fb.com/company-info/>. Acesso em: 13 nov. 2016.

NIKE. *APP & Device Support*. Disponível em: <https://secure-nikeplus.nike.com/plus/support#answers/detail/a_id/21061/kw/privacy%20policy> Acesso em: 07 ago. 2015.

NIXON, Ron. Visitors to the U.S. May Be Asked for Social Media Information. *The New York Times*, June 2016. Disponível em: <http://www.nytimes.com/2016/06/29/us/homeland-security-social-media-border-protection.html?_r=0> Acesso em: 18 nov. 2016.

OBBEMA, Fokke; VLASKAMP, Marije; PERSSON, Michael. China rates its own citizens - including online behaviour. *The Volkskrant*, Apr. 2015. Disponível em: <http://www.volkskrant.nl/buitenland/china-rates-its-own-citizens-including-online-behaviour~a3979668/>. Acesso em: 13 nov. 2016.

OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009). *UCLA Law Review*, v.57, p.1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12. Disponível em: <http://ssrn.com/abstract=1450006>. Acesso em: 1.º out. 2016.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *The OECD Privacy Framework*. 2013. Disponível em: <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. Acesso em: 20 nov. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *World population 2015*. Disponível em: <http://esa.un.org/unpd/wpp/Publications/Files/World_Population_2015_Wallchart.pdf>. Acesso em: 20 jan. 2016.

PAI, Aditi. Breathometer tops $1M in sales for smartphone breathalyzer. *Mobi Health News*, May 2014. Disponível em: <http://mobihealthnews.com/33325/breathometer-tops-1m-in-sales-for-smartphone-breathalyzer/>. Acesso em: 07 ago. 2015.

PALETTA, Damian. U.S. Working on Plan to Scrutinize Social Media in Visa Reviews. *The Wall Street Journal*, Dec. 2015. Disponível em: <http://www.wsj.com/articles/u-s-working-on-plan-to-scrutinize-social-media-in-visa-reviews-1450122633>. Acesso em: 18 ago. 2016.

PARISER, Eli. *The filter bubble*: how the new personalized web is changing what we read and how we think. New York: Penguin Books, 2012.

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

PEPPET, Scott R. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review*: v.93, p.85-176, 2014. Disponível em: <http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf>. Acesso em: 25 jun. 2015.

PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Rio de Janeiro: Renovar, 2008.

PRIES, Kim; DUNNIGAN, Robert. *Big Data Analytics*: A Practical Guide for Managers. Boca Raton: Taylor & Francis Group, 2015.

PRIVACY SHIELD. *Privacy Shield Program Overview*. Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em: 25 nov. 2016.

QUARTZ. *Why Apple is suddenly so obsessed with your privacy*. Disponível em: <http://qz.com/423320/apple-is-lagging-behind-google-in-context-so-its-fighting-back-with-privacy/. Acesso em: 25 jun. 2015.

READING, Viviane. *Data protection reform*: restoring trust and building the digital single market. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm>. Acesso em: 14 dez. 2016.

RENGEL, Alexandra. *Privacy in the 21st Century*. Leiden: Martinus Nijhoff Publishers, 2013.

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

ROYTE, Elizabeth. How ‘Ugly’ Fruits and Vegetables Can Help Solve World Hunger. *National Geographic*, Mar. 2016. Disponível em: <http://www.nationalgeographic.com/magazine/2016/03/global-food-waste-statistics/. Acesso em: 18 ago. 2016.

SCHNEIER, Bruce. 'Stalker economy' here to stay. *CNN*, Nov. 2013. Disponível em: <http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/>. Acesso em: 13 out. 2016.

SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2011.

_____. *Direitos civil e constituição*. São Paulo: Atlas, 2013.

_____. Marco civil da internet: avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.277-306.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. Reconciling Personal Information in the United States and the European Union. *California Law Review*, v.102, n.4, 2014. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4252&context=californialawreview>. Acesso em: 25 nov. 2016.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 22.ed. São Paulo: Revista dos Tribunais, 2003.

SOUZA, Carlos Affonso Pereira de. Responsabilidade civil dos provedores de acesso e de aplicações de Internet: evolução jurisprudencial e os impactos da Lei 12.695/2014 (Marco Civil da Internet). In: LEITE, George Salomão; LEMOS, Ronaldo (Coord.). *Marco civil da internet*. São Paulo: Atlas, 2014. p.791-816.

_____. As cinco faces da proteção à liberdade de expressão no marco civil da internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & Internet III*. São Paulo: Quartier Latin, 2015. Tomo II. p.377-408.

SOUZA, Carlos Affonso Pereira de; SILVA JUNIOR, Ronaldo Lemos da (Org.); VIOLA, M. (Org.). *Understanding Brazil's Internet Bill of Rights*. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2015. v.1.

STANLEY, Jay. China's Nightmarish Citizen Scores Are a Warning For Americans. *American Civil Liberties Union*, Oct. 2015. Disponível em: <https://www.aclu.org/blog/free-future/chinas-nightmarish-citizen-scores-are-warning-americans. Acesso em: 21 ago. 2016.

STARR, Sonja B. Evidence-Based Sentencing and the Scientific Rationalization of Discrimination. *Stanford Law Review, Forthcoming; University of Michigan Law & Econ Research Paper n.13-014*, 2013. Disponível em: <https://ssrn.com/abstract=2318940>. Acesso em: 10 nov. 2016.

STEYER, James. High-Tech Hypocrisy. *Recode*, May 2015. Disponível em: <http://recode.net/2015/05/18/high-tech-hypocrisy/> Acesso em: 25 jun. 2015.

TANG, Chunlei. *The data industry*: the business and economics of information and big data. New Jersey: Wiley, 2016.

TAVARES DA SILVA, Beatriz Regina; PEREIRA DOS SANTOS, Manoel J. (Coord.). *Responsabilidade civil na internet e nos demais meios de comunicação*. 2.ed. São Paulo: Saraiva, 2012.

TECHOPEDIA. *Internet of Things (IoT)*. Disponível em: <http://www.techopedia.com/definition/28247/internet-of-things-iot>. Acesso em: 04 ago. 2015.

TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o marco civil da internet. *Revista Fórum de Direito Civil – RFDC*, Belo Horizonte, v.4, n.10, set./dez. 2015. Disponível em: <http://www.bidforum.com.br/bid/PDI0006.aspx?pdiCntd=238166>. Acesso em: 17 dez. 2015.

TEIXEIRA, Tarcisio. A responsabilidade civil no comércio eletrônico: a livre-iniciativa e a defesa do consumidor. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo II.

TENE, Omer; POLONETSKY, Jules. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, v.11, n.5, 2013. Disponível em: <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip>. Acesso em: 1.º fev. 2016.

_____. Privacy and Big Data: Making Ends Meet. (September 3, 2013). *Stanford Law Review*, v.66, n.25, 2013. Disponível em: <http://ssrn.com/abstract=2628412>. Acesso em: 10 jan. 2016.

_____. Privacy in The Age of Big Data: A Time for Big Decisions. (September 2, 2012). *Stanford Law Review*, v.64, n.63, 2012. Disponível em: <http://www.stanfordlawreview.org/online/privacy-paradox/big-data>. Acesso em: 20 fev. 2016.

TEPEDINO, Gustavo. O Código Civil, os chamados microssistemas e a Constituição: premissas para uma reforma legislativa. In: Problemas de direito civil-constitucional. Rio de Janeiro: Renovar, 2000. p.1-16.

_____. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.3-19.

_____. Notas sobre a função social dos contratos. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.145-155.

_____. O direito civil-constitucional e suas perspectivas atuais. In: *Temas de direito civil*. Rio de Janeiro: Renovar, 2009. Tomo III. p.21-40.

_____. Liberdades, tecnologia e teoria da interpretação. *Revista Forense*, v.110, n.419, p.77-96, jan./jun. 2014.

_____. O papel atual da doutrina do direito civil entre o direito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (Coord.). *O direito civil entre o sujeito e a pessoa*: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. p.17-38.

THE GUARDIAN. *Will the internet of things result in predictable people?* Aug. 2015. Disponível em: <http://www.theguardian.com/technology/2015/aug/10/internet-of-things-predictable-people>. Acesso em: 14 ago. 2015.

THIERER, Adam. *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*. Disponível em: <http://jolt.richmond.edu/v21i2/article6.pdf>. Acesso em: 04 ago. 2015.

THORP, Jer. Big Data Is Not the New Oil. *Harvard Business Review*, Nov. 2012. Disponível em: <https://hbr.org/2012/11/data-humans-and-the-new-oil>. Acesso em: 20 nov. 2016.

UNDATA. *China*. Disponível em: <http://data.un.org/CountryProfile.aspx?crName=china>. Acesso em: 13 nov. 2016.

UNITED STATES DEPARTMENT OF COMMERCE. Disponível em: <https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf>. Acesso em: 27 ago. 2016.

UNITED NATIONS GLOBAL PULSE. *Global Pulse*. Disponível em: <http://www.unglobalpulse.org/about-new>. Acesso em: 02 nov. 2016

US DEPARTMENT OF HOMELAND SECURITY. *State and Major Urban Area Fusion Centers*. Disponível em: <https://www.dhs.gov/state-and-major-urban-area-fusion-centers>. Acesso em: 18 nov. 2016.

US DEPARTMENT OF STATE. *Precision Agriculture and Global Food Security*. Disponível em: <http://www.state.gov/e/stas/series/212172.htm>. Acesso em: 18 ago. 2016

VANIAN, Jonathan. Why Data Is The New Oil. *Fortune*, July 2016. Disponível em: <http://fortune.com/2016/07/11/data-oil-brainstorm-tech/>. Acesso em: 20 nov. 2016.

VIEIRA, Tatiana Malta. *O direito à privacidade na socidedade da informação*: efetividade desse direito fundamental diante dos avanços na tecnologia da informação. 2007. Dissertação (Mestrado em Direito, Estado e Sociedade) - UNB, Brasíia, 2007.

VOSS, Gregory; WOODCOCK, Katherine. *Navigating EU privacy and data protection laws*. Chicago, Illinois: American Bar Association, 2015.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Civilistica.com*, Rio de Janeiro, v.2, n.3, jul./set. 2013. Disponível em: <http://civilistica.com/the-right-to-privacy>. Acesso em: 20 abr. 2015.

WHATSAPP. *Informação legal do WhatsApp*. Disponível em: <https://www.whatsapp.com/legal/?l=pt_br>. Acesso em: 15 ago. 2015.

WAZE. *Privacy Policy*. Disponível em: <https://www.waze.com/pt-BR/legal/privacy>. Acesso em: 15 ago. 2015

WEISS, Martin A.; ARCHICK, Kristin. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service, Report R44257*, May 19, 2016. Disponível em: <https://www.fas.org/sgp/crs/misc/R44257.pdf>. Acesso em: 25 ago. 2016.

WEISER, Mark. The computer for the 21st century. *Scientific American*, v.265, n.3, p.66-75, Sept. 1991.

WILLIAMS, Timothy. Facial Recognition Software Moves From Overseas Wars to Local Police. *The New York Times*, Aug. 2015. Disponível em: <http://mobile.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html>. Acesso em: 14 ago. 2015.

WHITE HOUSE. *Big Data and Privacy: A Technological Perspective.* Executive Office of the President President's Council of Advisors on Science and Technology, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em: 10 set. 2016.

_____. *Big data*: Seizing Opportunities, Preserving Values, Executive Office of the President. Washington, May 2014. Disponível em: <https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>. Acesso em: 20 jan. 2016.

_____. *Big Data*: A Report on Algorithmic Systems, Opportunity, and Civil Rights. Executive Office of the President. May 2016. Disponível em: <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Acesso em: 29 ago. 2016.

WIRED. *Google Says Its AI Catches 99.9 Percent of Gmail Spam*. Disponível em: <https://www.wired.com/2015/07/google-says-ai-catches-99-9-percent-gmail-spam/>. Acesso em: 30 out. 2016.

_____. *The Internet of Everything Will Impact Everything, Including Your Next Tech Job*. Disponível em: <http://www.wired.com/2015/02/internet-of-everything-your-next-tech-job/>. Acesso em: 04 ago. 2015.

WISHPOND. *41 Up-to-Date Facebook Facts and Stats*. Disponível em: <http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats>. Acesso em: 22 jan. 2016.

WORLD ECONOMIC FORUM. *Big Data, Big Impact*: New Possibilities for International Development. Disponível em: <http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf>. Acesso em: 02 jan. 2017.

ZANATA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (Org.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. Tomo I. p.447-470.

ZDNET. *M2M and the Internet of Things*: A guide. Disponível em: <http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide/>. Acesso em: 25 jun. 2015.

DOCUMENTOS JURÍDICOS

BRASIL. Anteprojeto de Lei para a Proteção de Dados Pessoais. Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 15 ago. 2015.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Decreto n.º 8.771, de 11 de maio de 2016. Regulamenta a Lei n.º 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei Complementar n.º 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei n.º 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei n.º 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5.º, no inciso II do § 3.º do art. 37 e no § 2.º do art. 216 da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei n.º 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 1.º dez. 2016.

BRASIL. Ministério da Justiça. Anteprojeto de Lei. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <https://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf>. Acesso em: 1.º dez. 2016.

BRASIL. Projeto de Lei n.º 84/1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 1.º dez. 2016.

BRASIL. Superior Tribunal de Justiça. *AgREsp 917.162-SP*. Relator: Min. Ricardo Villas Bôas Cueva. Disponível em: <http://www.jusbrasil.com.br/diarios/documentos/386875692/ andamento-do-processo-n-2016-0122040-3-agravo-recurso-especial-21-09-2016-do-stj>. Acesso em: 1.º dez. 2016.

BRASIL. Superior Tribunal de Justiça. *ARE 660861-MG*. Relator: Min. Luiz Fux. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoAndamento.asp?incidente=4155926>. Acesso em: 27 dez. 2106.

BRASIL. Superior Tribunal de Justiça. *REsp 1.193.764/SP*. Relator: Min. Nancy Andrighi. Órgão Julgador: Terceira Turma. Publicação: DJe 8/8/2011.

BRASIL. Superior Tribunal de Justiça. *REsp 1.323.754*. Relator: Min. Nancy Andrigui. Julgamento: 19/06/2012. Órgão Julgador: Terceira Turma. Publicação: DJe 28/08/2012.

BRASIL. Superior Tribunal de Justiça. *Súmula 550*. Disponível em: <https://www.legjur.com/sumula/busca?tri=stj&num=550>. Acesso em: 1.º dez. 2016.

CÂMARA DOS DEPUTADOS. PL 2126/2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 29 dez. 2016.

CÂMARA DOS DEPUTADOS. PL 4060/2012. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 1.º dez. 2016.

CÂMARA DOS DEPUTADOS. PL 5276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 1.º dez. 2016.

CÂMARA DOS DEPUTADOS. Requerimento n.º 11/2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1517227&filename=Tramitacao-PL+4060/2012>. Acesso em: 18 dez. 2016.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIˆO EUROPEIA (2000/C 364/01). *Jornal Oficial das Comunidades Europeias*, 18 dez. 2000. Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 1.º dez. 2016.

COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>. Acesso em: 10 dez. 2016.

EUROPA. Acordo sobre o Espaço Económico Europeu. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:21994A0103(01)&from=EN>. Acesso em: 08 out. 2015.

ITALIA. Data Protection Code - Legislative Decree n.º 196/2003. Disponível em: <http://www.garanteprivacy.it/home_en/italian-legislation#1>. Acesso em: 1.º dez. 2015.

ITALIA. Garante per la protezione dei dati personali. Disponível em: <http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf>. Acesso em: 20 nov. 2015.

ITALIA. Protection of individuals and other subjects with regard to the processing of personal data. ACT no. 675 of 31.12.1996. Disponível em: <http://www.privacy.it/legge675encoord.html>. Acesso em: 1.º nov. 2015.

SÃO PAULO. Tribunal de Justiça de São Paulo. APELAÇÃO CÍVEL 556.090.4/4-00. Relator: Enio Zuliani. Julgamento: 12/06/2008. Orgão Julgador: 4.ª Câmara de Direito Privado. Publicação: 17/07/2008.

SENADO FEDERAL. Projeto de Lei do Senado n.º 330, de 2013. Estabelece princípios, garantias, direitos e obrigações referentes à proteção, ao tratamento e ao uso de dados pessoais. Disponível em: <http://livros-e-revistas.vlex.com.br/vid/protecao-dos-dados-pessoais-652787933>. Acesso em: 1.º dez. 2016.

THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). C-131/12. Disponível em: <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>. Acesso em: 20 nov. 2016.

THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf>. Acesso em: 23 dez. 2016.

THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Judgment in Case C-362/14 - Maximillian Schrems v Data Protection Commissioner. Disponível em: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>. Acesso em: 27 ago. 2016.

THE COURT OF JUSTICE OF THE EUROPEAN UNION (CURIA). Processo C-362/14. Disponível em: <http://curia.europa.eu/juris/documents.jsf?num=C-362/14>. Acesso em: 27 ago. 2016.

UNIÃO EUROPEIA. Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX:31995L0046>. Acesso em: 1.º dez. 2016.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 1.º dez. 2016.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:pt:PDF>. Acesso em: 10 dez. 2016.