# REVISTA INTERNACIONAL
# CONSINTER
# DE DIREITO

Publicação Semestral Oficial do
Conselho Internacional de Estudos
Contemporâneos em Pós-Graduação

**ANO IV – NÚMERO VII**

**2º SEMESTRE 2018**

## ESTUDOS CONTEMPORÂNEOS

017990

**Europa** – Rua General Torres, 1.220 – Lojas 15 e 16 – Tel: +351 223 710 600
Centro Comercial D'Ouro – 4400-096 – Vila Nova de Gaia/Porto – Portugal
Home page: *www.editorialjurua.com/revistaconsinter/*
e-mail: *internacional@jurua.net*

**ISSN: 2183-6396**

**Depósito Legal: 398849/15**

**DOI: 10.19135/revista.consinter.0007.00**



A presente obra foi aprovada pelo Conselho Editorial Científico da Juruá Editora, adotando-se o sistema *blind view* (avaliação às cegas). A avaliação inominada garante a isenção e imparcialidade do corpo de pareceristas e a autonomia do Conselho Editorial, consoante as exigências das agências e instituições de avaliação, atestando a excelência do material que ora publicamos e apresentamos à sociedade.

# REVISTA INTERNACIONAL CONSINTER DE DIREITO

Publicação Semestral Oficial do
Conselho Internacional de Estudos
Contemporâneos em Pós-Graduação

**ANO IV – NÚMERO VII**

**2º SEMESTRE 2018**

## ESTUDOS CONTEMPORÂNEOS

Porto
Editorial Juruá
2018

## COLABORADORES:

Alice Ribas Dias Bonizzato
Alvaro Luiz Travassos de Azevedo Gonzaga
Ana Isabel Segovia San Juan
Antonio Felipe Delgado Jiménez
Candida Joelma Leopoldino
Carla Benedetti de Oliveira Andrade
Carla Liliane Waldow Esquivel
Carlos de Fuentes Gª-Romero de Tejada
Diogo Basilio Vailatti
Dolores Palacios González
Edna Raquel Hogemann
Eugênio Facchini Neto
Flávio de Azambuja Berti
Francisco Javier Sosa Álvarez
Grasiele Augusta Ferreira Nascimento
Héctor Luis Lovera Esquivel
Icaro Reinaldo Teixeira
Jaime Gallegos Zúñiga
Jesús Víctor Alfredo Contreras Ugarte
José Laurindo de Souza Netto
Jose María Asencio Gallego
José Maurício Conti
Jozélia Nogueira
Judith Morales Barceló
Karine Silva Demoliner
Luigi Bonizzato
Luísa Munhoz Bürgel Ramidoff
Maria Celeste Cordeiro Leite dos Santos
Marilene Araújo
Mário Luiz Ramidoff
Maritza de la Caridad McCormack Bequer
Marta Madriñán Vázquez
Naiara Posenato
Nilton César da Silva Flores
Ricardo Delgado Preti
Roberta Maria Costa Santos
Roberta Soares da Silva
Rodrigo Polanco Lazo
Tatsiana Ushakova
Thiago Serrano Pinheiro de Souza
Tiago Martinez
Vanessa Fontana
Vinicius Figueiredo Chaves

# Integrantes do Conselho Editorial do

# APRESENTAÇÃO

A **Revista Internacional CONSINTER de Direito** é uma publicação de cariz periódico do **CONSINTER – Conselho Internacional de Estudos Contemporâneos em Pós-Graduação** que tem por objetivo constituir-se num espaço exigente para a divulgação da produção científica de qualidade, inovadora e com profundidade, características que consideramos essenciais para o bom desenvolvimento da ciência jurídica no âmbito internacional.

Outra característica dos trabalhos selecionados para a **Revista Internacional CONSINTER de Direito** é a multiplicidade de pontos de vista e temas através dos quais o Direito é analisado. Uma revista que se pretende internacional tem o dever de abrir horizontes para temas, abordagens e enfoques os mais diversos e, através deste espaço, colaborar com um melhor diálogo académico.

Resultado de um trabalho criterioso de seleção, este volume que agora se apresenta destina-se a todos aqueles que pretendem pensar o Direito, ir além da sua aplicação quotidiana, mas sem deixar de lado o aspecto prático, tão característico das ciências.

# DIREITO À PRIVACIDADE E NOVAS TECNOLOGIAS: BREVES CONSIDERAÇÕES ACERCA DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NA EUROPA

# RIGHT TO PRIVACY AND NEW TECHNOLOGIES: BRIEF CONSIDERATIONS ABOUT THE PROTECTION OF PERSONAL DATA IN BRAZIL AND EUROPE

DOI: 10.19135/revista.consinter.0007.01

*Eugênio Facchini Neto*[1] *– ORCID: https://orcid.org/0000-0001-9978-886X*
*Karine Silva Demoliner*[2] *– ORCID: https://orcid.org/0000-0003-3581-2466*

**Resumo:** O objetivo desse artigo é analisar a evolução do conceito de privacidade, sua transformação em direito à autodeterminação informativa e seus impactos normativos. O advento das tecnologias da comunicação e da informação transformou a sociedade contemporânea sob muitos aspectos. Um deles consiste na possibilidade de acessar, armazenar e sistematizar dados sobre cada indivíduo. Esse acúmulo de informações sobre alguém significa poder, político e econômico, diante da possibilidade de influenciar comportamentos. Assim, a privacidade que inicialmente significava o direito de ser deixado só converteu-se em direito de manter controle sobre as próprias informações, especialmente sobre os dados sensíveis. A partir dos anos setenta, com a primazia da Alemanha, diversos países começaram a regulamentar esse importante aspecto das sociedades contemporâneas. Recentemente a União Europeia substituiu Diretiva de 1995 por um novo e mais abrangente Regulamento, que entrou em vigor em maio de 2018. Referido Regulamento, pelo cuidadoso preparo a que foi submetido, tem potencial para influenciar as normas de países não integrantes da União Europeia, como é o caso do Brasil, onde atualmente o Congresso debate importante sistematização legislativa do setor. O presente artigo abordará essa evolução da noção de privacidade, a preocupação com o controle de dados, fazendo breve análise do Regulamento europeu e das propostas legislativas no Brasil. Conclui-se no sentido de que todos os esforços – legislativos e hermenêuticos – devem ser encetados para garantir maior proteção da autodeterminação informativa, pois isso significa, no mundo virtual em que passamos a viver parte de nossas vidas, maior proteção à pessoa humana.

**Palavras-chave**: Direito à Privacidade; *Dados Pessoais*; *Dados Sensíveis*; Tutela legal.

---

[1] Doutor em Direito Comparado, pela Università Degli Studi di Firenze/Italia, Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo, graduado em Ciências Jurídicas e Sociais pela Universidade de Passo Fundo, licenciado em Estudos Sociais pela Universidade de Passo Fundo. Professor titular dos cursos de graduação, mestrado e doutorado em Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Professor e ex-Diretor da Escola Superior da Magistratura/AJURIS. Desembargador no Tribunal de Justiça/RS.

[2] Doutora e Mestre em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul. Atualmente, realizando pós-doutoramento na mesma Instituição, sob a Supervisão do primeiro autor, Prof. Dr. Eugênio Facchini Neto. Especialista em Direito Internacional Público, Privado e Direito da Integração pela Universidade Federal do Rio Grande do Sul. Assessora Jurídica no TJRS. Artigo realizado com apoio do CNPq – PDJ 406937/2017-6.

**Abstract:** This article aims to analyze the evolution of the concept of privacy, its transformation into the right to informational self-determination and its normative impacts. The advent of communication and information technologies has transformed contemporary society in many ways. One of them is the possibility of accessing, storing and systematizing data about each individual. This accumulation of information about someone means power, political and economic, due to the possibility of influencing behaviors. Thus, the privacy that initially meant the right to be let alone became the right to maintain control over one's own data, especially over sensitive data. Since the 1970s, with the primacy of Germany, several countries have begun to regulate this important aspect of contemporary societies. The European Union has recently replaced the 1995 Directive with a new and more comprehensive Regulation, which entered into force in May 2018. This Regulation, because of the careful preparation it has undergone, has the potential to influence the standards of non-EU countries, as is the case in Brazil, where currently the Congress debates important legislative systematization of the sector. This article will address this evolution of the idea of privacy, the concern with data control, making a brief analysis of the European Regulation and legislative proposals in Brazil. It is concluded that all efforts – legislative and hermeneutical – should be undertaken to ensure greater protection of informational self-determination, as this means, in the virtual world in which we live part of our lives, greater protection of the human person.

**Keywords:** Right to Privacy; Personal data; Sensitive Data; Legal protection?

## INTRODUÇÃO

No passado, o poder de uma nação era evidenciado pela sua expansão físico-territorial: quanto maior a área de dominação de um reino, mais poderoso era, pois maiores seriam as possibilidades de adquirir riquezas. Guerras, batalhas sangrentas, meses – quiçá anos – de lutas eram recompensadas com a ampliação de territórios, mediante a incorporação de pontos estratégicos que permitiam o acesso à matéria-prima, a produtos valiosos ou a ampliação do mercado para colocação de seus produtos, sem falar da apropriação de parte da riqueza material dos povos subjugados.

Alguns séculos se passaram desde a queda do último grande império da antiguidade, bem como ficou para trás a época dos impérios coloniais oitocentistas, que viram seus estertores em meados do século passado. Especialmente a partir do final da segunda guerra mundial, as grandes potências modernas já não mais precisam de grandes territórios para mostrar seu poderio. O poder – ao menos uma de suas importantes facetas – já não mais necessita de uma grande base física. Ele se encontra substancialmente desmaterializado, caracterizado pelo acesso e disponibilidade de *informações,* especialmente após o advento da *internet*. O poder passou a ser garantido pela dominação "virtual", essa conquistada pela guarda/armazenamento de dados pessoais coletados a partir da rede mundial de computadores (*internet*). O gerenciamento de informações permite influenciar condutas e lucrar com isso. Hoje, mais do que nunca, informação é poder.

De se notar que desde o advento da *internet* estamos vivendo uma era de transições constantes. As mudanças sucedem-se em velocidade frenética. Os avanços tecnológicos exigem contínua adaptação de nossos estilos de vida, que mudaram radicalmente desde a "revolução" das comunicações virtuais, via e-mails, messengers, redes sociais, celulares, torpedos etc. Os ganhos passaram a ser enormes, mas

os riscos cresceram na mesma proporção, impondo-se, assim, a necessidade de se levar mais a sério as ameaças a que nossa esfera de intimidade passou a estar exposta.

O acesso praticamente irrestrito e ilimitado à rede mundial de computadores fez surgir um novo nicho no mercado agora globalizado, caracterizado pela sua tendência de montagem de bancos de dados cada vez maiores (em quantidade e complexidade), com mapeamentos sem precedentes dos comportamentos individuais, principalmente para fins comerciais. E o lucro proveniente da comercialização de dados mostrou-se tão promissor e atraente que o mercado investiu pesadamente no desenvolvimento de novas tecnologias, mais amplas, criando poderosas ferramentas de classificação, triagem, seleção e controle de indivíduos. E o mais grave é que isso tudo vem acontecendo sem que os indivíduos tenham, em sua maioria, a menor noção de que estão sendo classificados/rotulados/analisados/influenciados e discriminados. Cruzamentos de dados permitem a identificação dos usuários da rede – e isso explica que já se tenha evidenciado que alguns produtos e serviços são oferecidos na rede virtual a preços diferenciados conforme o comprador use Mac ou um andróide, ou consoante seu local de residência.

Não é demais lembrar que os dois acontecimentos de natureza política e econômica mais relevantes dos últimos anos, a saber a eleição de Donald Trump para Presidente dos Estados Unidos da América, e o *BREXIT* (saída do Reino Unido da União Europeia) tiveram seus cursos definidos por empresa especializada na manipulação (ilícita) de dados pessoais, o que restou desvendado no que passou a ser conhecido como "*escândalo Facebook – Cambridge Analytica*"[3].

Estamos vivendo a era da *sociedade da informação*, frequentemente apontada como a quarta grande revolução, onde essa (a informação) assume um papel de bem econômico central, e, ao mesmo tempo, de pilar estruturante do desenvolvimento das relações sociais. Os termos são recorrentes: "*mercado de informação*"[4], "*eco-*

---

[3] ALVES, P. **Facebook e Cambridge Analytica**: sete fatos que você precisa saber:"*O escândalo veio à tona porque os jornais New York Times e The Guardian revelaram que a Cambridge Analytica obteve ilegalmente dados de cerca de 50 milhões de perfis de usuários do Facebook nos Estados Unidos. A informação surgiu a partir de uma entrevista com o ex-funcionário da empresa britânica Christopher Wylie. Os dados teriam sido usados para alimentar um sistema capaz de traçar um perfil psicográfico da população americana para usar na campanha de Donald Trump à presidência. O mecanismo teria permitido entender os traços comportamentais dos eleitores para oferecer-lhes propaganda política com mais chances de êxito. A publicidade foi distribuída no Facebook em forma de anúncios patrocinados no feed. As informações foram obtidas a partir de um teste de personalidade aparentemente inofensivo, disponibilizado gratuitamente aos usuários da rede social em 2014. Segundo o criador, o pesquisador Aleksandr Kogan, o seu método de análise aplicado ao teste era capaz de traçar o perfil de qualquer pessoa rapidamente a partir de informações como páginas curtidas e postagens realizadas na plataforma. O problema era que o teste obtinha dados não só de quem preenchia os formulários e aceitava as condições de uso, mas de toda a rede de contatos dos participantes. Mais tarde, Kogan teria entregado os dados à Cambridge Analytica. A empresa diz ter usado a base de dados para criar uma campanha digital hiper-segmentada para clientes como Trump. O vazamento de perfis teria ocorrido por conta de uma política flexível do Facebook com relação à entrega de informações de perfis a aplicativos de terceiros na rede social. Entre 2007 e 2014, a empresa de Mark Zuckerberg ofereceu livremente dados de usuários a desenvolvedores de apps*". Matéria publicada em: <https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml>, no dia 24.03.2018. Acesso em: 24 jun. 2018.
Após o impacto inicial, surgiram novos rumores de que a empresa Cambridge Analytica teria atuado também em outros "mercados políticos" mundo afora, inclusive na vizinha Argentina (o que ainda não foi confirmado oficialmente).

[4] RODRIGUES, J. **Regulação, Ética e Governance**. Lisboa: RH, 2018.

*nomia da informação*"[5], "*capital-informação*"[6], dentre outros tantos, e servem para designar esse novo paradigma tecno-econômico que alçou a *informação* ao status de *meio dominante para o tráfego econômico*[7].

Todas essas mudanças tecnológicas obviamente alteram a fronteira entre o público e o privado, esfumaçam a distinção entre a praça e o quintal. Antigas e respeitadas demarcações (a esfera do público/político, regida pelo princípio da transparência e da igualdade; a esfera do social-privado, regida pelo princípio da diferenciação; a esfera da intimidade, regida pelo princípio da exclusividade) passaram a ser repensadas.

Esse repensamento atinge mais profunda e diretamente a noção de privacidade. Após o "11 de setembro" a privacidade passou a ser vista como verdadeiro empecilho/obstáculo à segurança pública, o que fortaleceu o discurso (cada vez mais forte, e a cada dia com mais adeptos) de que sua importância no contexto dos direitos fundamentais diminuiu sobremaneira, de sorte que deve ceder sempre que estiver em colisão com outros princípios e garantias fundamentais. Rodotá adverte, inclusive, que há quem sustente que a privacidade perdeu, nessa "era do terror", seu status de direito fundamental, sendo facilmente superada por "*legislações de emergência*"[8].

Não é demais lembrar que paralelamente ao mercado, o poder público também passou a investir pesadamente no desenvolvimento de tecnologias capazes de aprofundar ainda mais o conhecimento e o controle sobre cada indivíduo, especialmente para "vigiá-lo" constantemente e, com isso, talvez evitar novos ataques terroristas e/ou crimes de qualquer espécie. Passou, assim, a fomentar pesquisas sobre "digitais cerebrais", com o intuito de "mapear a memória" dos indivíduos, de sorte a buscar em seu inconsciente registros de fatos pretéritos e indícios de que tenham deles participado (leia-se, invadir a sua privacidade e, em maior intensidade, a sua dimensão mais íntima – e que deveria ser inviolável), tudo sob o pretexto de garantir a segurança da coletividade[9].

Além das pesquisas destinadas ao setor de segurança, os Estados também investiram fortemente na criação de bancos de dados e no cruzamento de informações para rastrear cada vez mais os cidadãos, permitindo identificar o seu comportamento

---

5 STIGLITZ, J. E. Economics of Information and the Theory of Economic Development, **Revista de Econometria**, v. 5, n. 1, p. 5-32, abr. 1985.

6 DANTAS, M. "**Capital-informação" e virtualização financeira**: isso ainda é capitalismo? Disponível em: <http://gindre.com.br/capital-informacao-e-virtualizacao-financeira-isso-ainda-e-capitalismo/>. Acesso em: 28 jun. 2018

7 BIONI, B. R. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. Projeto de Pesquisa Privacidade e Vigilância. Disponível em: <http://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em: 26 jun. 2018.

8 RODOTÁ, Stefano. **A vida da sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 14.

9 Nos Estados Unidos, as inovações ficaram por conta das restrições impostas à privacidade. Amitai Etzioni (**How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism**. New York-London: Routledge, 2004) analisa os efeitos do *Patriot Act*, lei norte-americana editada como parte da resposta ao atentado terrorista de 11 de setembro de 2001, estabelecendo severas restrições ao direito à privacidade das pessoas e suas comunicações. O fato é que do *Patriot Act* norte-americano à Diretiva comunitária sobre comunicações eletrônicas, de 2006, passando pelo acordo firmado entre os Estados Unidos e a União Europeia, em julho de 2007, sobre o denominado regime PNR (*Passenger Name Record*), toda uma legislação mais recente vem restringindo o âmbito das garantias relativas à privacidade e ao controle dos dados pessoais na esfera pública.

enquanto consumidor e, assim, traçar políticas e estratégias de arrecadação de impostos (*vide* os programas "notas fiscais").

E embora não se possa discordar do princípio regulador contido no art. 8 da Convenção Europeia dos Direitos do Homem, segundo o qual a tutela da *privacy* deve levar em conta as exigências da defesa nacional e pública, o fato é que, nas mãos de determinados agentes de segurança, tal ponderação entre interesses igualmente tutelados pode ser desvirtuada por um enfoque que, em nome da segurança nacional, toleraria abusos os mais diversos.

Segundo o *Cisco Visual Networking Index: global mobile data traffic forecast update, 2016-2021*[10], publicado em março de 2017, o tráfego mundial de dados móveis alcançará em 2021 a casa de 49 *Exabytes* mensais (587 *exabytes* anuais). Esses 587 *exabytes* anuais equivalem a mais de 122 vezes todo o tráfego mundial de dados móveis gerado em 10 anos (de 2011 a 2021), e 131 bilhões de imagens (como mms ou instagram). Para se ter uma ideia e traçar um breve paralelo, em 2006 estimava-se que o armazenamento de dados pessoais estava na casa de 161 milhões de *gigabytes* (unidade muitíssimo menor). O crescimento é vertiginoso e assustador. Se considerarmos a quantidade de dados pessoais armazenados, por sistemas de *data mining* que permitem delinear o perfil de um indivíduo qualquer, a partir do cruzamento de informações aparentemente triviais ou insignificantes, já que praticamente todas as nossas relações comerciais, atividades sociais e culturais são registradas em banco de dados, assim como nossa movimentação física é captada por aplicativos instalados nos celulares que carregamos permanentemente conosco, perceberemos os riscos a que estamos expostos.

Esse ensaio procura analisar, inicialmente, a evolução da proteção da privacidade, a mutação do seu conceito, bem como as formas legais que se tem procurado estabelecer para proteção do seu núcleo, na sociedade da comunicação e informação em que vivemos. Para tanto, faremos uma breve análise da recente normativa europeia de proteção de dados, bem como o atual debate legislativo sobre o tema, no Brasil.

## 1 DIREITO À PRIVACIDADE: EVOLUÇÃO HISTÓRICA E APROXIMAÇÕES CONCEITUAIS.

De certa forma, pode-se dizer que a liberdade está para o direito público como a autonomia privada está para o direito privado, ou seja, a possibilidade do indivíduo escolher como deseja viver, quais as metas que pretende elencar, com quem quer se associar, em que causas quer participar, que profissão ou atividade deseja empreender. E é esse conceito de autonomia privada que está na raiz da proteção dos direitos de personalidade.

Uma certa leitura constitucional permite identificar a noção de autonomia privada no vocábulo *vida privada*, que o constituinte tem como inviolável no art. 5º, inc. X, da Constituição Federal ("*São invioláveis a intimidade, a vida privada, a*

[10] Cisco Visual Neworking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?CAMPAIGN=Mobile+VNI+2017&COUNTRY_SITE=us&POSITION=Press+Release&REFERRING_SITE=PR&CREATIVE=PR+to+MVNI+white+paper>. Acesso em: 29 jun. 2018.

*honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*"). Vida privada, aqui, comparece como o direito do indivíduo de desenvolver livremente sua personalidade, sem ser direcionado ou influenciado pelo Estado, pela sociedade, pela Igreja ou pela família. Diversa é a noção de *intimidade*, igualmente tido como inviolável no mesmo dispositivo constitucional. Trata-se, aqui, daquela noção que Hannah Arendt, na sua **A condição humana**, afirmou estar regida pelo princípio da exclusividade, ou seja, do direito do indivíduo criar para si um círculo abrangendo o que lhe é próprio, dele excluindo terceiros. Tal noção implicaria três atributos principais – o direito de estar só e de ser deixado só (noção clássica de privacidade), o sigilo ou segredo, e a autonomia, ou seja, a liberdade de decidir sobre todas as coisas que lhe dizem respeito, sem qualquer condicionamento ou influência, seja do Estado ou da sociedade.

Os primeiros a publicar estudo sobre a *privacy* – Warren e Brandeis, em 1890 (The Right to Privacy)[11], – entendiam-na como um direito à "não intrusão", ou seja, o direito a não ser perturbado ou o direito a ser deixado só – *the right to be let alone.* Essa ideia fundamenta, por exemplo, o conhecido caso *Eisenstadt v. Baird*, julgado em 1972 pela Suprema Corte norte-americana, pela pena do *Justice* William Brennan. Para ele, a *privacy* consistiria "no direito do indivíduo de estar livre de intrusões públicas (*government*) não autorizadas", de sorte que a privacidade passou a revelar-se como um importante instrumento para garantir o próprio exercício da liberdade.

Para Rodotá, aqui surgiu um aparente paradoxo, pois "*a forte proteção da esfera privada em última instância não resguarda a privacidade nem a mantém protegida do olhar indesejável; na verdade, permite que crenças e opiniões individuais sejam tornadas públicas livremente. Isto abriu o caminho para aproximar ainda mais a associação entre privacidade e liberdade*"[12].

Posteriormente, uma segunda noção de *privacy* passou a identificá-la como possibilidade de **exclusão**, ou seja, o direito de excluir outros de nossa vida, e consequentemente de vivermos isolados, se o desejarmos, em paz e tranqüilidade (noção que, como vimos, remonta a H. Arendt).

Outros autores, como Ruth Gavison[13], William A. Parent[14] e Anita Allen[15], passaram a definir *privacy* como **limitação**[16]. Seria a zona em que o acesso à informação pessoal poderia ser limitado ou restringido. A *privacy* perfeita ocorreria quando ninguém tivesse informações sobre um sujeito determinado.

Reagindo a essa última concepção, Charles Fried lançou a ideia de *privacy* como **controle**, segundo a qual a *privacy* não seria a simples ausência de informa-

---

11 BRANDEIS, Louis. WARREN, Samuel. The Right to Privacy. **Harvard Law Review**, v. IV, December 15, 1980, n. 5. Artigo, na sua versão eletrônica. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 30 maio 2017.

12 RODOTÁ, Stefano. **A vida da sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 16.

13 GAVISON, Ruth. Privacy and the Limits of the Law. **Yale Law Journal**, 1980, 89.

14 PARENT, William A. Privacy, Morality and the Law. **Philosophy and Public Affairs**, 1983, 12, 4.

15 ALLEN, Anita. **Uneasy Access**: Privacy for Women in a Free Society. Totowa/NJ: Rowman and Littlefield, 1988.

16 *Apud* FACCHINI NETO, Eugênio. Prefácio da obra **Direitos da Personalidade**: disponibilidade relativa, autonomia privada e dignidade humana, de autoria de Fernanda Borghetti Cantalli. Porto Alegre: Livraria do Advogado, 2009.

ções sobre nós, por parte dos outros, mas sim o controle sobre a informação que temos sobre nós mesmos[17].

Depois de referir também as concepções de *privacy* como algo que ficaria **entre acesso restrito** e **controle limitado**, ou *privacy* como **informação**, discorrendo também sobre a tese **negacionista**, Ugo Pagallo[18], acentua a dificuldade de se chegar a um consenso universal sobre o significado de *privacy*, em razão do fenômeno do *multiculturalismo*. Refere ele a inexistência de enfoques semelhantes sobre o significado, realidade, extensão e importância da *privacy* em culturas distintas como a norte-americana, europeia, chinesa, japonesa e islâmica.

WESTIN, na mesma linha dos anteriores, passou a sustentar que a privacidade incorporou ***o direito a controlar a maneira pela qual os outros utilizam as informações a nosso respeito***; Friedman, igualmente, passou a defini-la como ***proteção de escolhas de vida contra qualquer forma de controle público e estigma social***; no mesmo sentido, Rosen aduziu que a privacidade deve ser vista como a ***reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto***. Por fim, Rodotá sugeriu que a privacidade venha a ser compreendida também como "***o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular***"[19].

Ao lado do trabalho teórico/doutrinário, jurisprudência e legislação também passaram a tratar o direito à privacidade de forma diferenciada.

Na casuística internacional, inúmeros são os precedentes envolvendo a proteção da *privacy*, de capital importância não só jurídica, como também social, diante de seu reflexo na vida dos cidadãos. Na jurisprudência da Suprema Corte norte-americana, são emblemáticos os casos *Griswold v. Connecticut* (1965), *Eisenstadt v. Baird* (1972), *Roe v. Wade* (1973), *Carey v. Population Services Int'l* (1977), *Planned Parenthood of Southeastern Pennsylvania v. Casey* (1992), *Whole Woman's Health v. Hellerstedt* (2016), sobre *privacy* como conceito amplo, envolvendo o direito do casal de decidir sobre planejamento familiar e métodos anticonceptivos; o caso *Katz v. United States* (1967), sobre expectativa de privacy a ser garantida contra gravações clandestinas, embora em espaços públicos, o caso *Lawrence v. Texas* (2003), sobre *privacy* sexual.

Numa escala global, percebe-se que a partir dos anos 60, com a aceleração do desenvolvimento tecnológico, e com a possibilidade inaugurada com a revolução informática de se recolher e agrupar dados pessoais, houve uma ampliação do conceito de privacidade, para envolver também a proteção aos dados e informações pessoais.

Segundo Rodotá, as ideias sobre privacidade evoluíram no sentido de que se passou do direito a ser deixado só ao direito de ter sob controle as informações que nos dizem respeito; da privacidade ao direito à autodeterminação informativa; da privacidade à não discriminação; do sigilo ao controle.

---

17 FRIED, Charles. Privacy: A Rational Context. *In*: **Computers, Ethics, and Society** (org. por M. D. Ermann, M.B.. Williams e C Gutierrez. New York: Oxford University Press, 1990, p. 54).

18 PAGALLO, Ugo. **La tutela della privacy negli Stati Uniti d'America e in Europa – Modelli giuridici a confronto**. Milano: Giuffrè, 2008.

19 RODOTÁ, Stefano. *Op. cit*., p. 15.

Entre nós, Doneda refere que nossos dados, devidamente sistematizados e aglutinados, significam nossa representação virtual. Quem tem acesso a eles pode decidir sobre conceder ou não um crédito, celebrar ou não um plano de saúde, conceder ou não uma vaga de emprego, e, se for um governo, autorizar ou não a entrada de alguém em seu país. Não por acaso vem se chamando a essa nossa representação virtual de "corpo eletrônico", "avatar eletrônico", "data shadow". Enfim, chega-se quase à conclusão de que "somos o que o google diz que somos": nossa biografia passa a ser definida pelo famoso algoritmo daquela multinacional.

Yuval Harari, em seu último livro – **Homo Deus** – discorreu sobre a possibilidade de manipulação de sentimentos através do conhecimento de dados sobre alguém. Ou seja, quem acumula e sistematiza dados sobre alguém, tem condições de enviar mensagens sabendo que elas terão o poder de fazer aflorar sentimentos previamente identificados, através dos dados conhecidos. Explicou também como os mecanismos de Inteligência Artificial, pela reunião e sistematização de um infinito número de dados dispersos, a ponto de revelar padrões de comportamento, são capazes de nos conhecer melhor do que nós mesmos.

Reagindo a essa situação, observa-se que na sociedade europeia, para além da previsão tradicional da proteção à privacidade em sua concepção clássica/original, a Carta da União Europeia 'inovou' ao incluir o direito à proteção de dados, **alçando-o à categoria de direito fundamental autônomo**. É o que se depreende da leitura conjugada dos arts. 3º (direito à integridade da pessoa, isto é, proteção do "corpo físico"), 7º (direito de respeito da vida privada e familiar – concepção 'clássica' da privacidade), e art. 8º (direito à proteção de dados, ou seja, do "corpo eletrônico")[20].

Não obstante a sua previsão normativa – o que é um avanço e um marco histórico – a sociedade europeia ainda se defronta com os limites conceituais e com as dificuldades de aplicação imediata e ampla de tais preceitos, estando em constante debate para aprimoramento de seu sistema, tanto que recentemente implementou o novo regulamento de proteção de dados pessoais (GDRP), sobre o qual falaremos mais adiante.

O que se quer, enfim, é garantir a todos os benefícios da sociedade da comunicação e informação em que inexoravelmente vivemos, impedindo, porém, os abusos na manipulação de pessoas. Este é o grande desafio contemporâneo.

---

[20] CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. "***Art. 3º. Direito à integridade do ser humano***: *1. Todas as pessoas têm direito ao respeito pela sua integridade física e mental. 2. No domínio da medicina e da biologia, devem ser respeitados, designadamente: – o consentimento livre e esclarecido da pessoa, nos termos da lei, – a proibição das práticas eugênicas, nomeadamente das que têm por finalidade a seleção das pessoas, – a proibição de transformar o corpo humano ou as suas partes, enquanto tais, numa fonte de lucro, – a proibição da clonagem reprodutiva dos seres humanos. (...)* ***Art. 7º. 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.* ***Art. 8º. 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 respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente*". Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv%3Al33501>. Acesso em: 30 maio 2017.

## 2 DADOS PESSOAIS, DADOS SENSÍVEIS E A NECESSIDADE DE APRIMORAMENTO CONSTANTE DE SUA TUTELA LEGAL

Não há dúvidas de que "*todos somos 'titulares de datos personales', nuestros datos son tratados cotidianamente por el sector público y privado, a veces con nuestro conocimiento, otras no tanto*"[21].

Todavia, dentre os dados que são armazenados, alguns tem mais relevância do que outros, o que nos remete para a definição do que seriam dados pessoais – e, dentre eles, quais seriam os dados sensíveis. Haveria um "rol taxativo" que valeria para, senão todos, grande parte dos ordenamentos jurídicos? Haveria alguma flexibilidade de inclusão ou exclusão de alguma informação a depender do contexto em que armazenada, utilizada, comercializada etc.? Ou uma vez considerada "dado pessoal" e "dado sensível" essa informação estaria blindada e não poderia ser utilizada para nenhum fim sem a autorização de seu titular?

Os legisladores de todo o mundo vêm se debruçado sobre o tema, especialmente a partir da década de 1960, época em que foram criados projetos governamentais como os do National Data Center[22] ou o SAFARI[23].

---

[21] POULLET, Y.; ASINARI, M. V. P.; PALAZZI, P. A. **Derecho a la indimidad y protección de datos personales**. Buenos Aires: Heliasta, 2009. p. 11.

[22] A ideia de formar um centro de dados nacional (*National Data Center)* surgiu na década de 1960, quando cientistas sociais norte-americanos sentiram a necessidade de obter maior acesso a microdados mantidos pelo governo federal. Como resultado, em 1965, recomendaram que o governo federal desenvolvesse um *Data Center* nacional que armazenasse e disponibilizasse aos pesquisadores os dados coletados por várias agências estatísticas, recomendação feita através de relatório do Comitê sobre a Preservação e Uso de Dados Econômicos para o Conselho de Pesquisa em Ciências Sociais, conhecido como "Relatório Ruggles". Nesse documento, o Comitê discutiu dados econômicos criados pelo governo federal e os papéis e responsabilidades das agências federais e instituições de pesquisa na preservação e uso de dados econômicos. Ruggles apareceria no ano seguinte (1966) para discutir as descobertas do comitê em uma audiência do Congresso intitulada "O computador e a invasão da privacidade". O endosso do governo à proposta do centro nacional de dados levou a protestos públicos e a um intenso escrutínio do Congresso sobre o potencial uso indevido dos dados coletados pelo Governo e ameaças à privacidade representadas por tecnologias emergentes. Embora a comunidade de pesquisa e o governo entendessem os benefícios potenciais de um data center nacional e concordassem que os dados seriam usados apenas para pesquisa, uma parte significativa do público parecia não compartilhar seu entusiasmo por um data center nacional. Medos de "Big Brother" e dossiês secretos do governo giraram em torno das discussões do data center nacional, culminando na aprovação da Lei de Privacidade de 1974 (*Privacy Act). Vide*, sobretudo: KRAUS, R. S. Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants. Disponível em: <https://www.census.gov/history/pdf/kraus-natdatacenter.pdf>. Acesso em: 29 jun. 2018. E também: RUGGLES, R. *et al*. **Report of the Committee on the Preservation and Use of Economic Data (1965)**. Disponível em: <https://ia800200.us.archive.org/31/items/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965/Ruggles_econdata_1965.pdf>. Acesso em: 29 jun. 2018.

[23] SAFARI, sigla de sistema automatizado para arquivos administrativos e o diretório de indivíduos (**Système automatisé pour les fichiers administratifs et le répertoire des individus)**, foi criado em 1974, na França, com o mesmo intento do *National Data Center* norte-americano. O sistema envolvia a criação de um banco de dados centralizado da população, usando o arquivo da previdência social como o identificador comum de todos os arquivos administrativos. Confrontado com o clamor generalizado provocado por este projeto, o jornal *Le Monde* publicou matéria intitulada "SAFARI, ou caça aos franceses". Isso levou a uma forte oposição popular, levando o governo a criar a Comissão Nacional de Informática e Liberdades. O projeto SAFARI, lançado durante a presidência de Georges Pompidou, não viu a luz do dia. *Vide*, sobretudo: Safari, la chasse aux Français 40 ans après. Disponível em: <https://donneesouvertes.info/2018/01/26/safari-la-chasse-aux-francais-40-ans-apres/>. Acesso em: 29 jun. 2018.

A doutrina também se dedicou ao tema. Segundo Doneda, "*o paradigma inicial para uma reflexão doutrinária partiu justamente da reação a estes projetos, para logo depois fundamentar as primeiras iniciativas legislativas na matéria*"[24]. A primeira obra de impacto sobre o tema foi Privacy and Freedom, de Alan WESTIN, publicada originariamente em 1967. Nela, o autor mudou o enfoque até então conferido à privacidade, propondo uma nova concepção, desta feita baseada na "autodeterminação informativa", noção posteriormente acolhida pela Corte Constitucional alemã.

Vale tecer um breve escorço histórico: as primeiras normas visando a tutela de dados pessoais surgiram na década de 1970 e são classificadas pela doutrina[25] como sendo a "**primeira geração**" de leis de proteção de dados. São elas: a Hessisches Datenschutzgesetz (Lei de Proteção de Dados Hessiana), em 1970; a Data Legen 289 (ou Datalag), em 1973, na Suécia; e o Privacy Atc nos Estados Unidos da América, em 1974[26].

Essas normas tinham em comum o forte receio de que os direitos e liberdades fundamentais pudessem ser solapados pela coleta ilimitada e uso indiscriminado de dados pessoais, atividade que até então se restringia basicamente ao Estado. Por isso, considerando a pouca experiência no tratamento daquelas que se apresentavam como novas tecnologias (os computadores recém estavam surgindo, e nem se imaginava o posterior boom da internet), seus criadores optaram por adotar princípios gerais de proteção, amplos e abstratos, focalizados essencialmente na atividade do processamento de dados em si, e não na privacidade dos titulares dos dados[27].

A "primeira geração" de leis de proteção de dados segue aproximadamente até o advento da Lei Federal sobre Proteção de Dados (*Bundesdatenschutzgesetz*), da República Federativa da Alemanha, em 1977, valendo observar que se tornaram obsoletas rapidamente, seja pelo próprio avanço da tecnologia, seja pela multiplicação dos centros de processamentos de dados, o que tornou "*virtualmente ineficaz um controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento*"[28].

A "**segunda geração**" dessas leis de proteção de dados, por assim dizer, surge no final da própria década de 1970, mais precisamente com a lei francesa de 1978, denominada de Loi relative à l´informatique, aux fichiers et aux libertés [29]. A grande diferença com as normas da geração anterior é que o enfoque passou a ser não mais o "fenômeno computacional em si", mas a proteção da privacidade e dos dados pessoais dos seus titulares, assim considerados **como reflexo de uma liberdade negativa**, exercida pelo próprio cidadão. Criou-se um sistema que fornecia

---

[24] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 205.

[25] Veja-se, sobretudo: RODOTÁ, S. **Tecnologie e diritti**. Bologna: Il Mulino, 1995; MAYER-SCHÖNEMBERGER. V. General development of data protection in Europe. *In*: AGRE, P.; ROTEMBERG, M. (Orgs.). **Technology and Privacy**: the new landscape. Cambridge: MIT Press, 1997. p. 219-242.

[26] DONEDA, *op. cit*., p. 208.

[27] SIMITIS, S. Il contesto giuridico e politico della tutela della privacy. **Rivista Critica del Diritto Privato**, p. 565 e ss., 1997.

[28] DONEDA, *op. loc. cit.*, p. 209.

[29] FRANCE. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>. Acesso em: 26 jun. 2018.

instrumentos ao indivíduo para que esse identificasse o uso indevido de suas informações pessoais, e propusesse a tutela. A mesma abordagem foi adotada pela Lei Austríaca (*Datenschutzgesetz*), igualmente de 1978. Semelhante enfoque se encontra em disposições sobre o tema nas Constituições Portuguesa e Espanhola.

Ocorre que mais uma vez o avanço tecnológico ocasionou o atrofiamento das referidas leis. Isso porque o fornecimento de dados pessoais pelos cidadãos passou a ser um requisito praticamente indispensável para a participação na vida em sociedade, sendo constantemente solicitados tanto por entes públicos, quanto por entes privados para possibilitar o desenvolvimento de atividades (das mais variadas) e/ou a realização de negócios. O indivíduo que não quisesse fornecer seus dados praticamente restaria alijado da sociedade, como um ermitão[30].

Abriu-se espaço, então, para uma "**terceira geração**" de normas, isso já na década de 1980, que teve como marco principal a decisão do Tribunal Constitucional Alemão no caso em que reconheceu a inconstitucionalidade da Lei do Censo, aprovada em 1982, frente aos arts. 1.1 e 2.1 da Lei Fundamental (base sobre a qual se estrutura o direito geral da personalidade)[31].

Nas palavras de Doneda, essa terceira geração de leis

> *sofistica a tutela dos dados pessoais, que continua sendo concentrada no cidadão, porém passa a abranger mais do que a liberdade de fornecer ou não os seus dados pessoais, preocupando-se em garantir a efetividade dessa liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – e assim proporcionando o efetivo e pleno exercício da autodeterminação informativa*[32].

Essas leis colocavam a participação do indivíduo como verdadeira mola propulsora, assumindo ele (ou devendo assumir) o papel de protagonista na defesa e proteção de seus dados pessoais. Contudo, a prática revelou que a grande maioria não estava disposta a exercitar a prerrogativa de autodeterminação informativa, preferindo muitas vezes concordar com situações que não eram as ideais em razão

---

30 MAYER-SCHÖNBERGER, V. *Op. cit.*, p. 229.

31 A referida lei previa que cada cidadão deveria responder a um questionário de 160 perguntas, cujas respostas eram posteriormente submetidas a tratamento informatizado, gerando grande desconfiança na população. Isso, porque previa a possibilidade de que os dados obtidos pelo censo fossem confrontados com os dados do registro civil para eventual retificação do próprio registro; a possibilidade de esses mesmos dados virem a ser transmitidos às autoridades federais e aos *Länder*; a existência de uma multa pecuniária relativamente alta para quem não respondesse ao censo, e, paralelamente, a existência de mecanismos para favorecer aqueles que denunciassem tais pessoas. Ao reconhecer a profunda incompatibilidade entre a Lei do Censo e a Lei Fundamental, o Tribunal acabou por "fixar" algumas diretrizes, a saber: (i) a necessidade de se observar o princípio da finalidade na coleta de dados pessoais (se o dado é coletado para um fim, no caso o estatístico/censo, não pode ser utilizado para outro, no caso, para fins administrativos visando eventual correção de registro civil, por exemplo); (ii) não existem dados "sem importância" e/ou irrelevantes para a privacidade (um dado que 'solto' aparentemente não significa nada, no âmbito da finalidade para a qual foi solicitado pode significar muito); (iii) a autodeterminação informativa (consistente no direito que os indivíduos têm de controlar as suas próprias informações, podendo decidir quando e dentro de que limites os seus dados pessoais podem ser utilizados); (iv) a proibição de transferência de dados pessoais entre autoridades federais e regionais etc.

32 DONEDA, *op. cit.*, p. 210.

do custo econômico e/ou social, o que fez os legisladores pensar em novas proposições.

Surgiram, então, as leis de "**quarta geração**" em matéria de proteção de dados, caracterizando-se pela instituição de mecanismos coletivos de proteção, buscando resultados mais concretos e evidentes. Entre as técnicas utilizadas por essas leis, destaca-se a intenção de fortalecer a posição da pessoa em relação às entidades que coletam e processam os seus dados – o que não havia sido resolvido com as medidas que se limitavam a reconhecer o direito à autodeterminação informativa; e também, a redução do papel da decisão individual na autodeterminação informativa[33].

Nessa geração se inserem as normas trazidas pela Carta dos Direitos Fundamentais da União Europeia, já referidas anteriormente, bem como a Diretiva 95/46/EC, que tratou especificamente da proteção de dados pessoais.

Sem incorrer no equívoco da "Convenção para Proteção dos Indivíduos com Respeito ao Processamento Automático de Dados Pessoais" que havia entrado em vigor em 1985, seguindo a mesma linha das "Diretrizes sobre proteção da privacidade e o fluxo transnacional de informações pessoais" publicada pela OECD no início dos anos 1980, a Diretiva 95/46/EC trouxe no seu art. 2º uma série de conceitos[34] e princípios. Abordaremos apenas as normas referentes aos *dados pessoais*, considerando os limites desse ensaio.

Pois bem, consta no art. 2º, a da referida Diretiva que *dado pessoal* é "*qualquer informação relativa a uma pessoa singular* ***identificada ou identificável***", o que nos permite concluir que alcança, claramente, não somente informações textuais, mas também fotografias, imagens audiovisuais, registros de sons e tudo o mais que puder identificar uma pessoa, estando ela viva ou não, sem que se retire desses aspectos as suas características de direitos autônomos também.

O conceito de dado pessoal é considerado chave, pois ao fim e ao cabo, determinará o que será objeto de uma lei de proteção de dados e o que não será. "*Diferenças sutis em torno de sua definição implicam em consequências drásticas para o alcance dessa proteção*"[35]. Ele é composto por palavras que poderão restringir (concepção reducionista) ou alargar (concepção expansionista) o espectro dessa proteção dos dados pessoais. Para Schwartz e Solove, Estados Unidos (reducionista) e Europa

---

33 *Idem*, *op. cit*., p. 212.

34 Outros conceitos importantes trazidos pela Diretiva 95/46 da então Comunidade Europeia são: o de processamento de dados pessoais, que consiste em "*qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a coleta, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição*" (art. 2º, b); o de controlador dos dados ou pessoa responsável pelo tratamento , que consiste na "*a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais*" (art. 2º, d); de "fichário de dados pessoais", de "subcontratante", de "terceiro", de "destinatário" e de "consentimento do sujeito dos dados" (art. 2º, "c", "e", "f", "g" e "h"). *Vide*: REINALDO FILHO, D. **A Diretiva Europeia sobre proteção de dados pessoais**: uma análise de seus aspectos gerais, fev. 2013. Disponível em: <https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais>. Acesso em: 26 jun. 2018.

35 BIONI, B. R. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. Projeto de Pesquisa Privacidade e Vigilância. Disponível em: <http://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_inicia tivas_legislativas_no_Brasil>. Acesso em: 26 jun. 2018.

(expansionista) são bons exemplos dessas concepções, embora ambas apresentem falhas[36].

A concepção reducionista parte de uma premissa restritiva através da qual o "dado pessoal" consiste em uma informação que deve estar associada direta e imediatamente a uma pessoa específica, isto é, aquela informação capaz de identificar a pessoa de forma precisa e inequívoca (pessoa identificada). Essa, por sinal, foi a definição adotada no texto original do Projeto de Lei 4.060/2012, da Câmara do Deputados do Brasil, e sobre o qual voltaremos a falar mais adiante. Já a concepção expansionista parte de uma premissa mais ampla e flexível, considerando 'dado pessoal' qualquer informação que permita a identificação de seu titular, ainda que não de imediato, mas de forma indireta e mediata (pessoa identificável).

De qualquer sorte, ainda que divergentes, ambas as correntes reclamam uma análise contextual de onde está inserido um dado, a fim de aferir-se o seu grau de identificabilidade, para somente então possibilitar a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou a uma pessoa identificável.

Essa Diretiva 95/46/EC foi substituída, recentemente, pelo novo regulamento geral de proteção de dados – GDPR – o que nos permite concluir que uma "**quinta geração**" de leis de proteção de dados está emergindo. É dela que passaremos a tratar.

## 3 BREVES CONSIDERAÇÕES SOBRE O NOVO *GENERAL DATA PROTECTION REGULATION* (GDPR) EUROPEU.

Como ocorreu com as leis integrantes das gerações anteriores, a Diretiva 95/46/EC acabou se tornando insuficiente para garantir a proteção dos dados dos cidadãos europeus em face do progresso tecnológico havido ao longo desses 20 (vinte) anos desde a sua entrada em vigor.

Inúmeros fatos demonstraram ao Parlamento e ao Conselho Europeus a necessidade de alteração da legislação com a adoção de regras mais rígidas para regulamentar a proteção dos dados pessoais de seus cidadãos. Dentre eles destacamos o *caso Yahoo*, ocorrido em 2013, consubstanciado na violação de contas com roubo de dados pessoais de cerca de 500 milhões de usuários (informação dada à época e que posteriormente verificou-se ser bem pior, pois cerca de 3 bilhões de pessoas foram atingidas)[37]; e o *caso Snowden*, também ocorrido/desencadeado no ano de 2013, em que o ex-agente da CIA revelou ao mundo detalhes de alguns programas de vigilância utilizados pelo Governo americano para espionar não apenas a população de seu país, mas também a de vários outros países, inclusive de seus presidentes, chanceleres, e autoridades. Mereceria também alusão o julgamento, pela Corte de Justiça da União Europeia, em 2014, do caso *Google Spain,* que chamou a atenção de todos para o problema do chamado *direito ao esquecimento.*

---

[36] SCHWARTZ, P. M. SOLOVE, D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *In*: **Berkeley Law Scholarship Repository**, 01.01.2011. Disponível em: <https://scholarship.law.berkeley.edu/facpubs/1638/>. Acesso em: 26 jun. 2018.

[37] AGÊNCIA EFE. Roubo de dados sofrido pelo Yahoo em 2013 foi 3 vezes maior do que o anunciado – três bilhões de contas foram afetadas. Matéria publicada em 04.10.2017. Disponível em: <ahttps://epocanegocios.globo.com/Tecnologia/noticia/2017/10/roubo-de-dados-sofrido-pelo-yahoo-em-2013-foi-3-vezes-maior-que-o-anunciado.html>. Acesso em: 26 jun. 2018.

Assim, em 27 de abril de 2016, o Parlamento Europeu e o Conselho Europeu emitiram o Regulamento (UE) 2016/679 relativo *à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, revogando a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Nas palavras de Franco Pizzetti "*la differenza 'sistemica' tra Direttiva e Regolamento*" é que houve um deslocamento de 'enfoque', por assim dizer, que passou "*dalla tutela del diritto fondamentale della persona alla tutela dei dati personali come interesse pubblico europeo*"[38].

O denominado de *GDPR – General Data Protection Regulation* – entrou em vigor apenas em 25 de maio do corrente ano de 2018, por conta do tempo dado aos países membros para se adequarem às novas regras, e já está causando "alvoroço" no mercado tecnológico (há notícias de que as gigantes Google, e seus "braços" Facebook e Instagram, e WhatsApp já estão sofrendo processos "bilionários" por descumprimento das novas regras – a denúncia é de que estariam "coagindo" os usuários a aceitarem as suas políticas de coletas de dados).

Vale destacar as principais inovações trazidas por este importante Regulamento, que, ao fim e ao cabo, não afetará apenas a Comunidade Europeia, mas também todos os países, todas as empresas e/ou pessoas que quiserem prestar algum tipo de serviço a cidadãos de qualquer um dos países do bloco.

Pois bem. Já de início, no art. 3º – destinado às definições – o GRPD inova ao expandir a concepção anterior prevista na Diretiva 95/46/CE, acrescentando outras expressões/definições que não estavam na primeira ('*limitação do tratamento'*, '*definição de perfis*', '*pseudonimização*', '*violação de dados pessoais*', '*dados genéticos*', '*dados biométricos*', '*dados relativos à saúde*', '*autoridade de controle*' e '*organização internacional'*); assim como acrescentando outros significados/conteúdo à grande parte dos já existentes (como é o caso da própria definição de *dados pessoais*, de *autoridade*, de *responsável pelo tratamento*, de *destinatários*, para exemplificar). Acerca dos *dados pessoais*", o GDPR assim dispõe:

> *Dados pessoais: informações relativas a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular*[39].

Também digno de destaque é o disposto no art. 10º – que se refere ao tratamento de categorias especiais de dados pessoais, isto é, aos chamados *dados sensíveis*:

> *O tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, o tratamento de dados genéticos, dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou à orientação sexual, só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se:*

[38] PIZZETTI, F. I **Diritti nella 'rete' della Rete – Privacy e il Diritto Europeo alla Protezione dei Dati Personali**: il Regolamento europeo 2016/679. Torino: Giappichelli, 2016. p. 4.

[39] Regulamento (UE) 2016/679, de 27 de abril de 2016. **General Data Protection Regulation**, art. 3°, "1".

*a. For autorizado pelo direito da União ou de um Estado-Membro;*
*b. Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou*
*c. Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.*

No que tange ao *consentimento*, o novo regulamento também traz alterações significativas. Pela regra anterior, o consentimento deveria ser "livre, específico e informado", reclamando um ato formal para o processamento de dados. Agora, o consentimento deverá ser "*livre, específico, informado* ***e inequívoco***". Ou seja, o consentimento só é válido se a vontade for expressa de maneira não equívoca, não dúbia. Para Califano a introdução desse último adjetivo consiste em uma "*significative novità, novità la cui portata non resulta sempre imediatamente percepibile, necessitando di tempi più lunghi per uma più profonda comprensione*"[40].

Outro aspecto importante disciplinado no GDPR são os "direitos" conferidos aos cidadãos, dentre os quais se destacam "o direito de ser excluído"; direito ao esquecimento; o "direito de se opor" (isto é, negar o uso de seus dados pessoais para determinadas situações, tais como campanhas de marketing, criação de perfis etc.); o "direito de retificação" dos dados incorretos, o "direito de transparência"[41] (que garante acesso sobre o processamento e armazenamento dos seus dados, incluindo: tempo de retenção, dados de contato do responsável pelos dados pessoais na organização, justificativa para manter o dado pessoal armazenado); e também o "direito à portabilidade" (tal qual ocorre com as operadoras de telefonia, para utilizar uma comparação, os cidadãos poderão optar por transferir os seus dados para outro "gestor" que considere mais adequado aos seus interesses, o que deverá ser possibilitado sem entraves burocráticos).

Quanto ao tratamento dos dados, o GDRP reforçou os seguintes princípios: (i) licitude, lealdade e transparência; (ii) limitação das finalidades; (iii) minimização dos dados; (iv) exatidão; (v) limitação do prazo de conservação; (vi) integridade e confidencialidade; e, por fim, (vii) responsabilidade.

Por certo, o novo Regulamento trouxe muitas novidades que mereceriam destaque. Todavia, considerando os limites desse ensaio, nos limitaremos aos comentários feitos até o momento.

Passamos, agora, a analisar a legislação brasileira sobre o tema.

## 4 BREVES CONSIDERAÇÕES SOBRE A LEGISLAÇÃO BRASILEIRA ACERCA DA PROTEÇÃO DE DADOS PESSOAIS

No Brasil, ainda não há uma lei específica, ampla e atualizada que tutele a proteção de dados pessoais tal qual o GDPR europeu, o que não significa que estamos absolutamente desprotegidos nesse campo. Existem algumas normas setoriais dispostas em leis esparsas que conferem certa "proteção" em alguns aspectos, mas claramente não se mostram suficientes para garantir a segurança jurídica necessária nesse campo tão tormentoso que é o do tratamento de dados pessoais nos dias atuais.

[40] CALIFANO, Licia. **Privacy**: affermazione e pratica di un diritto fondamentale. Napoli: Editoriale Scientifica, 2016. p. 102.

[41] DI GENIO, Giuseppe. Tranparenza e acesso ai dati personali. *In*: SICA, Salvatore; D'ÁNTONIO, Virgillio; RICCIO, Giovanni Maria (Org.). **La Nuova Disciplina Europea della Privacy**. Milano: Wolkers Kluwer, 2016.

A Constituição Federal de 1988 traz em seu bojo diversos dispositivos que tutelam a personalidade, inclusive a vida privada e a intimidade (art. 5º, X), sendo igualmente certo que os "dados pessoais" configuram facetas da privacidade (ainda que possam ser considerados também autonomamente). Logo, esse dispositivo serve, em princípio, para garantir a proteção do tratamento de dados pessoais. Mas, como é cediço, normas amplas e abstratas demais muitas vezes acabam por não garantir a eficácia almejada, mormente quando não se têm critérios objetivos para melhor permitir a sua aplicação ao caso concreto.

Além dessa regra de proteção geral à vida privada e à intimidade, a Carta Magna também prevê o "remédio constitucional" para assegurar ao titular do direito o conhecimento das informações a seu respeito constantes de registros ou bancos de dados de entidades governamentais ou de caráter público. Trata-se do *habeas data*, recurso esse que serve também para a retificação de dados que porventura venham a constar equivocadamente nos referidos registros públicos, quando não se puder fazê-lo por processo sigiloso, judicial ou administrativo. Muitos doutrinadores apontam para a ineficácia desse "remédio", afirmando que ele se mostrou de pouco uso e praticidade. De qualquer sorte, ele existe e serve, sim, como um potente instrumento para o cidadão ter um certo grau de controle sobre as informações que lhe digam respeito.

Para além da Carta Magna, temos no cenário nacional o Código de Defesa do Consumidor[42] – Lei 8.078/1990, que em seu art. 43 e parágrafos, traz diversas regras sobre o tratamento e armazenamento de dados de consumidores, notadamente daqueles dados de natureza creditícia e financeira. Contudo, assim como ocorreu com as demais normas que versam sobre proteção de dados, editadas na década de 1990, esses dispositivos específicos tornaram-se "obsoletos" para a realidade hodierna, diante das novas tecnologias de comunicação e informação, necessitando de revisão/ajustes.

Mais de duas décadas após o advento do CDC, vieram as leis do Cadastro Positivo (Lei 12.414/2011) – prestes a ser alterada –, e a de Acesso à Informação (Lei 12.527/2011): a primeira, visando formar um banco de dados "positivos", como o próprio nome já diz, reunindo informações "boas" acerca dos consumidores (pon-

[42] BRASIL. LEI 8.078/1990 – Código de Defesa do Consumidor. "***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.*
***§ 1º*** *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.*
***§ 2º*** *A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*
***§ 3º*** *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.*
***§ 4º*** *Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*
***§ 5º*** *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.*
***§ 6º*** *Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor*" (Incluído pela Lei 13.146/2015).

tualidade no pagamento de contas, capacidade de endividamento etc.), para se contrapor aos até então exclusivos bancos de dados "negativos" (ou de 'proteção ao crédito), os quais reúnem informações de consumidores inadimplentes; e a segunda, visando garantir maior transparência no âmbito da Administração Pública.

Ambas as leis geraram fortes polêmicas à época em que entraram em vigor. A do Cadastro Positivo, em razão da falta de clareza acerca dos dados a serem computados para a "formação do *scoring*" do consumidor, fato que ensejou uma "enxurrada" de ações no Judiciário[43] e acabou por forçar o STJ a firmar tese pelo rito dos recursos repetitivos (art. 543-C do CPC) – "*Tema 710*"[44]. Já a do Acesso à Informação, porque em nome da máxima transparência possível acerca da Administração Pública, a lei permitiu não só a divulgação dos salários de todos os servidores públicos, mas também mecanismos capazes de identificar e individualizar cada um deles, o que para muitos caracterizou violação direta à privacidade, com exposição desnecessária de dados pessoais.

Ainda quanto a Lei do Cadastro Positivo, vale observar que a previsão do legislador foi a de que o referido cadastro somente poderia ser aberto com a autorização expressa do consumidor (consentimento informado e expresso). Porém, essa regra – que estava de acordo com as legislações mais 'modernas' sobre o tema, inclusive com a Diretiva 95/46/EC da União Europeia que vigorava na época, e também com o atual GDPR, dando aplicabilidade ao princípio da *autodeterminação informativa* – está prestes a cair por terra. Isso porque a Câmara dos Deputados aprovou há pouco mais de 30 dias (em 09.05.2018) o PLP 441/17, que altera substancialmente não só esse aspecto (a entrada do consumidor deixa de ser um ato voluntário, opcional, passando a ser automática), mas também outros de suma importância, pois deixa de considerar quebra de sigilo das instituições financeiras o repasse de dados sobre pagamento às agências de crédito e bancos de dados para a formação do *scoring* do consumidor. Será, em princípio, um grande retrocesso.

Há, ainda, uma outra norma em vigor no Brasil que versa sobre a tutela dos *dados pessoais.* Trata-se da Lei 12.965/2014, mais conhecida como *Marco Civil da Internet*, a qual destinou parte do "capítulo 3" (mais precisamente do art. 10º ao 21º) para disciplinar acerca da "proteção aos registros, aos dados pessoais e às comunicações privadas", "da guarda de registros de conexão", "guardas de registros de acesso

---

43 Informação disponível em: <http://www.tjba.jus.br/nugep/index.php/informativos/40-scoring>. Acesso em: 28 jun. 2018.

44 Trata-se do REsp 1419697/RS, onde se firmaram as seguintes teses: "*I – TESES: 1) O sistema 'credit scoring' é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei 12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei 12.414/2011. 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. 5) O desrespeito aos limites legais na utilização do sistema 'credit scoring', configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados*".

e aplicações de internet" (tanto na provisão de conexão quanto na de aplicações), bem como acerca "da responsabilidade por danos decorrentes de conteúdo gerado por terceiros". Todavia, vários aspectos dessa lei estão sendo questionados, estando o Supremo Tribunal Federal para decidir, em sede de repercussão geral, o alcance de vários desses dispositivos.

De qualquer forma, é lugar comum entre os juristas e doutrinadores que o Marco Civil da Internet é deveras insuficiente para garantir a efetiva proteção de dados pessoais no Brasil, razão pela qual estão tramitando projetos de lei no Congresso Nacional para disciplinar nova e profundamente a questão.

Tramitavam inicialmente na Câmara dos Deputados o PL 4.060/2012, de autoria do Deputado Milton Monti (cujo texto era bastante simples, com poucos artigos, adotando conceito 'reducionista' para os dados pessoais), o PL 5.276/2016 (de autoria do Poder Executivo), bem como o PL 6.291/2016 (de autoria do Deputado João Derly). Ditos Projetos foram apensados e em dado momento encaminhados à Comissão Especial destinada a proferir parecer conjunto, sobrevindo, ao final, um texto único [mantido sob o primeiro número, ou seja PL 4.060, muito mais completo e complexo do que o texto original, mais semelhante com o GDPR e mais condizente com o atual contexto internacional.

O referido texto foi aprovado pela Câmara dos Deputados há cerca de um mês (em 29.05.2018), e agora o Projeto segue para o Senado, onde tramitam outros três PLs versando sobre a temática, a saber: 330/2013, 131/2014 e 181/2014, que foram fundidos em um substitutivo apresentado pelo Senador Aloysio Nunes, .

Nesse ínterim, diversos estudos comparativos entre os textos normativos debatidos no legislativo foram realizados pelos mais diversos órgãos[45]. O estudo que nos parece mais completo e relevante é aquele desenvolvido pelo Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação da Universidade de São Paulo, encabeçado por BIONDI. Sob o título "*Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil*"[46], o texto traça um comparativo analítico entre os principais aspectos a serem tutelados pela nova legislação, a saber: (i) conceito de dados pessoais; (ii) dados anônimos; e (iii) consentimento do titular dos dados pessoais, mostrando como aparentes 'sutis' diferenças conceituais acarretam drásticas diferenças de proteção.

Sintetizando o referido estudo – já que neste ensaio não há espaço para o aprofundamento desejado – é possível concluir que:

No que tange ao conceito de *dados pessoais*, o texto original do PL 4.060/2012 contemplava a versão reducionista[47]; já o PL 5.276/2016 contemplava versão expansionista completa, com rol exemplificativo[48]; já o texto do Senado,

[45] Veja-se, por exemplo, o estudo intitulado "Proteção de dados pessoais no Brasil: análise dos projetos de lei em tramitação no congresso nacional", realizado pela organização Artigo19. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 15 jun. 2018.

[46] BIONDI, B. Xeque-Mate, *cit*.

[47] PL 4.060/2012 CÂMARA DOS DEPUTADOS. Projeto originário. "***Art. 7º, inc. I** – dado pessoal: qualquer informação que permita a identificação exata e precisa de uma pessoa determinada*".

[48] PL 5276/2016 DO EXECUTIVO. "***Art. 5º, inc. 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*".

contemplou conceito expansionista, porém mais simples, nos seguintes termos: "*Art. 3º, I: dado pessoal: qualquer informação sobre pessoa natural identificável ou identificada*". Por certo, não é tão completo quanto o do GDPR, mas permite a proteção no mesmo nível conferido pelo novel regime europeu.

No que tange aos dados anônimos "*e a sua pseudo-dicotomia com o conceito de dados pessoais*"[49], o autor sugere a adoção de um "filtro de razoabilidade" explicando que esse nada mais é do que "uma diretriz acerca do que venha a ser um risco aceitável em torno da reversibilidade do processo de anonimização, a fim de que os dados anonimizados estejam fora do conceito de dados pessoais". Novamente o autor faz um comparativo entre as três proposições analisadas, concluindo que o PL originário da Câmara dos Deputados sequer previa definição e aplicação para os dados anônimos. Já o PL do executivo e o PL do Senado adotaram os conceitos e filtros pertinentes[50].

Por fim, no que tange ao "*consentimento*", considerado aspecto de suma importância em todos os ordenamentos jurídicos, BIONDI destaca os "adjetivos" que, se e quando adotados, conferem maior "carga participativa" ao titular dos dados e, consequentemente, maior consciência acerca do tipo e da extensão das informações que efetivamente se está disponibilizando quando inocentemente se clica no ícone "de acordo" ou similar.

Novamente o autor compara os artigos correspondentes de cada uma das proposições, concluindo que no projeto originário da Câmara era nula/inexistente, pois o PL sequer adotou o consentimento como estratégia regulatória central, só cogitando a vontade do titular dos dados pessoais após o início do tratamento de dados pessoais (*opt-out*), sem qualquer tipo de qualificação em torno do consentimento, e isso mesmo, para um grupo restrito (menores de idade). Já no PL de autoria do Executivo era intermediária, e no texto do Senado, máxima[51].

O texto final da Câmara enviado ao Senado ainda dependerá de aprovação por aquele colegiado, e poderá sofrer substanciais modificações a partir da "junção" com o texto dessa Casa. De qualquer sorte, a tendência é que não se distancie muito do que foi enviado pela Câmara, na medida em que o texto reflete o esforço conjun-

---

[49] BIONDI, *op. cit*., p. 25 e ss.

[50] No que tange aos dados anônimos e/ou anonimizados, o autor faz as seguintes comparações: No PL da Câmara dos Deputados, não há definição sobre as expressões, e tampouco filtro de razoabilidade. No PL do senado, os dados anônimos estão previstos no art. 2º, inc. IV, alínea 'a' (*anonimizados e dissociados, desde que não seja possível identificar o titular*). No PL do Executivo, no art. 5º, inc. V (*dados anonimizados: dados relativos a um titular que não possa ser identificado*); Como definição de anonimização, o PL do Senado diz no art. 2º, inc. IV, § 4º que "*os dados desanonimizados, assim compreendidos aqueles dados inicialmente anônimos que, por qualquer técnica, mecanismo ou procedimento, permitam a qualquer momento a identificação do titular, terão a mesma proteção dos dados pessoais, aplicando-se aos responsáveis por sua coleta, armazenamento e tratamento o disposto nesta lei*". Já a definição contida no PL do Executivo (5.276) consta no art. 5º, inc. XII: "*anonimização: qualquer procedimento por meio do qual um dado deixa de poder ser associado, direta ou indiretamente, a um indivíduo*". Por fim, no que tange ao filtro de razoabilidade, os Projetos de Lei assim disciplinam: Senado: art. 3º, inc. XIV (autorregulação total), e o do Executivo no art. 13, *caput* e § 2º, sendo o (heterorregulação total).

[51] O consentimento está previsto em todos os três projetos analisados (Câmara, nos arts. 15 e 17; Senado, art. 6º, IV e 12, I; Executivo, art. 5º, VII e 7º, I). No que tange à carga participativa do titular dos dados e a estratégia regulatória central, o PL da Câmara (texto original) sequer a adota. Já o PL do Senado a adota com carga "máxima", enquanto que o do Executivo a adota com carga "intermediária".

to da sociedade, dos órgãos de controle (tais como a CGU) e do próprio Governo. Ademais, é interesse do País adotar normas semelhantes ao GDPR, até por questões econômicas/mercadológicas, valendo ressaltar que em alguns aspectos o PL do Senado inclusive se mostrou mais rígido/protetivo.

## CONSIDERAÇÕES FINAIS

Poucos temas jurídicos mostraram-se tão sensíveis aos impactos tecnológicos e às mudanças culturais do que o direito à privacidade. As invenções da fotografia, das gravações e da telefonia (com a possibilidade de interceptações), consistiram em inovações tecnológicas que, ao seu tempo, já mostraram seu potencial ameaçador para clássica noção de privacidade. A moderna revolução da comunicação, com o advento da *internet* e a conexão global daí resultantes, alterou radicalmente nossa forma de viver – e nossa forma de conceber a privacidade.

O antigo *right to be let alone* – embora ainda importante – parece ser menos relevante do que os riscos acarretados pela possibilidade de coletar e sistematizar dados pessoais. Isso porque aquele antigo direito parece interessar a uns poucos, em situações específicas, ao passo que a nova ameaça atinge a todos.

De fato, a maneira como passamos a existir deixa rastros virtuais facilmente captáveis por quem se dedicar a isso. Todas as nossas transações comerciais, das mais simples às mais complexas, são transformadas em dados armazenados na rede. Cada vez mais os pagamentos que fazemos por produtos e serviços que adquirimos são feitos por cartões de crédito – facilmente rastreáveis. Nossa localização geográfica é identificada por aplicativos presentes em nossos celulares, com nosso consentimento. Acessamos sites e baixamos conteúdos que revelam nossas predileções culturais, tendências ideológicas, gostos e interesses. Nossas comunicações com amigos, conhecidos e simples coparticipantes de grupos, são relativamente fáceis de acessar.

Quem se dedica a reunir tais informações, sistematizá-las e analisá-las, facilmente tem uma ideia precisa de quem somos, o que pensamos, do que gostamos. Os mecanismos de inteligência artificial conseguem reunir milhões de pequenas informações, isoladamente irrelevantes, mas que agrupadas possuem significados que talvez não sejam percebidos pela própria pessoa. Sabendo quem alguém é permite saber o que ele provavelmente fará. Daí a provocar tal ação é um pequeno passo. Enquanto esse conhecimento é usado – e já o é há muito tempo – para nos induzir ao consumo, os danos não são tão intoleráveis. Mas acontecimentos recentes – como a última eleição presidencial norte-americana e o plebiscito relativo ao *Brexit* – mostraram como a manipulação de pessoas, explorando e reforçando artificialmente tendências, podem acarretar mudanças significativas para todo um país.

São essas as preocupações que fizeram com que juristas e legisladores de todo o mundo voltassem suas atenções para a necessidade de estabelecer normas claras e mais rígidas, buscando garantir os benefícios que as tecnologias de comunicação e informação propiciam a todos, mas procurando senão eliminar, ao menos reduzir a possibilidade de utilização de dados pessoais para manipulação das pessoas e influências indevidas, com riscos para o viver democrático.

A União Europeia está fazendo o seu "dever de casa": atenta para o fato de que as regras previstas na Diretiva 95/46/EC restaram ultrapassadas em decorrência do avanço tecnológico, tratou de elaborar um novo marco legal para substituí-la,

vindo a editar o *General Data Protection Regulation*, instrumento extremamente completo e complexo, capaz de garantir – ao menos por um tempo – a proteção necessária aos direitos e garantias fundamentais de seus cidadãos, em especial o direito à privacidade e à autodeterminação informativa.

O Brasil, contudo, não está tão bem assim. Somente após a entrada em vigor do GDPR Europeu é que passou a agilizar a tramitação de Projetos de Lei sobre o tema em suas casas legislativas. Não obstante, continua 'pecando' pela falta de informação (que ironia!) à sociedade, na medida em que não a chama para debater assunto de tamanha importância. De fato, muitas pessoas sequer imaginam o risco que correm com a captura, tratamento e armazenamento de dados pessoais seus, muitas vezes (senão a maioria) obtidos sem a sua permissão e/conhecimento.

De qualquer sorte, é de se saudar o fato de que se começou a debater o tema, ao qual deve voltar sua atenção a comunidade jurídica e toda a sociedade, pois desse debate e das decisões normativas que forem tomadas poderá resultar, nesse particular, "o Brasil que queremos".

## REFERÊNCIAS


ALLEN, Anita. **Uneasy Access: Privacy for Women in a Free Society**. Totowa/NJ: Rowman and Littlefield, 1988.

ALVES, P. **Facebook e Cambridge Analytica**: sete fatos que você precisa saber. Matéria publicada em: <https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml>. Acesso em: 24 jun. 2018.

BIONI, B. R. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. Projeto de Pesquisa Privacidade e Vigilância. Disponível em: <http://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciati vas_legislativas_no_Brasil>. Acesso em: 26 jun. 2018.

BRANDEIS, Louis. WARREN, Samuel. The Right to Privacy. **Harvard Law Review**, v. IV, December 15, 1980, n. 5. Artigo, na sua versão eletrônica. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 30 maio 2017.

BRASIL. LEI 8.078/90 – Código de Defesa do Consumidor.

BRASIL. PROJETO DE LEI 4.060/2012 – CÂMARA DOS DEPUTADOS.

BRASIL. PROJETO DE LEI 5.26/2016 – EXECUTIVO

BRASIL. PROJETO DE LEI ... SENADO FEDERAL.

CALIFANO, Licia. **Privacy**: affermazione e pratica di un diritto fondamentale. Napoli: Scientifica, 2016.

CISCO VISUAL NEWORKING INDEX: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html?CAMPAIGN=Mobile+VNI+2017&COUNTRY_SITE=us&POSITION=Press+Release&REFERRING_SITE=PR&CREATIVE=PR+to+MVNI+white+paper>. Acesso em: 29 jun. 2018.

DANTAS, M. **Capital-informação**" **e virtualização financeira**: isso ainda é capitalismo? Disponível em: <http://gindre.com.br/capital-informacao-e-virtualizacao-financeira-isso-ainda-e-capitalismo/>. Acesso em: 28 jun. 2018

DI GENIO, Giuseppe. Tranparenza e acesso ai dati personali. *In*: SICA, Salvatore; D'ÁNTONIO, Virgillio; RICCIO, Giovanni Maria (Org.). **La Nuova Disciplina Europea della Privacy**. Milano: Wolkers Kluwer, 2016.

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

ETZIONI, Amitai. **How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism.** New York-London: Routledge, 2004.

FACCHINI NETO, Eugênio. Prefácio da obra **Direitos da Personalidade**: disponibilidade relativa, autonomia privada e dignidade humana, de autoria de Fernanda Borghetti Cantalli. Porto Alegre: Livraria do Advogado, 2009.

FRANCE. Loi 78-17 du 6 janvier 1978 relative à l´informatique, aux fichiers et aux libertés. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>. Acesso em: 26 jun. 2018.

FRIED, Charles. Privacy: A Rational Context, in: ERMANN, M. D.; WILLIAMS, M.B.: GUTIERREZ, C. (Org.). **Computers, Ethics, and Society**. New York: Oxford University Press, 1990.
GAVISON, Ruth. Privacy and the Limits of the Law. **Yale Law Journal**, 1980.
KRAUS, R. S. **Statistical Déjà Vu**: The National Data Center Proposal of 1965 and Its Descendants. Disponível em: <https://www.census.gov/history/pdf/kraus-natdatacenter.pdf>. Acesso em: 29 jun. 2018.
MAYER-SCHÖNEMBERGER. V. General development of data protection in Europe. *In*: AGRE, P. ROTEMBERG, M. (Orgs.). **Technology and Privacy**: the new landscape. Cambridge: MIT Press, 1997. p. 219-242.
PAGALLO, Ugo. **La tutela della privacy negli Stati Uniti d'America e in Europa – Modelli giuridici a confronto**. Milano: Giuffrè, 2008.
PARENT, William A. Privacy, Morality and the Law. **Philosophy and Public Affairs**, 1983.
PIZZETTI, F. **I Diritti nella 'rete' della Rete – Privacy e il Diritto Europeo alla Protezione dei Dati Personali**: il Regolamento europeo 2016/679. Torino: Giappichelli Editore, 2016.
POULLET, Y., ASINARI, M. V. P,, PALAZZI, P. A. **Derecho a la indimidad y protección de datos personales**. Buenos Aires: Heliasta, 2009.
REINALDO FILHO, D. **A Diretiva Europeia sobre proteção de dados pessoais**: uma análise de seus aspectos gerais, fev. 2013. Disponível em: <https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais>. Acesso em: 26 jun. 2018.
Regulamento (UE) 2016/679, de 27.04.2016. **General Data Protection Regulation**, art. 3°, "1". Disponível em: <https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf>.
RODOTÁ, Stefano. **A vida da sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.
RODOTÁ, Stefano. **Tecnologie e diritti**. Bologna: Il Mulino, 1995.
RODRIGUES, J. Regulação, Ética e **Governance**. Lisboa: RH, 2018.
RUGGLES, R. *et all*. Report of the Committee on the Preservation and Use of Economic Data (1965). <https://ia800200.us.archive.org/31/items/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965/Ruggles_econdata_1965.pdf>. Acesso em: 29 jun. 2018.
SCHWARTZ, P. M. SOLOVE, D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *In*: **Berkeley Law Scholarship Repository**, 01.01.2011. Disponível em: <https://scholarship.law.berkeley.edu/facpubs/1638/>. Acesso em: 26 jun. 2018.
SIMITIS, S. Il contesto giuridico e politico della tutela della privacy. **Rivista Critica del Diritto Privato**, 1997.
STIGLITZ, J. E. Economics of Information and the Theory of Economic Development, **Revista de Econometria**, v. 5, n. 1, p. 5-32, abr. 1985.