UNIVERSIDADE TIRADENTES
DIRETORIA DE PESQUISA E EXTENSÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITOS HUMANOS

JÉFFSON MENEZES DE SOUSA

A EFETIVIDADE DA PROTEÇÃO DE DADOS PESSOAIS FRENTE AO *BIG DATA*

ARACAJU
2017

UNIVERSIDADE TIRADENTES
DIRETORIA DE PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITOS HUMANOS

A EFETIVIDADE DA PROTEÇÃO DE DADOS PESSOAIS FRENTE AO *BIG DATA*

Autor: Jéffson Menezes de Sousa

Orientadora: Profa. Dra. Liziane Paixão Silva Oliveira

Coorientador: Prof. Dr. Marco Aurélio Rodrigues da Cunha e Cruz

ARACAJU, SE - BRASIL
MARÇO DE 2017

A EFETIVIDADE DA PROTEÇÃO DE DADOS PESSOAIS FRENTE AO *BIG DATA*

JÉFFSON MENEZES DE SOUSA

DISSERTAÇÃO SUBMETIDA AO PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA UNIVERSIDADE TIRADENTES COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM DIREITOS HUMANOS.

Aprovada por:

_____
Profa. Dra. Liziane Paixão Silva Oliveira (Orientadora)

_____
Prof. Dr. Marco Aurélio Rodrigues da Cunha e Cruz (Coorientador)

_____
Prof. Dr. Ricardo José das Mercês Carneiro

_____
Profa. Dra. Clara Cardoso Machado Jaborandy

ARACAJU, SE - BRASIL
MARÇO DE 2017

S725ec

Sousa, Jéffson Menezes de
A efetividade da proteção de dados pessoais frente ao *big data* / Jéffson Menezes de Sousa ; orientação [de] Profª. Drª. Liziane Paixão Silva Oliveira; Coorientador [de] Prof. Dr. Marco Aurélio Rodrigues da Cunha e Cruz – Aracaju : UNIT, 2017.

111 f. il.: 30cm

Inclui bibliografia.
Dissertação (Mestrado em Direitos Humanos)

1. *Big data*. 2. Dados pessoais. 3. Privacidade. 4. Proteção. 5. Tecnologia. I. Oliveira, Liziane Paixão Silva . (orient.) II. Cruz, Marco Aurélio Rodrigues da Cunha e. III. Universidade Tiradentes. IV. Título.

CDU: 004.738.52.056:346.458

Dedico esse trabalho aos meus orientadores que me acolheram desde a graduação, aos quais serei eternamente grato pelos ensinamentos durante todos esses anos, indispensáveis para a elaboração desse trabalho.

AGRADECIMENTOS

Considerando que *agradecer* é mostrar ou manifestar gratidão, faço uso desse espaço, ainda que de forma breve, mas indispensável, para agradecer e demonstrar meu carinho a todos àqueles que me acompanharam durante essa trajetória, por todo o incentivo nos momentos em que medos e angústias afloraram e pela compreensão quando meus compromissos com a academia me tornaram indisponível. Assim, agradeço à (aos):

*DEUS***,** por representar meu porto seguro.

MEUS PAIS, Fátima e Francisco, e *MEU IRMÃO*, Ricardo, por todos os sacrifícios e por depositarem em mim a confiança que serve de combustível para cada superação.

MEUS ORIENTADORES, profa. Liziane Paixão e prof. Marco Aurélio, pela generosidade ao compartilharem seus conhecimentos indispensáveis para a concretização dessa dissertação, assim como pela parceria e paciência comigo que vem desde a graduação com a iniciação científica, meu muitíssimo obrigado.

PROFESSORES DO PPGD-UNIT, que a partir de suas aulas, encontros e leituras recomendadas contribuíram decisivamente na construção desse trabalho e por terem me estimulado a desbravar ainda mais o universo da pesquisa.

AMIGOS DO PPGD-UNIT, por terem sido espetaculares e mostrado que a pós-graduação além de representar uma experiência de vida inigualável e nos conceder ao final um título acadêmico, nos presenteia com verdadeiras e valiosas amizades, tendo sido eu ao final um grande sortudo em transitar por duas turmas maravilhosas 2015 e 2016, destacando aqui em especial aqueles que me acompanharam por mais tempo e de maneira mais próxima, *Rosane Bezerra, Fernanda Oliveira, Kellen Muniz, Luíz Ricardo, Renata Mendonça, Laura Braz, Thiago Santana.*

Não podendo deixar de registrar ainda meu especial agradecimento ao amigo *Afonso Oliva* por ter me ajudado, com toda sua experiência e conhecimento sobre proteção de dados pessoais, durante a minha qualificação no mestrado.

FUNCIONÁRIOS DO PPGD-UNIT por todo apoio durante esses dois anos.

AMIGOS, meu muito obrigado por todo incentivo, compreensão e torcida não só no mestrado, mas por estarem sempre vibrando comigo, com especial atenção a *Andrezza Barbosa, Hellen Nayara, Pablo Sousa, Anderson Costa, Douglas Barreto, Isabela Souza, Conceição Bezerra e Abelardo Figueredo*, *Uellington Oliveira e Tiago Santos. Vocês definitivamente fizeram parte dessa agradável surpresa em forma de superação*.

Peço apenas que permaneçamos abertos, benevolentes, receptivos em relação à novidade.

Pierre Lévy (Cibercultura)

RESUMO

O avanço da tecnologia da informação e o número de usuários da internet vêm crescendo numa proporção exponencial, facilitando o acesso e o armazenamento de grandes quantidades de dados, rapidamente. Um dos riscos deste fenômeno tecnológico é que o indivíduo deixa de ter controle sobre a precisão, a localização e o que está sendo feito com os seus dados, ficando, assim, cada vez mais vulnerável. Diante dessa problematização, o objetivo principal desta pesquisa é examinar a efetivação da proteção jurídica aos dados pessoais no contexto do *big data*, visto que este proporciona o grande armazenamento dos dados. Para isso, tal conceito é abordado no contexto da sociedade de controle, vista como desdobramento da sociedade disciplinar, caracterizando o *big data* pelo grande volume de dados que possui, pela velocidade, devido à quantidade de dados novos criados em segundos, e pela variedade, buscando verificar os riscos trazidos pela nova tecnologia do *big data* à privacidade. Foi examinada, também, a construção do direito à proteção de dados pessoais como direito fundamental, delimitando a proteção jurídica a esses dados no ordenamento jurídico brasileiro, especialmente pela Constituição Federal, o Código Civil de 2002, o Código de Direito do Consumidor e a o Marco Civil da Internet (Lei 12.965/2014), bem como a influência da legislação internacional sobre a legislação brasileira acerca da proteção de dados pessoais. A pesquisa é de cunho bibliográfico para um referencial teórico com embasamento científico, e foram utilizados os métodos dedutivo e qualitativo. Por conduto das ideais expostas neste estudo, conclui-se que o Brasil, comparado aos países europeus e alguns da América Latina, encontra-se atrasado, tendo em vista não existir ainda legislação específica sobre a proteção de dados pessoais, mas, somente, Projeto de Lei que visa ao tratamento deste direito. O direito fundamental à proteção de dados pessoais no Brasil é violado, inefetivo, possui um déficit legiferante e está pendente de uma resposta jurídico-normativa que desenvolva a sua importância na Sociedade da Informação. Assim, diante das inovações tecnológicas e principalmente do *big data*, para uma efetiva proteção jurídica aos dados pessoais, mostra-se mais adequada uma regulação principiológica, fundada especialmente na finalidade, responsabilidade e segurança, a fim de que o avanço tecnológico não seja inviabilizado e o indivíduo não esteja desprotegido. Por fim, ressalta-se que este trabalho está vinculado à linha de pesquisa “direitos humanos, novas tecnologias e desenvolvimento sustentável”.

Palavras-chave: *Big data*. Dados pessoais. Privacidade. Proteção. Tecnologia.

ABSTRACT

The advance of the technology of information and the number of internet users have been increasing in an exponential proportion, facilitating the access and the storage of big quantity of data, quickly. One of the risks of this technological phenomenon is that people no long have control about the accuracy, the localization and what is been doing with its data, being, thus, every time more vulnerable. In the face of this problematization, the main objective of this research is to exam the realization of legal protection of personal data in the big data context, whereas this provides large data storage. For this purpose, such concept is addressed in the regulation of society context, seen as unfolding of disciplinary society, characterizing the big data by the big volume of data that it belongs, by speed, due the quantity of new data created in seconds, and by variety, searching to check the risks brought by the new technology of big data to privacy. it was also examined the construction of the right to the personal data protection as a fundamental right, delimiting the law protection to these data on Brazilian legal framework, specially by the Federal Constitution, Civil Code of 2002, Consumer Defense Code and Brazilian Civil Rights Framework (law 12.965/2014), such as the influence of the international law on the Brazilian law about the personal data protection. The research is bibliographic and it used the deductive and qualitative methods. By conduct of the exposed ideas in this study, it concludes that Brazil, compared to the European countries and some of Latin America, is delayed, In view of the fact that there is still no specific legislation on the protection of personal data, but only, Law Project which aims the treatment to this right. The fundamental right to personal data protection in Brazil is violated, ineffective, it has a legislate deficit and it is pending a legal-normative response which develops its importance in the Information Society. Thus, facing the technological innovation and mainly the big data, for an effective juridical protection to the personal data, it shows more appropriated a principiological regulation, based specially on the objective, responsibility and security, so the technological advance is not invalidated and the individual is not unprotected. Finally, it must be observed that this work is linked to the “human rights – new technologies and sustained development” research line.

Keywords: Big data. Personal Data. Privacy. Protection. Technology.

LISTA DE SIGLAS E ABREVIATURAS

CADE	*Conselho Administrativo de Defesa Econômica*
CDC	Código de Defesa do Consumidor
Ceweb	Centro de Estudos sobre Tecnologias Web
CF88	Constituição Federal de 1988
GPS	*Global Positioning System*
InWeb	Instituto Nacional de Ciência e Tecnologia para a Web
LAI	Lei de Acesso à Informação
LCP	Lei do Cadastro Positivo
MCI	Marco Civil da Internet
MIT	*Massachusetts Institute Technology*
Nic.br	Núcleo de Informação e Coordenação do Ponto BR
OECD	*Organisation for Economic Co-operation and Development*
OMS	Organização Mundial de Saúde
PL	Projeto de Lei
RSAS	Regulamento de Salvaguarda de Assuntos Sigilosos
SFICI	Serviço Federal de Informações e Contra-Informações
SNI	Serviço Nacional de Informações
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TIA	*Total Terrorism Information Awareness*

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O surgimento e a adesão de sociedades às novas tecnologias da informação e comunicação criaram um novo padrão de organização social: a Sociedade da Informação. Por meio dos recursos tecnológicos implementados pelo uso da informática, os indivíduos que compõem esta sociedade passaram a armazenar informações em grande escala e, igualmente, acessar, de maneira simples, fácil e rápida, conteúdo gerado a todo instante seja por *smartphones*, aplicativos *on-line*, entre outros. É inegável que, em decorrência das novas tecnologias e seus efeitos, há uma modificação dos tradicionais comportamentos da sociedade.

Conforme a Pesquisa Brasileira de Mídia 2015[1], cerca de 48% dos brasileiros usam internet regularmente, dos quais 67% utilizam essa tecnologia para se informar, outros 67% para se divertir, 38% para passar o tempo livre e 24% para estudar. Uma pesquisa da *Deloitte*[2] com dois mil brasileiros das cinco regiões do país aponta que 31% das pessoas aceitam compartilhar dados pessoais com empresas, especialmente se puderem escolher quais as informações, enquanto que 17% dizem não fazer nenhuma restrição à coleta de seus dados pela internet. Uma terceira pesquisa realizada em fevereiro de 2015 pelo *YouGov*[3], solicitada pela organização Anistia Internacional, que entrevistou 15 mil pessoas em 13 países do mundo, incluindo o Brasil, indica que apenas um em cada quatro brasileiros concorda que o governo deve monitorar e vigiar dados de internet e telefonia da população.

Todos os dados levantados servem para demonstrar que é crescente a utilização da internet pelos indivíduos, assim como cada vez mais o sujeito está vulnerável, pois, desde o cadastro no primeiro acesso à internet com o registro do usuário em rede, inicia-se a transmissão de dados que serão armazenados em bancos de dados remotos automatizados, como os *data centers* do Google, um dos

---

[1] CERCA de 48% dos brasileiros usam internet regularmente **Portal Brasil,.** 19 dez. 2014. Disponível em: < http://www.brasil.gov.br/governo/2014/12/cerca-de-48-dos-brasileiros-usam-internet-regularmente>. Acesso em 15 maio 2016.

[2] CONVERGÊNCIA DIGITAL. **Pesquisa diz que 31% dos brasileiros aceitam compartilhar dados pessoais**, 28 out. 2015b. Disponível em: < http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActive Template=site&infoid=40999#.V0s3-hjgozm>. Acesso em 15 maio 2016.

[3] CONVERGÊNCIA DIGITAL. **Brasileiros reagem à espionagem e rejeitam repasse de dados por empresas de tecnologia**, 18 mar. 2015a. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39185&sid=18#.VRvPH7kU-9I>. Acesso em 15 maio 2016.

principais em Oregon, nos Estados Unidos[4], utilizados para armazenar todo o conteúdo disponibilizado em suas ferramentas de busca na internet. Estima-se que o Google processa mais de 24 *petabyte*[5] de dados por dia, volume milhares de vezes maior que todo o material impresso na Biblioteca do Congresso dos Estados Unidos[6].

Tim Berners-Lee, o inventor da *world wide web* publicou uma carta[7] aberta sobre suas preocupações no contexto do aniversário de 28 anos da sua invenção, dentre elas destaca-se a perda do controle de nossos dados pessoais em razão dos termos e condições longas e confusas nas quais concordamos ceder nossos dados pessoais aos sites que oferecem em contrapartida conteúdo e serviços gratuitos. Alerta que, além das empresas privadas, os governos estão cada vez mais observando nossos movimentos on-line e passando leis extremas que atropelam nossos direitos à privacidade. As preocupações a que se refere Tim Berners-Lee podem ser vistas, a exemplo, a partir da recente proposta de venda da base de dados de usuários do Bilhete Único pela Prefeitura de São Paulo que inclui dados pessoais como: nome, endereço, cadastro de pessoa física, registro geral, nome da mãe, foto de rosto, entre outros[8].

Nesse cenário contextualizado da sociedade da informação, é inegável que os dados pessoais demandem uma maior proteção. As fichas e pastas utilizadas no passado para o armazenamento de dados, manualmente, foram abandonadas para dar espaço ao processamento eletrônico de dados que possibilitam o armazenamento das informações em grande escala, tornado possível pelo *big data*.

---

[4] PATI, Camila. **Conheça o data center do Google em que empregados não entram**, 29 mar. 2016. Disponível em: < http://exame.abril.com.br/tecnologia/noticias/conheca-o-data-center-do-google-que-nem-funcionarios-entram>. Acesso em 15 maio 2016.

[5] *Petabyte* representa "uma medida de memória ou armazenamento. Um petabyte tem, aproximadamente 1.000 terabytes (tecnicamente, o numero 2 elevado à 50ª potência)." (SYMANTEC. **Glossário.** Disponível em: <www.symantec.compt/br/security_response/glossary/define.jsp?letter=p&word=petabyte>.Acesso em 20 fev. 2017)

[6] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013, p. 5.

[7] BERNERS-LEE, Tim. Tim Berners-Lee: I invented the web. Here are three things we need to change to save it, 12 mar. 2017, **The Guardian**. Disponível em: <https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet?CMP=share_btn_fb>. Acesso em 15 mar. 2017.

[8] LEMOS, Ronaldo. Proposta de Doria de vender os dados do Bilhete Único é ilegal, 20 fev. 2017, **Folha de São Paulo**. Disponível em: < http://www1.folha.uol.com.br/colunas/ronaldolemos/2017/02/1860214-proposta-de-doria-de-vender-os-dados-do-bilhete-unico-e-ilegal.shtml>. Acesso em 15 mar. 2017.

As novas tecnologias foram pensadas para facilitar o acesso e compartilhamento entre diversos bancos de dados, porém trazem um ônus, pois o indivíduo deixa de ter controle sobre a exatidão, localização e os usos que estão sendo feitos de seus dados pessoais.

Emerge, assim, o dever de proteção do Estado contra os riscos à personalidade causados pelo tratamento de dados pessoais, considerando ainda que, na maioria das vezes, o indivíduo sequer pode decidir, de forma autônoma e livre, sobre o fluxo de seus dados pessoais na sociedade, motivo pelo qual se aumenta a necessidade de proteção estatal[9].

No contexto da sociedade da informação, do surgimento das novas tecnologias, especificamente do *big data,* e da vulnerabilidade dos dados pessoais dos indivíduos, o problema reside na seguinte questão: há uma efetiva proteção jurídica aos dados pessoais no contexto do *big data*? Para responder a essa pergunta utilizam-se três discursos: o científico, o normativo e o judicial; no primeiro, vale-se de uma revisão bibliográfica com suporte em um referencial teórico sobre os marcos conceituais “big data” e “direito fundamental à proteção de dados pessoais”; no segundo, analisam-se os mecanismos jurídicos e dispositivos legais pensados pelo legislador para tutelar os dados pessoais, na esfera internacional e nacional; e, no terceiro discurso, o judicial, examina-se como os tribunais têm se posicionado acerca da matéria.

Superada a introdução, na segunda seção partindo de um viés filosófico, antes de manejar os conceitos, características e adentrar na influência do *big data* no tratamento e armazenamento de dados pessoais, a fim de perceber como atua essa nova tecnologia, situa-se a passagem da “sociedade disciplinar” de Michel Foucault para a “sociedade de controle” de Gilles Deleuze. As considerações iniciais dessa seção buscam identificar em Foucault o que representa a “vigilância” na metáfora do Panóptico, para compreender que na sociedade de controle permanece a “vigilância” a partir de “bancos de dados”, uma espécie de versão “ciberespacial” do Panóptico, que tem sua concretização arquitetônica a partir dos *data centers* da Google, a exemplo, do que se faz também revisitando as lições de Zygmunt Bauman. Para tratar da natureza do *big data* e discutir os riscos e benefícios trazidos

[9] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 181-182.

por essa nova tecnologia, utiliza-se como referencial teórico Viktor Mayer-Schonberger, Kenneth Cukier, Thomas Davenport e Paul C. Zikopoulos.

Ainda na segunda seção, estabelecem-se os conceitos de dados pessoais, informação e banco de dados, com suporte na doutrina de Bertram Antônio Sturmer, Laura Schertel Mendes e José Afonso da Silva, com o auxílio do Regulamento Geral da União Europeia 2016/679 sobre proteção de dados pessoais, no qual a matéria está consolidada.

É na terceira seção do trabalho que figura a proteção de dados pessoais como direito fundamental, na qual se distinguem as nomenclaturas “proteção de dados pessoais” e “autodeterminação informativa", com base na conceituação técnico-jurídica realizada pelos autores espanhóis Antonio Enrique Pérez Luño e Pablo Lucas Murillo de la Cueva, elegendo a primeira como mais adequada ao ordenamento jurídico brasileiro. Têm espaço também os documentos internacionais que cuidam do direito fundamental à proteção de dados pessoais, bem como a influência da legislação internacional com enfoque nos países europeus Portugal, Espanha e Alemanha, tendo em vista que nesses países o direito em análise está positivado. Além dos europeus, examina-se o ordenamento jurídico da Colômbia, país latino-americano que, à frente do Brasil, conta com legislação específica sobre a matéria de dados pessoais.

Uma vez identificado o problema de pesquisa, buscou-se respondê-lo examinando a efetividade do direito à proteção de dados pessoais frente ao *big data*, considerando o marco legal do direito à proteção de dados pessoais, revisitando a Constituição Federal de 1988, o Código Civil de 2002, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, de Acesso à Informação, o Marco Civil da Internet e, por fim, as proposições legislativas para proteção de dados pessoais, especificamente o Projeto de Lei nº 5.276/2016.

O discurso normativo é abordado na quarta seção na qual prevalece o marco regulatório do direito em voga, com enfoque no ordenamento jurídico brasileiro, a partir da Constituição Federal de 1988 e legislação infraconstitucional até as proposições legislativas que tramitam no Congresso Nacional, a fim de examinar, a partir da leitura dos dispositivos legais em questão, em qual grau de proteção aos dados pessoais o ordenamento jurídico pátrio se encontra, assim como perceber quais mecanismos de proteção o legislador tem elegido/pensado para tutelar os

dados pessoais. Após, realçam-se as estratégias tradicionais de consentimento individual, opção de exclusão e anonimização utilizadas na atualidade para proteção dos dados pessoais a fim de constatar a sua aptidão para uma efetiva proteção frente ao *big data*. Ao final ofertam-se as conclusões.

Elucida-se que, por ser uma pesquisa bibliográfica com revisão de literatura, a fim de embasar o tema desenvolvido, o referencial teórico ao qual se recorreu é composto por teóricos que argumentam acerca da proteção dos dados pessoais, dos direitos à personalidade, à privacidade e *big data*. Além disso, examina-se a legislação brasileira, especialmente a Constituição Federal de 1988, o Código Civil de 2002, o Código de Defesa do Consumidor, Marco Civil da Internet (Lei 12.965/2014) e os projetos de lei específica sobre a matéria, bem como articula-se o discurso legal com o judicial destacando o entendimento do Supremo Tribunal Federal, por meio da sua jurisprudência, acerca do *habeas data* e do Superior Tribunal de Justiça.

A fim de alcançar os resultados pretendidos, utilizou-se o método dedutivo, visto que a pesquisa tem a finalidade de explicar o conteúdo das ideias expostas, partindo de uma concepção geral para uma especifica, de um viés filosófico para viés técnico na configuração do *big data*, com atenção aos riscos para a privacidade, por meio do tratamento de dados pessoais tornado possível a partir dessa nova tecnologia, bem como na delimitação do direito à proteção de dados pessoais como direito fundamental, por meio dos documentos internacionais, percorrendo as gerações de leis de proteção de dados, para, ao fim, estabelecer a proteção jurídica conferida pelo ordenamento jurídico brasileiro.

A abordagem metodológica utilizada foi a qualitativa que permite o emprego de "[...] diferentes concepções filosóficas; estratégias de investigação; e métodos de coleta, análise e interpretação dos dados"[10]. Em relação ao objeto, a pesquisa foi do tipo bibliográfico-documental. A pesquisa bibliográfica foi utilizada para obtenção de dados em livros, revistas e sites de internet especializados no tema; e a pesquisa documental foi feita através da jurisprudência do Supremo Tribunal Federal e tribunais superiores para a construção de um referencial teórico que constitui um debate inserido na produção do texto argumentativo em torno da temática contemplada.

[10] CRESWELL, J. W. **Projeto de pesquisa**: método qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010, p. 206.

O procedimento de coleta de dados baseou-se na obtenção, na catalogação e na análise de documentos públicos em sua origem, tais como iniciativas legislativas e decisões judiciais de tribunais brasileiros e internacionais, a fim de subsidiar o discurso científico e examinar a concretização do discurso normativo.

Por fim, destaca-se que o presente trabalho está vinculado à linha de pesquisa “direitos humanos, novas tecnologias e desenvolvimento sustentável” por compreender a análise das novas tecnologias e suas repercussões, com foco nos direitos da personalidade e a promoção dos direitos humanos, e foi financiado com bolsa pelo Programa de Suporte à Pós-Graduação de Instituições de Ensino Particulares/ PROSUP-CAPES.

2 INTRODUZINDO O *BIG DATA* COMO FENÔMENO DA SOCIEDADE DE CONTROLE

No presente capítulo, apresenta-se o *big data* no contexto da sociedade de controle, através do pensamento do filósofo Gilles Deleuze, como desdobramento da sociedade disciplinar objeto dos estudos de Michel Foucault, para, assim, situar os bancos de dados automatizados como projeto arquitetônico de vigilância pós-moderno. Adiante, são esclarecidos os conceitos de dados pessoais, informação e bancos de dados por representarem categorias conceituais recorrentes durante todo o texto. Após, traz-se uma definição mais técnica do *big data* correlacionando com suas principais características que auxiliam sua compreensão. Por fim, abordam-se os valores científico, econômico e social do *big data*, refletidos nos bens e serviços tornados possíveis por essa nova tecnologia, articulando com os riscos à privacidade intrínsecos ao processo de coleta, tratamento e uso de dados pessoais.

2.1 BANCO DE DADOS AUTOMATIZADOS: A VERSÃO “CIBERESPACIAL” DO PANÓPTICO NA SOCIEDADE DE CONTROLE

A revolução nos meios de produção, aliada ao progresso da tecnologia, desencadearam a formação de uma nova sociedade que passou a se organizar de maneira distinta, por exemplo, com a difusão da internet, as relações sociais tomaram outros espaços, agora virtuais, e a sociedade passou a conviver em rede[11].

Com a investida tecnológica, surgem, a todo instante, redes sociais que exigem interação. Pessoas ficam cada vez mais reféns de seus *smartphones* e seus aplicativos, que revelam o perfil de consumidor graças ao uso constante do cartão de crédito seja em estabelecimentos físicos ou em lojas virtuais. É imprescindível manter-se conectado. A vida passa a concentrar-se na velocidade intransponível e

[11] O termo “rede” aqui suscitado refere-se às redes sociotécnicas que o filósofo Rogério Costa, professor da PUC-SP, descreve como: “[...] água, transportes, comércio, telecomunicação, telefonia, comunicação, TV, jornal, computação, *web*, portáteis. Estamos dentro de muitas redes simultaneamente e permanentemente. [...] Na cidade digital, em casa ou no trabalho, pelo fato de essas redes estarem interconectadas, podemos acessar múltiplos serviços sem a necessidade de nos deslocarmos. Temos entrega de produtos, pagamentos tipo *homebanking*, serviços públicos, trabalho e muitas outras coisas possíveis pelo fato de que a cidade está digitalizada” (COSTA, Rogério da. Sociedade de controle. **São Paulo Perspec.** São Paulo, v. 18, n. 1, p. 161-167, mar. 2004. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-88392004000100019&lng=pt&nrm=iso>. Acesso em 10 jun. 2016, p. 166, excluímos).

incessante em uma sociedade na qual ficar fora dos bancos de dados significa não existir como sujeito, tudo isso tornado possível mediante a relação entre tecnologia e economia, pois,

> [...] são os fatores econômicos que têm produzido a construção de infovias de um mercado globalizado, para que o resultado de processos sociais de construção dos conteúdos da Internet devam ser acondicionados em uma formatação comercializável, em uma caixa preta (software, ou demais dispositivos), que, em embalagens de fantasia e atraente estímulo de segredos de conhecimentos sofisticados de gestão operacional proveja as necessidades de uns e o lucro de outros[12].

A internet conferiu certa notoriedade a cada indivíduo, que antes dela muitas vezes era invisível, e tornou "[...] tangível e irrefutável o ser e o estar no mundo"[13]. Isso explica a facilidade que cada sujeito tem em dispor suas informações pessoais, seja para sentir-se notado, seja para adquirir bens e serviços. O fator econômico, que se sobressai na sociedade capitalista, é uma das molas propulsoras que alimentam os bancos de dados automatizados e que fazem com que grandes corporações estejam cada vez mais interessadas em se apropriar das novas tecnologias como as análises de *big data*, o que, em contrapartida, demanda pensar na proteção jurídica dos dados pessoais.

Adepta das novas tecnologias, a sociedade acabou por concebê-las como instrumentos ora bons, ora ruins, mas sempre em sua neutralidade, e eficácia e nunca como arma que domina e destrói, o que se denota, até então, uma relação de dependência. Isto porque o indivíduo, por meio das tecnologias, desenvolve mecanismos que buscam facilitar sua vida, significando dizer que as inovações tecnológicas têm valor para a sociedade, seja ele econômico, social ou científico.[14]

De antemão, cabe destacar aqui que não se percebe uma recusa da tecnologia, mas sim a intenção de, a partir do exame dos usos e seus efeitos, situar como suas inovações podem conviver, ou melhor, adaptar-se à máxima eficiência dos bens e serviços que oferecem, sem ultrapassar as barreiras que protegem a privacidade do indivíduo na sua condição de usuário e membro-usuário da nova sociedade, que pode ser exemplificada a partir da passagem do mundo analógico

---

[12] RUARO, Regina Linden; MOLINARO, Carlos Alberto. Acoplamento entre internet e sociedade. **Revista da AGU**, Brasília-DF, ano XIII, n. 40, abr./jun. 2014, p. 47.
[13] BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2014, p. 88.
[14] ECO, Umberto. **Apocalípticos e integrados**. São Paulo: Perspectiva, 2001.

para o digital tratado por Paula Sibilia que, para exemplificar o impulso massificante e individualizante[15] da sociedade industrial, cita a "carteira de identidade", considerando que,

> Tal documento faz referência a um Estado-nação, contém um número que localiza o indivíduo dentro da massa, uma foto, uma assinatura e uma impressão do dedo polegar. Todos dados analógicos. De outro lado, o sujeito da sociedade contemporânea detém cada vez mais cartões de crédito e senhas de acesso: dispositivos digitais. De maneira crescente, a identificação do consumidor pelo perfil: uma série de dados sobre a condição socioeconômica, seus hábitos e suas preferências de consumo, colhidos através de formulários de pesquisas e processados digitalmente, para serem armazenados em bancos de dados conectados em rede que serão acessados, vendidos, comprados e utilizados pelas empresas em suas estratégias de marketing.[16]

No cenário das novas tecnologias, a partir da criação dos bancos de dados automatizados, nas quais as informações disponibilizadas em rede são colhidas e armazenadas pelas grandes empresas, na maioria das vezes sem a autorização do usuário, ou até que se admitam casos em que há expresso consentimento, ainda assim sem o conhecimento[17] acerca dos usos secundários que serão feitos dos dados disponibilizados, surge o *big data*. Essa nova tecnologia consiste em análises que correlacionam os dados armazenados dos indivíduos e revelam informações pessoais em uma quantidade e velocidade jamais vistas. Não há mais tempo para descanso e tranquilidade, mas apenas a constante precaução ao mover-se na era em que os dados, as informações adquirem valor supremo.

Nesse contexto, percebe-se que os bancos de dados automatizados aliados às análises de *big data* revelam uma forma de controle e vigilância dos

---

[15] Paula Sibilia explica que "[...] na sociedade contemporânea, tanto a noção de massa quanto a de indivíduo estão perdendo força. No lugar dessas figuras, outras emergem. O papel do consumidor, por exemplo, assume uma relevância cada vez maior. Em vez de integrar uma massa - como os cidadãos dos Estados-nação da era industrial - ele faz parte de diversas amostras, nichos de mercado, segmentos de público, *target*s e bancos de dados." (SIBILIA, Paula. **O homem pós-orgânico:** o corpo, subjetividade e tecnologias digitais. Rio de Janeiro: Relume Dumará, 2002, p. 34)

[16] SIBILIA, Paula. op. cit., 2002, p. 34.

[17] Uma pesquisa publicada na Harvard Business *Review* Brasil em fevereiro de 2016 aponta que as pessoas, apesar de terem pleno conhecimento de que suas informações pessoais são coletadas pelas empresas com que mantêm relação, surpreendem-se com a falta de informação quanto aos tipos específicos de dados que fornecem; a pesquisa aponta que, das pessoas entrevistadas, 27% percebem que compartilham a sua lista de amigos em redes sociais, 25% que compartilham a sua localização, 23% suas buscas na *web*, 18% seus históricos de comunicação como "chat logs", 17% seus endereços de IP e 14% percebem que compartilham seu histórico de navegação na *web*. (MOREY, Timothy; FORBATH, Theodore; SCHOOP, Alisson, Dados dos consumidores: modelos de transparência e confiança. **Harvard Business Review Brasil,** São Paulo, fevereiro 2016, p. 47)

indivíduos, pelos seus gestores, sobre toda a sociedade, a qual, diariamente, vê captadas informações pessoais a partir da simples conexão à internet. Assim, para melhor situar a discussão a cerca do que constitui o *big data* e a necessidade de uma efetiva proteção jurídica aos dados pessoais no cenário das novas tecnologias, cabe examinar a transição das sociedades disciplinares para as sociedades de controle. Esta última posicionada como receptora da nova tecnologia, sendo os grandes bancos de dados automatizados como o seu novo Panóptico[18], em uma metáfora à construção de Jeremy Bertham utilizado por Michel Foucault para descrever as relações de poder nas sociedades disciplinares.

2.1.1 Da Sociedade Disciplinar para a Sociedade de Controle: a Vigilância Constante

Para compreender a inserção e atuação das novas tecnologias, especificamente do *big data,* na nova sociedade incitada pelos impulsos tecnocráticos que seguiram o pós-guerra, é indispensável considerar dois filósofos que acreditavam na evolução do pensamento por meio de crises: Gilles Deleuze e Michel Foucault. O primeiro interlocutor do pensamento do segundo, dando um prosseguimento às ideias do outro. Enquanto Foucault debruçou-se sobre a chamada sociedade disciplinar, Deleuze introduziu o que chama de sociedade de controle[19], marcando a transição da primeira para a segunda, quando afirma que

[18] Foucault (2010) explica a arquitetura do panóptico que atribui a Bentham; segundo o autor, consiste "[...] na periferia uma construção em anel; no centro, uma torre: esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível. O dispositivo panóptico organiza unidades espaciais que permitem ver sem parar e reconhecer imediatamente. Em suma, o princípio da masmorra é invertido; ou antes, de suas três funções – trancar, privar de luz e esconder – só se conserva a primeira e suprimem-se as outras duas. A plena luz e olhar de um vigia captam melhor que a sombra, que finalmente protegia. A visibilidade é uma armadilha" (FOUCAULT, op. cit.2010, p. 190).

[19] Deleuze explica, ao referir-se à sociedade de controle, que o termo "controle" foi proposto por Burroughs para designar o novo monstro e que Foucault reconhece como o futuro próximo; menciona ainda outro autor que também analisa as formas de controle que funcionam como substitutas das antigas disciplinas, referenciando Paul Virilio (DELEUZE, G. *Post-scriptum* sobre as sociedades de controle. In: _____. **Conversações (1972-1990).** São Paulo: Ed. 34, 1992, p. 224).

“[...] são as *sociedades de controle* que estão substituindo as sociedades disciplinares”[20].

Não é objetivo de Deleuze retratar o futuro com ficção, mas, diagnosticar o presente lançando uma nova imagem do pensamento sobre a contemporaneidade. Para ele as sociedades de controle surgem como desdobramento das sociedades de soberania e disciplinares demonstradas do século XVII ao início do XX, por Foucault.

Para Braga e Vlach “[...] devemos entender a sociedade de controle como aquela (que se desenvolve nos limites da modernidade e se abre para a pós-modernidade)”[21]. Nesse interim, Silvana Tótora afirma que “[...] no capitalismo pós-industrial, os próprios homens são peças constitutivas da máquina e não seus meros usuários; são partes de uma engrenagem de circulação de informação”[22].

No seu texto *Post-Scriptum sobre as Sociedades de Controle*, Gilles Deleuze, aparentemente, faz com que o leitor imagine uma ficção científica. No entanto não é essa sua intenção, por isso esclarece não haver necessidade de ficção científica “[...] para se conceber um mecanismo de controle que dê, a cada instante, a posição de um elemento em espaço aberto, animal sem reserva, homem numa empresa (coleira eletrônica)”[23].

Nas chamadas sociedades disciplinares, imperava o espaço fechado da disciplina dos corpos, a fim de torná-los dóceis. Por esse motivo “[...] forma-se então uma política das coerções que são um trabalho sobre o corpo, uma manipulação calculada de seus elementos, de seus gestos, de seus comportamentos”[24]. A disciplina está associada aos espaços fechados aos quais o individuo está submetido e deles migra constantemente, “[...] primeiro a família, depois a escola [...], depois a caserna [...], depois a fábrica, de vez em quando o hospital, eventualmente a prisão, que é o meio de confinamento por excelência”[25].

---

[20] DELEUZE, op. cit.1992, p. 224.
[21] BRAGA, S.;VLACH, V. Os usos políticos da tecnologia, o biopoder e a sociedade de controle: considerações preliminares. **Scripta Nova. Revista electrónica de geografía y ciencias sociales.** Barcelona: Universidad de Barcelona, 1 de agosto de 2004, vol. VIII, núm. 170(42). Disponível em: <http://www.ub.es/geocrit/sn/sn-170-42.htm>. Acesso em 5 maio 2016, n.p.
[22] TÓTORA, Silvana. Democracia e sociedade de controle. **Verve**, 10: 237-261, 2006, p. 239. Disponível em: <http://revistas.pucsp.br/index.php/verve/article/viewFile/5441/3888>. Acesso em 15 maio 2016.
[23] DELEUZE, op. cit.,1992, p. 228-229.
[24] FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. 38. ed. Petrópolis (RJ): Vozes, 2010, p. 133.
[25] DELEUZE, op. cit., 1992, p. 223; suprimimos.

Denota-se que na sociedade disciplinar a vigilância adquire um aspecto determinante para o encarceramento que isola o olhar. Abre-se espaço para a impossibilidade de se escapar ao olhar do outro, em razão das aberturas que vazam os interiores e colocam o individuo em uma situação de constante observação[26].

De uma sociedade para outra, o homem passa de confinado para endividado[27]. Endividado, porque nas sociedades de controle os homens estão submetidos a um controle contínuo, sem delimitação de início, meio e fim, num processo modificado a todo instante.

As diferenças entre sociedades de disciplina e sociedades de controle são estabelecidas por Deleuze como sendo característico da primeira o constante recomeço, fosse ele da escola à caserna, da caserna à fábrica, enquanto que na segunda, nunca se termina nada. Menciona que "[...] as sociedades disciplinares têm dois polos: a assinatura que indica o *indivíduo*, e o número de matrícula que indica sua posição numa *massa*"[28], diferente do que ocorre nas sociedades de controle, nas quais "[...] a linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição"[29].

Nas sociedades de controle, o indivíduo tem suas informações registradas a partir de uma cifra que, como uma senha, fornece acesso a todas as informações. Isto é possível em detrimento da geração de informação cibernética e computadorizada visto que, "[...] as máquinas da informática e os computadores não são apenas evoluções tecnológicas, mas operam uma mutação no capitalismo"[30]. As tecnologias detectam a posição de cada um, lícita ou ilicitamente, e operam uma modulação universal, através do controle contínuo e da comunicação instantânea[31].

Considerando os elementos e configuração da sociedade de controle, percebe-se que esta tem "[...] como valores máximos de mercadoria o prestígio, a informação, o conhecimento e como dispersão máxima a força de trabalho"[32]. É na

---

[26] CHEVITARESE, Leandro; PEDRO, Rosa Maria Leite Ribeiro. Da sociedade disciplinar à sociedade de controle: a questão da liberdade por uma alegoria de Franz Kafka, em O Processo, e de Phillip Dick, em Minority Report. **Estudos de Sociologia. Rev. do Prog de Pós-graduação em Sociologia da UFPE**, v. 8, n. 12. 2002, pp. 129-162.
[27] DELEUZE, op. cit., 1992, pp. 223-230.
[28] DELEUZE, op. cit., 1992, p. 226; destaque no original.
[29] DELEUZE, op. cit.,1992, p. 226.
[30] BRAGA; VLACH, op. cit., 2004, n.p.
[31] DELEUZE, op. cit., 1992, pp. 223-230.
[32] NEVES, Cláudia E. Abbês Baêta. Sociedade de Controle, o neoliberalismo e os efeitos de subjetivação. In: SILVA, André do et al. (Org.). **Subjetividade:** questões contemporâneas. São Paulo: Hucitec, 1997, p. 87.

sociedade de controle que “os indivíduos tornaram-se ‘*dividuais*’”, divisíveis, e as massas tornaram-se amostras, dados, mercados ou *bancos*”[33].

Acredita-se que a nova caracterização do indivíduo deve-se principalmente às máquinas que operam a sociedade de controle, notadamente as máquinas de informática e computadores, nas quais operam e imperam a comunicação virtual e o controle de dados pessoais como forma de vigilância. Quanto às sociedades que se sucederam na história, atribuem-se a elas diferentes máquinas que, respectivamente, as fizeram operar, como exemplo, para as sociedades de soberania estavam as máquinas simples, alavancas, relógios; para as sociedades disciplinares as máquinas energéticas[34].

A partir do endividamento do individuo, que se encontra submetido a um controle contínuo, no qual imperam os computadores e a informática, tornando os sujeitos seres divisíveis, torna possível perceber a permanência da “vigilância”, a mesma retratada por Foucault em sua obra *Vigiar e Punir*[35], com a figura do Panóptico, de enorme valor ao poder disciplinar, cujo efeito mais importante era “[...] induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder”[36].

Figura 01 - Figura retratando o modelo panóptico

Fonte: TRINDADE, 2014[37]

[33] DELEUZE, op. cit., 1992, p. 226; destaque no original.
[34] DELEUZE, op. cit., 1992, pp. 223-230.
[35] FOUCAULT, op. cit., 2010.
[36] FOUCAULT, op. cit., 2010, p. 191.
[37] TRINDADE, Rafael. **Foucault** – panóptico [ou, “a visibilidade é uma armadilha”], 2014. Disponível em: < https://goo.gl/images/baOdKf>. Acesso em: 18 jan. 2017.

Para estabelecer a relação entre o Panóptico de Jeremy Bentham, utilizado por Foucault, com os bancos de dados, Bauman[38] recorre a um ensaio de Mark Poster que trata os bancos de dados eletrônicos como uma versão ciberespacial atualizada do Panóptico, nos quais os indivíduos seriam fisgados dentro das redes, dos bancos de dados, sem poder apresentar qualquer resistência. Estaríamos, pois, diante do "superpanóptico", mas com uma diferença "[...] os vigiados, fornecendo os dados a armazenar, são fatores primordiais – e *voluntários* – da vigilância"[39].

Ao traçar a diferença entre o Panóptico e os bancos de dados, Bauman[40] afirma que o primeiro tem como função primordial evitar que qualquer pessoa escape do espaço estritamente vigiado, enquanto que o segundo tem como principal função garantir que nenhum indivíduo entre nos bancos de dados sob falsas alegações ou sem credibilidade. O autor associa o fato de que os bancos de dados representam uma possibilidade de conferir ao individuo certa credibilidade, haja vista que são criados e geridos por empresas que têm interesses em traçar o perfil do indivíduo como consumidor, bom-consumidor, adiantando aqui o cadastro positivo que será abordado no item 4.4 deste trabalho.

Os bancos de dados automatizados, aliados às análises de *big data,* possibilitam que a prisão dos indivíduos dispense um lugar fixo e fechado, pois permitem que, em qualquer lugar, seja aberto ou fechado, todos estejam sob controle pela vigilância daqueles que rastreiam os passos, correlacionando dados. Um dos maiores exemplos que confirmam esta assertiva é o acesso às informações do *Global Positioning System* (GPS), as quais descrevem as rotas e lugares mais frequentados pelas pessoas, a ponto de identificar o trabalho, a residência, a escola dos filhos, entre outros lugares.

Para demonstrar como os bancos de dados automatizados representam o novo Panóptico na sociedade de controle, basta observar o projeto americano *Total Terrorism Information Awareness (TIA),* cujo objetivo é colher o máximo de informações pessoais acessando registros financeiros, médicos, de comunicação, viagens, entre outros, associando todas essas informações e criando um grande banco de dados, virtual e centralizado. Através desse banco de dados, o projeto

---

[38] BAUMAN, Zygmunt. **Globalização:** as consequências humanas. Rio de Janeiro: Jorge Zahar Ed., 1999.
[39] BAUMAN, op. cit., 1999, p. 58; destaque no original.
[40] BAUMAN, Zygmunt. op. cit., 1999.

poderá rastrear os indivíduos para detectar suas atividades potenciais. Com isso, percebe-se que "[...] o reconhecimento de padrões está diretamente ligado à mudança nos métodos de controle das ações individuais"[41].

O projeto americano *TIA* é um exemplo claro de inovação, tornado possível devido à tecnologia do *big data*. Com isso, é imperioso observar que há um valor intrínseco em cada banco de dados, muitas vezes oculto, pois, como expõem Viktor Mayer-Schonberger e Kenneth Cukier[42], desde o século XX os dados são o petróleo da economia da informação. Isto justifica a corrida para descobrir e captar esse valor intrínseco, abrindo espaço para violações à privacidade dos indivíduos, quando nestes bancos de dados estão presentes dados pessoais. No contexto do *big data,* as máquinas acabam por possibilitar a criação de modelos estatísticos onde se encaixam aos dados, otimizam-nos e os preveem[43].

Ao tratar do modelo Panóptico do poder moderno concebido por Michel Foucault, Zygmunt Bauman[44] esclarece que esse projeto arquitetônico de vigilância tinha como propósito manipular e rearrumar a transparência do espaço como relação social, e até como relação de poder. Isto porque os internos estavam em total situação de visibilidade e os supervisores em toda invisibilidade, fazendo com que os primeiros se comportassem como se estivessem em constante vigilância.

Retratando a vigilância como disfarçada de serviçal da segurança, David Lyon, em diálogo travado com Bauman, problematiza a questão do panóptico pós-moderno, a partir do contexto que insere:

> Os olhos eletrônicos sempre abertos nas ruas, a coleta de dados abrangente, os fluxos de informações pessoais com sua pressão cada vez mais alta são vistos como reações racionais aos riscos da vida. Precisamos desesperadamente de vozes que perguntem: "Por quê?" "Para quê?" "Você tem alguma ideia das consequências disso tudo?" Eu fico atento, esperando ouvir alguém dizer: "Haveria outras maneiras de conceber o que há de errado com o mundo, e como seus males poderiam ser abordados?"[45]

A partir das provocações de David Lyon, ainda que não se tenham respostas prontas - e essa sequer seria a melhor saída, face à dinamicidade dos fenômenos tecnológicos - o "por quê?", "para quê?" e "quais as consequências?" da utilização

---

[41] COSTA, op. cit.. 2004, p. 165.
[42] MAYER-SCHONBERGER; CUKIER, op. cit., 2013.
[43] DAVENPORT, Thomas H.. **Big data no trabalho:** derrubando mitos e descobrindo oportunidades. Tradução Cristina Yamagami. Rio de Janeiro: Elsevier, 2014.
[44] BAUMAN, op. cit., 1999.
[45] BAUMAN, op. cit., 2014, p. 79-80.

das novas tecnologias, como o *big data,* fica evidente a necessidade da discussão sobre uma efetiva proteção jurídica aos dados pessoais, a fim de que seja possível refletir acerca de como se tem constituído a nova vigilância na sociedade de controle, a partir das tecnologias da informação e, analisando os instrumentos jurídicos disponíveis, seja possível averiguar como podem ser garantidas a preservação da liberdade do individuo e sua autonomia em relação aos seus dados pessoais, sem obstar o avanço tecnológico, na conjuntura da sociedade da informação que segundo Manuel Castells, organiza

> "[...] seu sistema produtivo em torno de princípios de maximização da produtividade baseada em conhecimentos, por intermédio do desenvolvimento e da difusão de tecnologias da informação e pelo atendimento dos pré-requisitos para sua utilização (principalmente recursos humanos e infra-estrutura de comunicações)."[46]

Ante o exposto, resta concluir que Foucault ilumina as conexões entre o Panóptico e a modernidade, em que as figuras da punição e reforma das práticas disciplinares no discurso pós-moderno, evidenciado por Bauman, tomam outra proporção, abrindo espaço para a vigilância como punição, e a prática disciplinar rompe as barreiras dos espaços confinados ao que, anteriormente, estava restrita a figura do panóptico, para adotar uma nova roupagem: a vigilância eletrônica, na qual os detalhes pessoais da vida dos indivíduos passam a circular fora no seu controle para dentro de bancos de dados remotos e automatizados que representam uma espécie de versão "ciberespacial" do Panóptico, que tem sua concretização arquitetônica, a exemplo, a partir dos *data centers*[47] do *Google*. Com isso fica estabelecido que o indivíduo está inserido na sociedade de controle, movido pela difusão da tecnologia que em decorrência da sociedade da informação.

2.2 DADO PESSOAL, INFORMAÇÃO E BANCO DE DADOS: CONCEITOS E DISTINÇÕES

Com a evolução tecnológica evidenciada, principalmente pela informática, tem-se buscado, cada vez mais assegurar a proteção dos direitos à privacidade e à inviolabilidade dos dados pessoais, face ao crescente número de usuários da

---

[46] CASTELLS, Manuel. **A sociedade em rede.** 9. ed. São Paulo: Paz e Terra, 2006, p. 268.

[47] Para fazer um tour em um dos principais *data centers* do provedor *Google*, que fica em The Dalles acesse: <http://exame.abril.com.br/tecnologia/noticias/conheca-o-data-center-do-google-que-nem-funcionarios-entram> Acesso em 10 maio 2016.

internet e os riscos a que estão expostos. A versão “ciberespacial” do Panóptico concebida na sociedade de controle materializada através dos grandes bancos de dados automatizados - *big data* – evidencia uma forma de controle e vigilância do indivíduo que convive na sociedade da informação, e, consequentemente, torna vulneráveis os dados pessoais. Urge, portanto, esclarecer os conceitos e as peculiaridades pertinentes acerca de dados pessoais, informação e banco de dados.

Segundo a lei federal alemã de proteção de dados, os dados pessoais são informações específicas sobre as circunstâncias pessoais ou materiais de uma pessoa singular identificada ou identificável[48]. Nesse sentido, a Diretiva Europeia 95/46/CE, no seu art. 2º, acrescenta que um indivíduo pode ser identificável ao ser associado “[...] a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”. O atual Regulamento Geral da União Europeia 2016/679 sobre proteção de dados pessoais, que substituiu a mencionada Diretiva 95/46/CE, no seu art. 4º, item 1[49], acrescenta que uma pessoa pode ser identificada também a partir dos seus dados de localização e identificadores por via eletrônica. Neste sentido, dados pessoais consistem em informações aptas a revelar aspectos físicos, psíquicos ou sociais do indivíduo, capaz de distingui-los dos demais.

A definição de dado pessoal pode ser exemplificada a partir de alguns casos julgados pelo Tribunal da União Europeia, como no caso *Lindquist*, no qual o Tribunal decidiu que o nome de uma pessoa, em conjunto com seu número de telefone e informações sobre suas condições de trabalho ou *hobbies,* constituem dados pessoais[50]. Ainda é conveniente citar o caso *Worten*, em que se firmou o entendimento de que os dados constantes em registros de trabalho, em relação a

---

[48] § 3º (1) GERMAN PARLIAMENT. **Federal Data Protection Act**. (***Bundesdatenschutzgesetz*** (BDSG)). [s.d.] [on line] Disponível em: <http://www.bfd.bund.de>. Acesso em 20 jan. 2017.

[49] “‘Dados pessoais’, informação relativa 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 por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.” (UNIÃO EUROPEIA. **Regulamento (EU) 2016/679**, 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 17 dez. 2016).

[50] LAUDATI, Laraine. **Summaries of EU Court decisions relating to data protection 2000-2015**. OLAF Data Protection Officer, 28 January, 2016, p. 6. Disponível em: <https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf>. Acesso em 20 jan. 2017.

cada trabalhador, do qual constem o período diário de trabalho e de descanso, também constituem dados pessoais, porque tratam de informações relativas a uma pessoa singular identificada ou identificável[51].

Existem ainda outras categorias de dados, são eles: dados sensíveis e dados anônimos. Os primeiros referem-se a dados cujo armazenamento, processamento e circulação, podem acarretar maior risco à personalidade do indivíduo, podendo inclusive serem utilizados para fins discriminatórios, por estarem no rol exemplificativo desses dados aqueles que se referem a origem racial, saúde, vida sexual e condenações penais[52]. Enquanto que os dados anônimos, segundo Laura Schertel Mendes se referem a pessoas indeterminadas e podem ser utilizados para fins estatísticos, tendo como finalidade proteger a pessoa por meio do anonimato[53]. Nesse sentido a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002[54], relativa à privacidade e às comunicações eletrônicas exige o anonimato dos dados (art. 6º, I), inclusive ao tratar sobre o processamento de dados de localização dispõe que estes dados somente poderão ser tratados se forem tornados anônimos ou com consentimento daqueles a que se refiram (art. 9º, I).

Quando se fala de informação, mister se faz diferenciar informação pessoal de outras informações. A primeira se difere das outras ao passo que possui um vínculo objetivo com a pessoa, tendo em vista que acaba por revelar aspectos que lhe dizem respeito.[55] Inobstante o caráter revelador dos dados pessoais acerca de aspectos da personalidade do indivíduo, oportunizando a sua identificação, merece destacar a abordagem de Laura Schertel Mendes, para quem "[...] fundamental é perceber que tal tutela [jurídica] visa à proteção da pessoa e de sua personalidade e não dos dados *per se*"[56].

Cabe, assim, diferenciar os termos "dado" e "informação". O primeiro seria revestido de um caráter mais primitivo, fragmentado, uma informação em estado

---

[51] LAUDATI, op. cit., 2016, p. 24
[52] MENDES, op. cit., 2014.
[53] MENDES, op. cit., 2014.
[54] PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Directiva 2002/58/CE**, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF >. Acesso em 21 jan. 2017.
[55] DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 157.
[56] MENDES, op. cit., 2014, p. 56.

potencial de “pré-informação”. Como a informação representa algo além do que está contido no dado, pressupõe uma fase inicial de depuração de seu conteúdo, carrega um sentido instrumental, e, em certos contextos, chega a representar diversas ordens de valores – direito à informação, liberdade de informação[57].

Há categorias de informações que, propriamente dizendo, não têm relação com a pessoa, porém, dentre essas características situa-se a informação pessoal. Ela acentua a existência de um vínculo objetivo significando que a informação se refere às características ou ações da pessoa em particular, que podem ser atribuídas a ela em conformidade com a lei[58]. Danilo Doneda[59] concorda com Pierre Catala, que identifica uma informação pessoal quando o objeto da informação é a própria pessoa:

> [...] o Conselho Europeu, por meio da Convenção de Strasbourg, de 1981, ofereceu uma definição que condiz com essa ordem conceitual. Nela, informação pessoal é “qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação.” É explícito, portanto, o mecanismo pelo qual é possível caracterizar uma determinada informação como pessoal: o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta. [Convenção nº 108 – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, art. 2º]

Uma equação que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa pode servir para explicar como a proteção das informações pessoais ganhou espaço no ordenamento jurídico brasileiro, como um desdobramento da tutela do direito à privacidade[60].

Estabelecido o conceito de dados pessoais, passa-se a configurar “banco de dados”. Este se “[...] caracteriza por ser um conjunto organizado e lógico de dados, de fácil utilização e acesso”[61], podendo ainda ser tecnicamente definido como “[...] um conjunto de arquivos relacionados entre si, dividindo a mesma relação geral de contexto, pois as entidades e eventos descritos são geralmente comuns a todos os arquivos em questão”[62].

---

[57] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico** Journal of Law, Joaçaba-SC, v. 12, n. 2, p. 91-108, jul./dez. 2011.
[58] DONEDA,op. cit., 2011.
[59] DONEDA, op. cit., 2011, p. 94.
[60] DONEDA, op. cit., 2011.
[61] MENDES, op. cit., 2014, p. 58.
[62] VERZELLO, Robert J.; REUTTER III, John. **Processamento de dados**. Tradução Regina Szwarcfiter, Heraldo Luiz Marin. São Paulo: McGraw-Hill do Brasil, 1984.

O Regulamento Geral da União Europeia, nº 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[6364] conceitua banco de dados como "[...] qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico [...]", reiterando os mesmos termos utilizados pela Diretiva Europeia revogada (art. 2º, "c").

Na leitura de Bertram Antônio Sturmer[65], banco de dados consiste na reunião de informações sobre uma pessoa, independentemente de sua finalidade ser determinada ou não. Para o autor, os bancos de dados podem ser organizados de formas distintas, seja através de fichas manuais ou por meio de processamento eletrônico. Situando como definição fundamental do que seja banco de dados, Danilo Doneda refere a estes como "[...] um conjunto de informações estruturado de

[63] No tocante à revogação da Diretiva Europeia 95/46/CE que dispunha sobre proteção de dados pessoais, o Regulamento dispõe no item 171 o seguinte: "A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento. Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor. Se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento. As decisões da Comissão que tenham sido adotadas e as autorizações que tenham sido emitidas pelas autoridades de controlo, com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas." (PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Regulamento UE 2016/679,** de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), n.p. Disponível em: <http://www.privacy-regulation.eu/pt/r171.htm>. Acesso em: 21 jan. 2017)

[64] "A diretiva é um dos instrumentos jurídicos ao dispor das instituições europeias para a aplicação das políticas da União Europeia (UE). Trata-se de um instrumento flexível utilizado principalmente como meio de harmonizar as legislações nacionais. Exige que os países da UE alcancem um determinado resultado, deixando-lhes a competência quanto à forma de o fazer. [...] O artigo 288º do Tratado sobre o Funcionamento da União Europeia estabelece que a diretiva vincula os países aos quais se destina (um, vários ou todos) quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. Contudo, a diretiva é diferente do regulamento ou da decisão. Ao contrário do que acontece com o regulamento, que é imediatamente aplicável na ordem jurídica interna dos países da UE após a sua entrada em vigor, a diretiva não é diretamente aplicável nos países da UE. Para que governos, empresas e particulares possam recorrer a uma diretiva, esta deve ter sido objeto de transposição para o direito nacional." Para saber mais sobre Diretivas Europeias sugere-se visita ao Portal EUR-Lex que dá acesso à legislação da União Europeia através do link: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=URISERV%3Al14527>. Acesso em 20 jan. 2017.

[65] STÜRMER, Bertram Antônio. Banco de dados e "habeas data" no código do consumidor. **Revista de Direito do Consumidor,** vol. 1, p. 55-94, Jan – Mar/1992.

acordo com determinada lógica - e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível"[66].

Os bancos de dados representam uma nova definição dos poderes e direitos a respeito das informações pessoais, logo, sobre a própria pessoa[67]. Hoje são comuns devido às consequências da evolução tecnológica mais especificamente o advento dos computadores para o tratamento dos dados pessoais, que realizaram a transição da informação dispersa para organizada, tendo como resultado uma maior maleabilidade e utilização.

Cabe, assim, mencionar que no art. 5º, LXXII da Constituição Federal de 1988 (CF88) que prevê a garantia constitucional do *habeas data* que se presta a "[...] assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público"[68]. O Código de Defesa do Consumidor (CDC)[69], no seu art. 43, § 4°, trata de banco de dados relativo a consumidores, atribuindo a este caráter público. Novamente vê-se a menção expressa ao atributo da "publicidade", ao que se vê indispensável, segundo a legislação, significando que somente serão tutelados os dados pessoais que estejam depositados em bancos de dados de caráter público.

Ao tratar da proteção aos dados pessoais pelo *habeas data* e o Código de Defesa do Consumidor, Temis Limberger[70] afirma que, tanto um quanto o outro representam uma proteção jurídica fragilizada. Argumenta, do ponto de vista da aplicabilidade da norma, que tal fragilidade é percebida quando o indivíduo está diante de uma entidade de caráter privado e não se estabelece uma relação de consumo.

Em contraponto, cabe destacar a concepção do professor José Afonso da Silva[71] de que qualquer banco ou registro de dados pessoais deve ser entendido como público, independente de ser regido por órgão estatal ou privado, tendo em vista que os dados armazenados representam a pessoa na sociedade, motivo pelo

---

[66] DONEDA, op. cit., 2011, p. 92.
[67] DONEDA, op. cit., 2011.
[68] BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.
[69] BRASIL. **Lei 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < http://www.casadoempresario.org.br/wp-content/uploads/2013/04/CDC.pdf>. Acesso em: 20 jan. 2017.
[70] LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 189.
[71] SILVA, José Afonso da. **Curso de direito constitucional positivo.** 35. ed. São Paulo: Malheiros, 2012, p. 457-458.

qual somente não será considerado público aqueles cadastros utilizados para fins pessoais e domésticos. Logo, não haveria que se falar em fragilidade na proteção jurídica pelo *habeas data* ou CDC.

Assim como Laura Schertel Mendes[72], há de se entender que esta concepção é a mais adequada em face da efetividade do direito à privacidade numa sociedade da informação. Como não há uma legislação nacional própria, ressalte-se que tal interpretação coaduna com um dos paradigmas contidos no art. 2º, item 2, alínea c, do Regulamento Geral da União Europeia 2016/679 sobre proteção de dados pessoais.

Assim, cabe dizer que a proteção de dados do cidadão antecede a proteção de dados do consumidor[73]. Isto porque a proteção ao cidadão é mais ampla, posto que "consumidor" é um atributo do indivíduo que se encontra numa relação de consumo. A proteção de dados pessoais do indivíduo, na condição de cidadão demanda do direito que garanta a inviolabilidade da sua intimidade e vida privada, a fim de que ao sujeito seja assegurado mover-se com liberdade e dignidade na sociedade da informação, com prevalência da dignidade humana, fundamento no qual se funda o Estado Democrático de Direito (art. 1º, III, da Constituição Federal de 1988). Este fundamento foi "nacionalizado" tendo como parâmetro o modelo jurídico europeu.

A Constituição Alemã de 1949 que também no art. 1º dispõe que "[...] a dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público [...]" e no art. 2º que "[...] todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral [...]"[74]. O constitucionalismo lusitano 1976, inegavelmente influenciado pelo alemão de 1949, menciona logo no seu artigo primeiro do texto da atual Constituição da República Portuguesa que "Portugal é uma República soberana, baseada na dignidade da

[72] MENDES, op. cit., 2014, p. 184.
[73] Para um estudo aprofundado sobre a proteção de dados pessoais do consumidor ler: OLIVA, Afonso Carvalho de. **O direito fundamental à proteção de dados pessoais do consumidor brasileiro:** do código de defesa do consumidor ao caso "score". Dissertação (Mestrado em Direitos Humanos). Aracaju, SE: Universidade Tiradentes, 2016.
[74] ALEMANHA, **Lei Fundamental da República Federal da Alemanha**, 1919, atualizada até 2011. Disponível em: <http://www.brasil.diplo.de/contentblob/3160404/Daten/1330556/Gundgesetz_pt.pdf>. Acesso em 04 fev. 2017, p. 18.

pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária"[75].

No mesmo sentido a Espanha por meio de sua Constituição de 1978 no título I que trata dos direitos e deveres fundamentais, especificamente no art. 10 situam entre os fundamentos da ordem política e da paz social: a dignidade da pessoa humana e o livre desenvolvimento da personalidade[76]. A Constituição Política da Colômbia de 1991 influenciada pelo direito europeu adota a dignidade humana como um dos fundamentos do Estado Social de Direito, como se reconhece (art. 1º), assegurando no rol dos direitos fundamentais o direito à intimidade pessoal e familiar, bem como de conhecer, atualizar e retificar as informações sobre sua pessoa que estejam em bancos de dados públicos ou privados (art. 15º)[77].

2.3 O *BIG DATA* E SUA INFLUÊNCIA NO TRATAMENTO E ARMAZENAMENTO DE DADOS PESSOAIS

Os avanços dos investimentos nas tecnologias de informação, a criação da rede mundial de computadores e todas as tecnologias digitais fizeram com que as informações encontrassem maior propulsão para circularem e se desenvolverem. Consequentemente, com esse novo cenário da sociedade da informação, novas tecnologias surgiram com o intuito de modernizar e amparar as necessidades humanas, e, uma delas repousa na elaboração de ideias e criação de bens e serviços, a partir da correlação de dados que se encontram em grandes bancos de dados, ou seja, o *big data*.

A impressionante velocidade da escalada tecnológica, desta vez, ditou uma tendência em tecnologia que está abrindo caminho para um novo método de compreensão do mundo, o *big data*[78]. Bilhões de consumidores deixam rastros

---

[75] PORTUGAL, **Constituição da República Portuguesa**, 1976, VII Revisão Constitucional [2005], n.p. Disponível em: <http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 04 fev. 2017.

[76] ESPANHA. **Constituição Espanhola.** 29 de dezembro de 1978. Madrid, 1978. Disponível em: <http://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Acesso em: 21 jan. 2017.

[77] COLOMBIA, **Constitución Política de Colombia**. Actualizada con los Actos Legislativos a 2015. Disponível em: <http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia%20-%202015.pdf>. Acesso em 22 jan. 2017.

[78] HENRIQUES, Daniela Aparecida; COSTA, Helder Rodrigues. ***Big data*** – como utilizar a extraordinária quantidade de informações coletadas por novas tecnologias para obter vantagens

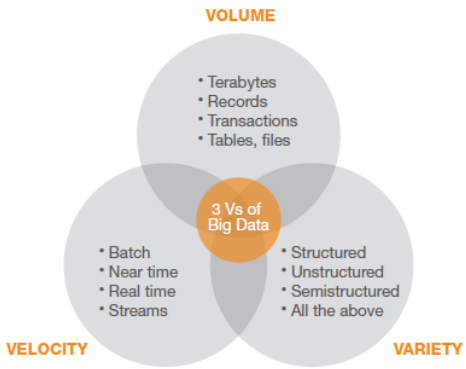
digitais ao fazerem pesquisas no *Google*, editar comentários em redes sociais, acessar vídeos no *YouTube* ou utilizar o GPS do automóvel. Esses dados estão gerando um imenso banco de dados, denominado *big data*[79].

2.3.1 Big Data: afinal, o que é?

O termo *big data* foi cunhado pelas ciências como a astronomia e a genômica, que vivenciaram uma explosão nos anos 2000, e atualmente tem migrado para todos os campos do conhecimento humano. Ainda não se tem uma definição rigorosa para o termo. Considerando as suas características, Viktor Mayer-Schonberger e Kenneth Cukier[80] concebem o *big data* como um conjunto de tendências tecnológicas que consiste em uma abordagem que aplica a matemática a enorme quantidade de dados a fim de prever probabilidades, permitindo analisar muito mais dados, sem observar o rigor da exatidão, buscando descobrir novos padrões e correlações nos dados que propiciam novas e valiosas ideias.

Ao falar sobre *big data*, a quantidade dos dados importa, mas não é tudo. Assim explica Philip Russom[81] ao considerar que outras características do *big data,* as quais são imprescindíveis para definir essa nova tecnologia, referindo-se a: *volume, velocidade e variedade*, os três Vs, ressaltando que cada característica possui suas ramificações, conforme se analisa na figura a seguir.

Figura 02 - Características que definem o *big data*



Fonte: RUSSOM, 2011, p. 6[82].

---

competitivas. Disponível em: <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a72.pdf> Acesso em 25 abr. 2016.

[79] FEIJÓ, Bruno Vieira. A revolução dos dados. **Revista Exame PME – Pequenas e Médias Empresas**, São Paulo, p. 30-43, set. 2013.

[80] MAYER-SCHONBERGER; CUKIER, op. cit., 2013.

[81] RUSSOM, Philip. **Big data analytics.** Renton: TDWI Research, 2011.

[82] RUSSOM, 2011, op. cit., p. 6.

O principal atributo do *big data* é o *volume*[83] de dados que está envolvido nas análises feitas por meio dessa tecnologia, razão pela qual a maioria das pessoas costuma definir *big data* em *terabytes* e às vezes *petabytes.* Explica Philip Russom[84] que o *big data* não é só quantificado pelo volume dos dados, mas também por contagem de registros, transações, tabelas ou arquivos. Isto porque, muitas vezes, nem todos os dados coletados para armazenamento serão necessariamente coletados para análise. Além disso, em razão do enorme volume de dados envolvidos que leva a dificuldade de uma quantificação, a definição de *big data* acaba por não se restringir apenas ao volume de dados, representando assim, uma das suas características que, aliada a outras, conseguem defini-lo com maior propriedade. Para melhor compreender esse volume de dados no qual se insere o *big data*, Philip Chen e Chun-Yang Zhang descrevem que:

> Na era da informação, quase todas as grandes empresas encontram problemas com Big Data, especialmente as corporações multinacionais. Por um lado, essas empresas, em sua maioria, têm um grande número de clientes em todo o mundo. Por outro lado, há grande volume e velocidade de transação de dados. Por exemplo, o sistema de detecção de fraude de cartão de crédito Falcon da FICO gerencia mais de 2,1 bilhões de contas válidas em todo o mundo. Há acima de 3 bilhões de pedaços de conteúdo gerados no Facebook todos os dias. O mesmo problema acontece em todas as empresas de Internet. A lista poderia continuar, como nós testemunhamos os campos futuros da batalha dos negócios que focalizam em Big Data.[85]

Sabendo que o *big data* foi criado para analisar grande *volume* de dados, seu grande diferencial está explicado na segunda característica que é a maior *variedade* das fontes (*web,* mídias sociais, aparelhos eletrônicos, entre outros) utilizadas para

---

[83] "The thing about Big Data and data *volumes* is that the language has changed. Aggregation that used to be measured in petabytes (PB) is now referenced by a term that sounds as if it's from a Star Wars movie: zettabytes (ZB). A zettabyte is a trillion gigabytes (GB), or a billion terabytes!" (ZIKOPOULOS et al., op. cit., 2012, p. 9). Disponível em: <http://www.dotgroup.co.uk/wp-content/uploads/2014/11/Harness-the-Power-of-Big-Data-The-IBM-Big-Data-Platform.pdf>. Acesso em 20 dez. 2016.

[84] RUSSOM, op. cit., 2011.

[85] "In the era of information, almost every big company encounters Big Data problems, especially for multinational corporations. On the one hand, those companies mostly have a large number of customers around the world. On the other hand, there are very large volume and velocity of their transaction data. For instance, FICO's falcon credit card fraud detection system manages over 2.1 billion valid accounts around the world. There are above 3 billion pieces of content generated on Facebook every day. The same problem happens in every Internet companies. The list could go on and on, as we witness the future businesses battle fields focusing on Big Data." (CHEN, C.L, Philip; ZANG, Chun-Yang. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, ***Inform. Sci.***, v. 275, 10 ago. 2014, p. 3, traduzimos. Disponível em: <http://dx.doi.org/10.1016/j.ins.2014.01.015>. Acesso em: 15 jan. 2017).

coletar todo tipo de informação, seja pessoal ou não. Com a variedade das fontes, os usuários de *big data,* as corporações, passaram a não simplesmente acumular os dados coletados, como analisá-los para extrair e direcionar bens e serviços, o *big data* trouxe para as corporações uma mudança significativa:

> As poucas organizações que têm vindo a analisar estes dados agora o fazem a um nível mais complexo e sofisticado. O big data não é novo, mas o alavancamento analítico efetivo do big data é. A recente exploração dessas fontes para análise significa que os dados chamados estruturados (que anteriormente possuíam hegemonia incontestada na análise) agora são associados por dados estruturados (texto e linguagem humana) e dados semiestruturados (XML, *feeds* RSS). Há também dados que é difícil de categorizar, como os de áudio, vídeo e outros dispositivos[86].

A *variedade* como característica do *big data* refere-se, portanto, à capacidade de capturar todos os dados necessários para a tomada de decisões, independente de onde esteja, incluindo assim opiniões no *Facebook*, imagens e outros, dados estruturados, semiestruturados ou não estruturados[87], que Zikopoulos et al. esclarecem que "[...] todos os dados têm alguma estrutura, quando nos referimos a dados não estruturados, estamos nos referindo aos subcomponentes que não têm estrutura, como o texto de forma livre em um campo de comentários."[88]

Aliado ao *volume* dos dados e à *variedade* das fontes de coleta, a *velocidade* com que são gerados, entregues e processados os dados é o terceiro atributo do *big data.* A *velocidade* torna possível a análise de todo o fluxo de dados coletados num fluxo contínuo onde há necessidade de dar sentido aos dados e, ao mesmo tempo, tomar decisões em tempo real[89]. Essa característica é também definida como "[...] a taxa na qual os dados chegam à empresa e são processados ou bem

---

[86] "The few organizations that have been analyzing this data now do so at a more complex and sophisticated level. Big data isn't new, but the effective analytical leveraging of big data is. The recent tapping of these sources for analytics means that so-called structured data (which previously held unchallenged hegemony in analytics) is now joined by unstructured data (text and human language) and semistructured data (XML, RSS feeds). There's also data that's hard to categorize, as it comes from audio, video, and other devices." (RUSSOM, op. cit., 2011, p. 7; traduzimos).

[87] Sobre a definição de dados estruturados e desestruturados, Judith Hurwitz et al. explicam que os primeiros, "[...] se referem a dados que possuem um formato e comprimento definido. Exemplos de dados estruturados incluem números, datas e grupos de palavras e números chamados *strings* (por exemplo, o nome de um cliente, endereço e assim por diante)", enquanto que os dados desestruturados "são dados que não seguem um formato específico. [...] São, realmente, a maioria dos dados, [...] até recentemente a tecnologia não suportava fazer sua manipulação, exceto amarzená-los ou analisa-los manualmente." (HURWITZ, Judith et al. **Big data for dummies.** Rio de Janeiro, Alta Books, 2015, p. 26, 29)

[88] "To clarify, all data has some structure; when we refer to unstructured data, we are referring to the subcomponents that don't have structure, such as the freeform text in a comments field or the image in an auto-dated picture." (ZIKOPOULOS, et al, op. cit., 2012, p. 10; traduzimos).

[89] RUSSOM, op. cit., 2011.

compreendidos [...]"[90], a velocidade está intimamente ligada à vantagem e à eficiência, quanto mais rápido se entendem os dados, mais vantagem adquire-se no mercado competitivo entre as empresas, e torna possível chegar a uma análise eficiente.

As características de *big data* não ficam restritas aos três Vs, anteriormente abordados. Outros autores como Zikopoulos et al.[91] dizem que o *big data* caracteriza-se por cinco aspectos: *volume, velocidade, variedade, veracidade, valor*.

A *veracidade,* segundo Zikopoulos et al., acaba sendo sinônimo de qualidade e confiabilidade dos dados, fazendo com que as análises de *big data* possam oferecer *insights* confiáveis. O *valor* da nova tecnologia está na vantagem competitiva que as análises de *big data* podem conferir às empresas duas vezes mais chances de ultrapassar seus concorrentes na indústria (segundo resultados de um estudo chamado *The New Intelligent Enterprise* realizado pelo *Institute of Business Value* em parceria com o *Sloan Management Review* do *Massachusetts Institute of Technology (*MIT)[92]*.*

Ainda sobre o conceito de *big data,* Thomas Davenport, afirma que:

> [...] big data é um termo genérico para dados que não podem ser contidos nos repositórios usuais; refere-se a dados volumosos demais para caber em um único servidor; não estruturados demais para se adequar a um banco de dados organizado em linhas e colunas; ou fluidos demais para serem armazenados em uma data *warehouse* estático. Embora o termo enfatize seu tamanho, o aspecto mais complicado do big data, na verdade, evolve sua falta de estrutura.[93]

Como visto, o *big data* é um grande volume de dados que permite sua coleta, tratamento, armazenamento e reutilização dos dados, inclusive, dados pessoais sendo que a mudança de escala leva a uma mudança de estado. São tantos os dados e de variáveis características que podem não parecer informações pessoais explícitas, mas que, correlacionados, reordenados ou reidentificados[94], após os processos de análises com o *big data*, podem facilmente dizer a quem se referem ou levar ao conhecimento de detalhes íntimos da vida de uma pessoa.

---

[90] "We define velocity as the rate at which data arrives at the enterprise and is processed or well understood." (ZIKOPOULOS et al., op. cit 2012, p. 10; traduzimos).
[91] ZIKOPOULOS, op. cit., 2014.
[92] ZIKOPOULOS, et al., op. cit., 2012.
[93] DAVENPORT, op. cit., 2014, p. 1.
[94] O processo de reidentificação refere-se ao processo de análise e tratamento de dados anônimos que, a partir das análises de *big data,* podem revelar informações pessoais, este assunto é abordado adiante nos itens 4.7 e 4.8.

2.3.2 O Valor, os riscos e oportunidades

Dois fatos podem constituir a premissa deste tópico. O primeiro foi em 2009, quando o vírus H1N1 assolou o mundo. O *Google* conseguiu, a partir da combinação de centenas de bilhões de termos de busca, identificar o surgimento de um surto de gripe, de forma precisa, em tempo real gerando respostas mais rápidas e eficientes a órgãos oficiais como a Organização Mundial de Saúde (OMS), enquanto que os Centros de Controle e Prevenção de Doenças, em meio à pandemia, estavam sempre defasados em uma ou duas semanas em relação aos dados sobre os novos casos emitidos pelos médicos. O outro foi pela Lei de Etzioni. Através de uma análise da variação de preços das passagens aéreas, pode-se prever o melhor dia e horário para realizar a compra de um bilhete aéreo com o menor custo, dando assim um significativo poder econômico para o consumidor. É nítido que o *big data* é uma ferramenta que, em si, dita novas maneiras de agir, e interfere diretamente na compreensão e reestruturação da sociedade[95], isso porque esse fenômeno sociotécnico em questão está interligado à mudança de escala dos bancos de dados que aumentam a cada dia.

É inquestionável que a internet provocou mudanças radicais ao acrescentar a comunicação aos computadores. Nessa mesma perspectiva, o *big data* mudará aspectos fundamentais da vida ao lhe dar uma dimensão quantitativa que ela jamais teve[96]. Uma razão evidente que confirma tal assertiva é o valor científico e social da nova tecnologia, bem como sua representação como nova fonte de valor econômico e inovação.

Considerando que a finalidade do *big data* está em analisar volume de dados para convertê-los em conhecimento, inovação e valor[97]. A partir de sua abordagem que busca interpretar grande quantidade de dados para extrair novas ideias, é inegável que traga consigo um avanço para diversos setores, dos negócios, às ciências e saúde, governo, educação, e todos os demais setores da sociedade que possam dele se apropriar.

Contudo, o valor da informação não se encontra somente em um propósito (hipoteticamente) primário, com vistas a resultar somente em benefícios para os

[95] MAYER-SCHONBERGER; CUKIER, op. cit., 2013.
[96] MAYER-SCHONBERGER; CUKIER, op. cit., 2013.
[97] DAVENPORT, op. cit., 2014.

indivíduos. A partir das análises de *big data,* as informações depositadas nos bancos de dados passam a ter usos secundários. Essas análises referem-se ao processo de correlações dos dados que acaba por revelar informações pessoais, seja o comportamento do indivíduo como consumidor, suas condições de saúde e até atividades ilegais. Em linhas gerais, o *big data* busca desvendar para as empresas, o comportamento, preferências e aversões dos indivíduos, estes na condição de cliente-consumidor, a fim de possibilitar uma maior segmentação de anúncios, produtos e serviços com base nesse conhecimento[98].

Os riscos, portanto, passam a residir na capacidade de captação de dados pessoais[99], assim como na utilização dos dados coletados e armazenados pelo *big data*, que, explicitamente, podem não parecer dados pessoais, mas implicitamente são quando submetidos às análises do *big data* que correlacionam os dados coletados fazendo com que estes transmitam informações pessoais sobre os indivíduos. Assim, une-se a informação coletada, e confere-se valor à informação para propósitos secundários. Diante todo o processo de captação dos dados e correlação, os indivíduos não podem consentir ou optar por não conceder suas informações, pois sequer sabem com exatidão quais os seus dados estão sendo coletados e para quais fins estão sendo destinados os usos secundários.

As oportunidades de *big data* centram-se, em sua maioria, em produtos, serviços e clientes. Davenport lista inúmeras empresas e exemplos que evidenciam essas oportunidades:

> Por exemplo, Reid Hoffman, cofundador e presidente do conselho do LinkedIn, montou, com seus cientistas de dados, uma equipe de linha de produto que desenvolveu funcionalidades como “Pessoas que talvez você conheça”, “Grupos que podem ser de seu interesse”, “Vagas que podem ser de seu interesse”, “Quem viu seu perfil”, entre várias outras. A GE se concentra no big data principalmente para melhorar seus serviços e já está usando a ciência de dados para otimizar os contratos de serviço e os intervalos de manutenção para seus produtos industriais. A Google, é claro – a empresa suprema do big data -, usa os cientistas de dados para refinar seus algoritmos centrais de busca e anúncios. A Zynga usa cientistas de dados para orientar o desenvolvimento de games e produtos relacionados com

[98] DAVENPORT, op. cit., 2014.

[99] “A *Google* coleta praticamente todos os dados que puder sobre os clientes e seu comportamento e às vezes, coleta dados que não deveria. Um bom exemplo disso foi o projeto de mapeamento do *Google StreetView*, que também coletou dados de redes *wi-fi* não criptografadas ao passar pelas cidades. Essas empresas têm recursos suficientes para se darem ao luxo de coletar dados sem qualquer propósito em vista - embora elas pudessem ter ainda mais sucesso se pensassem na finalidade antes da coleta dos dados.” (DAVENPORT, op. cit., 2014, p. 165)

> os clientes. A Netflix criou o famoso Netflix Prize para a equipe de cientistas de dados que conseguisse otimizar mais as recomendações de filmes para os clientes[100].

O que as empresas e grandes corporações, que fazem uso das análises de *big data,* têm em comum? Além de ter facilmente à sua disposição os meios de criação de bens e serviços, têm o "conhecimento sobre o conhecimento", ou seja, a partir das análises de *big data* elas sabem como encontrar, coletar e correlacionar, para, então, direcionar seus bens e serviços aos seus clientes. Todas essas vantagens na era da informação são tão importantes quanto saber quais são as informações.

Na conjuntura da sociedade da informação em que as liberdades individuais são colocadas em risco em razão do surgimento das novas tecnologias, o direito não pode se omitir a esse cenário, como ensina o eminente professor Antonio Enrique Pérez Luño,

> En un mundo interdependiente, en el seno de sociedades interconectadas, la garantía de los derechos cívicos, se halla en directa conexión, para bien o para mal, con los processos que definem su instalación tecnológica. El estudio actual de los derechos humanos no puede omitir esa referencia contextual, ni puede abdicar del juicio crítico de sus implicaciones. Se trata de lograr que los desarrollos tecnológicos no menoscaben ni se alcancen a costa de las libertades cívicas. Por ello, las reflexiones interdisciplinarias tendentes a estabelecer un diálogo fluido entre el universo tecnológico y la esfera de los derechos de los ciudadanos se han hecho cada vez más perentorias[101].

Por essas razões, diante do valor científico, social e econômico do *big data*, assim como os riscos que recaem sobre os dados no processo de coleta, tratamento e usos desses dados, emerge a necessidade de se discutir a efetividade da proteção jurídica dos dados pessoais como forma de resguardar a privacidade, indispensável no contexto das novas tecnologias, tema objeto do próximo capítulo.

---

[100] DAVENPORT, op. cit., 2014, p. 15.
[101] PÉREZ LUÑO, A-E. **La terceira generación de derechos humanos**. Cizur Menor (Navarra): Thomson-Aranzadi, 2006, p. 89.

3 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DESDOBRAMENTO DO DIREITO À PRIVACIDADE

Resta ausente na jurisprudência e na doutrina um conceito unitário adequado para o termo “privacidade”[102]. Muitas vezes pela confusão entre inúmeros assuntos como liberdade de pensamento, controle sobre informações pessoais, proteção da reputação, desenvolvimento da personalidade, autodeterminação informativa, entre outros, que acabam sendo manejados de diferentes formas por diversos doutrinadores na tentativa de conceituar “privacidade”, resultando em conceitos ora abrangentes ora restritivos[103].

Embora seja difícil, ou praticamente impossível atribuir o conceito mais adequado a “privacidade”, Marcel Leonardi concebe os conceitos unitários deste termo enquadrando em quatro categorias: a) o direito a ser deixado só (*the right to bel et alone*); b) o resguardo contra interferências alheias; c) segredo ou sigilo; d) controle sobre informações e dados pessoais[104]. Importa para o presente estudo especialmente a última categoria, a qual, conforme se verifica a seguir, representa um desdobramento do direito à privacidade, configurando-se como o direito fundamental à proteção de dados pessoais.

3.1 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Nesta seção, apresenta-se o direito à proteção de dados pessoais como direito fundamental a partir do conceito materialmente aberto dos direitos fundamentais com suporte na doutrina de Sarlet[105]. Sustenta-se, pois, na premissa de que o direito à proteção de dados pessoais é um direito autônomo, que se desdobra do direito à privacidade, distinguindo ainda as nomenclaturas direito à proteção de dados pessoais e autodeterminação informativa, esta última utilizada primordialmente na Europa. Por fim, analisam-se os documentos internacionais dos quais se extrai o direito à proteção de dados pessoais.

---

[102] LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011, p. 49.
[103] LEONARDI, op. cit., 2011.
[104] Sobre os conceitos unitários de privacidade analisados por Marcel Leonardi ver: LEONARDI, 2011.
[105] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

3.1.1 Proteção de Dados Pessoais e Autodeterminação Informativa: o *Status* de Fundamentalidade

A proteção de dados pessoais está intimamente ligada a liberdade e dignidade pessoais, e adquire papel indispensável para o desenvolvimento da personalidade, conforme ensina o professor Stefano Rodotà "a proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio[106]".

A doutrina brasileira ao tratar da proteção de dados pessoais insere a questão como uma continuidade da disciplina da privacidade, atualizando-a e impondo características próprias. Nesse sentido, Danilo Doneda ensina que por meio do direito à proteção de dados pessoais "garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente"[107], acrescenta que:

> [...] a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada a esta, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento jurídico brasileiro[108].

Marcel Leonardi acrescenta que o direito à proteção de dados pessoais "tem como enfoque as informações e dados sobre os quais o indivíduo quer exercer controle"[109]. A proteção dos dados pessoais exige a compreensão da dupla dimensão de sua tutela, fundada na liberdade e na igualdade. Além do controle do indivíduo sobre as suas próprias informações, a tutela abarca o combate à discriminação passível de ocorrer em razão das informações sensíveis extraídas dos bancos de dados[110].

Delimitado o conceito do direito à proteção de dados pessoais, antes de avançar a configuração deste direito como fundamental, cabe destacar que o

---

[106] RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17.
[107] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico** Journal of Law, Joaçaba-SC, v. 12, n. 2, p. 91-108, jul./dez. 2011 p. 95.
[108] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006, p. 326.
[109] LEONARDI, op. cit., 2011, p. 75.
[110] MENDES, L. S. F. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Dissertação (Mestrado em Direito). Brasília, DF: Universidade de Brasília, 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em 01 dez. 2016.

presente trabalho adota a concepção de direitos fundamentais[111] de Robert Alexy, segundo o qual,

> "[...] Os direitos fundamentais personificam "também um ordenamento de valores objetivo". [...] os direitos fundamentais têm não só o caráter de regras, mas também de princípios. [...] os valores jurídico-fundamentais ou princípios valem não somente para a relação entre o estado e o cidadão, mas muito além disso "para todos os âmbitos do direito".[112]

Esta noção de direitos fundamentais coaduna-se com as lições de Ingo Wolfgang Sarlet, no sentido de que em razão da maior participação ativa da sociedade, os bens jurídicos fundamentais assegurados pela ordem constitucional - e tendo como foco neste trabalho a privacidade e liberdades individuais - passaram a demandar proteção não só contra ameaças do Estado, como também de contra os mais fortes no âmbito da sociedade, pessoas físicas ou jurídicas, oriundas da esfera privada[113].

À luz do direito constitucional pátrio, Sarlet defende um sistema de direitos fundamentais aberto e flexível, sendo insustentável a concepção, segundo a qual "[...] os direitos fundamentais formam um sistema em separado e fechado da Constituição [...]"[114]. Pugna, pois, por um conceito materialmente aberto de direitos fundamentais consagrado pelo art. 5º, § 2º, da CF88, que reconhece a existência de direitos fundamentais: a) positivados em outros trechos da Constituição, b) integrantes de tratados internacionais, c) não-escritos, ou seja, implícitos na Constituição, d) decorrentes do regime de princípios da Constituição. Adota este trabalho o conceito de Sarlet, para o qual,

---

[111] O trabalho adota a concepção de direitos fundamentais de Robert Alexy porque desenvolve a construção teórica defendida por Ingo Wolfganga Sarlet no tocante ao sistema de direitos fundamentais aberto e flexível, e que o próprio Sarlet ao conceituar direitos fundamentais refere-se a Robert Alexy, mencionando que "importa considerar, ainda, que uma conceituação de cunho genérico e universal somente parece viável, à medida que propositalmente aberta, de modo a permitir a sua permanente adaptação à luz do direito constitucional positivo. Assim sendo, poderíamos propor a seguinte definição, baseada - importa ressaltá-lo - no conceito de Robert Alexy, mas que não deixa de considerar a abertura material consagrada expressamente pelo direito constitucional positivo pátrio." (SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2011, p. 77)

[112] ALEXY, Robert. Direitos fundamentais, ponderação e racionalidade. **Revista de Direito Privado,** vol. 24, out - dez, 2005, p. 335.

[113] SARLET, Ingo Wolfgang. Direitos fundamentais e direito privado: algumas considerações em torno da vinculação dos particulares aos direitos fundamentais, **Revista de Direito do Consumidor**, vol. 36, out - dez, 2000, p. 54 - 104.

[114] SARLET, op. cit., 2011, p. 71.

> Direitos fundamentais são, portanto, todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo pátrio, foram, por seu conteúdo e importância (fundamentalidade formal), bem como as que, por seu conteúdo e significado, possam lhes ser equiparados, agregando-se à Constituição material, tendo, ou não, assento na Constituição formal (aqui considerada a abertura material do Catálogo).[115]

A Constituição Federal de 1988 não prevê taxativamente, no rol dos direitos fundamentais o direito à proteção de dados pessoais ou autodeterminação informativa. Não utilizou qualquer dessas nomenclaturas ao tratar dos direitos da personalidade, especialmente no que se refere aos dados pessoais do indivíduo. Inobstante isto, a Constituição Federal de 1988 reconhece a dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito (art. 1º, III), garantindo ao indivíduo a inviolabilidade da sua intimidade, vida privada, honra, imagem, sigilo da correspondência e das comunicações telegráficas, e dados e comunicações telefônicas (art. 5º, X, XII). A par do Texto Constitucional, a fim de subsidiar o argumento de que há possibilidade de se admitir a existência do direito fundamental à proteção de dados pessoais, Augusto Tavares Rosa Marcacini opina que

> [...] quando se fala no direito à privacidade de dados, cumpre destacar duas situações distintas. Pela primeira, dados estão sendo transmitidos estabelecendo uma forma de comunicação por redes públicas ou privadas; esta goza de larga proteção constitucional, insculpida no inciso XII, do art. 5º de nossa carta. Estes dados transmitidos não podem ser licitamente interceptados, nem mesmo mediante autorização judicial. Uma vez armazenados os dados transmitidos, esta informação passa a ser considerada uma informação fixa, caso em que deixa de incidir o inciso XII. Igualmente, sobre bancos de dados em geral, informatizados ou não, não se pode falar da aplicação de referida norma. Entretanto, uma vez que contenham informações e dados de caráter pessoal, esses bancos de dados são também sigilosos e merecem proteção legal e judicial, à luz do inciso X [...]. Apesar de se atribuir a mesma qualidade de inviolável a estes direitos, intimidade, vida privada, honra e imagem são expressões de larga amplitude, de modo que podem por vezes conflitar com outros direitos e garantias. Por esta razão, aplicado a critério da proporcionalidade, os bancos de dados estão protegidos por um sigilo relativo, não imune à ordem da autoridade judicial.[116]

---

[115] SARLET, op. cit., 2011, p. 77.

[116] MARCACINI, Augusto Tavares Rosa **Direito e informática**: uma abordagem jurídica sobre criptografia, São Paulo: Forense, 2002, p. 146.

Logo, o direito à proteção de dados pessoais, apesar de não estar formalmente previsto no texto, há de ser reconhecido como direito fundamental implícito e/ou decorrente, com base no seu conteúdo, como desdobramento do direito à privacidade - formalmente incorporado à Constituição Federal, com respaldo na inviolabilidade da intimidade e vida privada (art. 5º, X, CF88) - e por sua importância acentuada, nas palavras do professor José Afonso da Silva:

> o intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.[117]

A importância do tema remete a 1995 quando a jurisprudência do Superior Tribunal de Justiça já decidia no Recurso Especial 22.337 que:

> [...] a inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.[118]

---

[117] SILVA, José Afonso da. **Curso de direito constitucional positivo**. 29. ed. São Paulo: Malheiros, 2008, p. 209-210.

[118] BRASIL, Superior Tribunal de Justiça, **Recurso Especial 22.337-RS**. Inserção de dados pessoais do cidadão em bancos de informações. Relator: Ministro Rui Rosado de Aguiar Júnior. Turma Julgadora: Quarta Turma. Data do julgamento: 13 de fevereiro de 1995; publicação: DJ 20/03/1995a, p. 1. Disponível em: < https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Acesso em 15 jan. 2017.

Sobre o reconhecimento deste direito no ordenamento jurídico brasileiro, questionou Ricardo Villas Bôas Cueva[119] "há um direito à autodeterminação informativa no Brasil?". O autor conclui que sim, com a ressalva da ausência de disposição normativa que robusteça tal direito. Sendo assim, resta imprescindível esclarecer o que essas nomenclaturas representam, bem como, a que mais se amolda ao ordenamento jurídico brasileiro[120].

Preceitua Ricardo Villas Bôas Cueva[121] que o direito à autodeterminação informativa consiste na faculdade de o indivíduo decidir por si só sobre a exibição e o uso de seus dados pessoais (levando-se em conta, obviamente, outros bens jurídicos tutelados, por meio da aplicação do postulado da proporcionalidade). Para J.J. Gomes Canotilho e Vital Moreira[122] esse direito se desenrola em vários direitos: a) o direito de acesso; b) o direito ao conhecimento da identidade dos responsáveis pela guarda, bem como o direito aos esclarecimentos sobre a finalidade dos dados; c) o direito de contestação/retificação dos dados; d) o direito de atualização; e) direito à eliminação dos dados cujo registro é interdito.

A autodeterminação informativa como um direito fundamental de defesa e de prevenção incide no poder de disposição e de controle por parte do indivíduo que legitima o recolhimento, utilização, exibição e eliminação dos seus dados pessoais, exigindo um consentimento inequívoco, livre e informado, como condição de licitude das atividades de captação e utilização dos seus dados pessoais por terceiros, estabelecendo-se como uma liberdade e poder de determinação e autotutela quanto às suas informações pessoais, podendo acionar a qualquer tempo quem houver utilizado indevidamente seus dados.

Na doutrina brasileira há quem opine pela existência de um direito à proteção de dados pessoais[123] ou de um direito à autodeterminação informativa[124]. Inobstante

---

[119] CUEVA, R. V. B. Há um direito a autodeterminação informativa no Brasil? In: MUSSI, J.; SALOMÃO, L. F.; MAIA FILHO, N. N. (Org.). **Estudos jurídicos em homenagem ao Ministro Cesar Asfor Rocha**. Ribeirão Preto: Migalhas, 2012.

[120] Ver também CUNHA E CRUZ, Marco Aurélio Rodrigues da; SOUSA, Jéffson Menezes de; COSTA, C. . Proteção de dados pessoais ou autodeterminação informativa no Brasil?. In: OLIVEIRA, Rafael Santos de; SILVA, Rosane Leal da. (Org.). **Direito e novas mídias**. Curitiba: Ithala, 2015, p. 179-193.

[121] CUEVA, op. cit., 2012.

[122] CANOTILHO, J.J; MOREIRA, V. **Constituição da República Portuguesa anotada**. 4. ed., vol. I. Coimbra: Coimbra Editora, 2007.

[123] BARRIENTOS-PARRA, J. D.; BORGES MELO, E. C. O Direito à intimidade na sociedade técnica: rumo a uma política pública em matéria de tratamento de dados pessoais. **Revista de Informação Legislativa**, ano 45, v. 180, p. 197-214, out./dez. 2008. DONEDA, D., op. cit., 2011. GEDIEL, J. A. P; CORRÊA, A. E. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado.

isso, na leitura de alguns autores não há uma distinção clara entre as duas expressões, razão pela qual se recorre à distinção técnico-jurídica realizada por dois autores espanhóis.

Antonio Enrique Pérez Luño[125] aposta na metamorfose do direito à intimidade para incluir a proteção de dados pessoais em seu âmbito de proteção. Advoga que o conceito de intimidade emergiu do filosófico foro interno, intrassubjetivo, estático, da interioridade ao foro externo, dinâmico, prático, da alteridade, respeitadas suas implicações intersubjetivas. À delimitação conceitual do direito à intimidade, antes referido como a faculdade de se isolar, adicionou-se, portanto, o poder de controle sobre as informações/dados pessoais. Tal dilatação conceitual conecta-se à capacidade de interação da pessoa humana, assumindo esta uma postura de sujeito socializado, que não renuncia, igualmente, à sua individualidade.

Pablo Lucas Murillo de la Cueva afirma que o direito à autodeterminação informativa se constrói a partir da noção de intimidade[126], mas é autônomo em relação a esta, por ser um novo direito fundamental que inclui a proteção de dados pessoais. Defende o tratamento diferenciado desses dois direitos, para que os problemas específicos que suscitam a informática invoquem a defesa jurídica dos dados pessoais desde uma posição de independência sistemática com relação a outros perfis da intimidade[127].

Revista da Faculdade de Direito (UFPR), Curitiba, v. 47, p. 141-153, 2008. REINALDO FILHO, D. A privacidade na sociedade da informação. In: REINALDO FILHO D. (Coord.). **Direito da Informática, temas polêmicos**. Bauru, SP: Edipro, 2002, p. 25-40. RUARO, R., RODRIGUEZ, D., FINGER, B. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito da UFPR**, n° 53, p. 45-66, 2011. Disponível em: <http://ojs.c3sl.ufpr.br/ojs2/index.php/direito/article/view/30768/19876>. Acesso em: 20 de mar. 2016.

[124] CARVALHO, A. P. G. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de direito do consumidor** (RT), ano 12, n. 46, p. 77-119, abril/jun. 2003. CUEVA, op. cit., 2012, v.3, p. 220-241. NAVARRO, A. M. N. P. O direito fundamental à autodeterminação Informativa. In: NASPOLINI SANCHES, S. H D. F.; DUARTE, F.; ALENCAR, M. L. P. (Coord.). CONPEDI/UFF. (Org.). Direitos fundamentais e democracia II. CONGRESSO NACIONAL DO CONPEDI, XXI. **Anais....** FUNJAB, 2012, p. 429-458. SOUZA, V. R. C. O acesso à informação na legislação brasileira. **Revista da Seção Judiciária do Rio de Janeiro**, v. 19, p. 161-181, 2011.

[125] PÉREZ LUÑO, A-E. Informática y libertad: Comentario al artículo 18.4 de la Constitución. **Revista de estudios políticos**, nº 24, p. 31-54, 1981; PÉREZ LUÑO, A-E. **Derechos Humanos, Estado de Derecho y Constitución**. Madrid: Tecnos, 2005; PÉRE LUÑO, A-E. La protección de los datos personales del menor en internet. **Anuario Facultad de Derecho** (Universidad de Alcalá), n 2, p. 143-175, 2009.

[126] MURILLO DE LA CUEVA, P. L. **El derecho a la autodeterminación informativa**. Tecnos: Madrid, 1990, p. 25.

[127] MURILLO DE LA CUEVA, P. L. La primera jurisprudencia sobre el derecho a la autodeterminación informativa.**Datospersonales.org**: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, ISSN-e 1988-1797, Nº. 1, 2003. Disponível em: <

A par disso, considerando que a expressão “direito à proteção de dados pessoais” possui maior abrangência, pois inclui a proteção de informações pessoais, inclusive incorporando os problemas específicos que suscitam a informática, no presente trabalho discute-se a efetividade desse direito frente ao *big data*, é juridicamente mais adequada a expressão “direito à proteção de dados pessoais”.

Por outro lado, a “autodeterminação informativa” é utilizada em sistemas jurídicos com proteção jurídico-normativa positivada, a exemplo de Portugal, Espanha e Alemanha. A importação desta expressão, por não corresponder à atual realidade jurídica brasileira, pode levar a um juízo de negação teórica e prática deste direito.

3.1.2 Documentos Internacionais

O direito à proteção de dados pessoais pode ser lido no artigo 12 da Declaração Universal dos Direitos Humanos de 1948[128], no artigo 17 do Pacto Internacional dos Direitos Civis e Políticos 1966[129] (Decreto nº 592, de 06/07/19925); e no artigo 11 do Pacto de San José da Costa Rica de 1969[130] (Decreto n° 678, de 6/11/1992)[131].

---

https://www.researchgate.net/publication/28060693_La_primera_jurisprudencia_sobre_el_derecho_a_la_autodeterminacion_informativa>. Acesso em: 20 maio 2016; MURILLO DE LA CUEVA, P. L. La construcción del derecho a la autodeterminación informativa. **Revista de estudios políticos**, nº 104, p. 35-60, 1999; MURILLO DE LA CUEVA, P. L. La protección de los datos de carácter personal en el horizonte de 2010, **Anuario de la Facultad de Derecho (Universidad de Alcalá)**, nº. 2, p. 131-142, 2009; MURILLO DE LA CUEVA, P. L. Perspectivas del derecho a la autodeterminación informativa. **IDP**: revista de Internet, derecho y política = revista d'Internet, dret i política, nº. 5, 2007. Disponível em: <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf>. Acesso em: 20 maio 2016; MURILLO DE LA CUEVA, P. L. Derechos fundamentales y avances tecnológicos: Los riesgos del progreso. **Boletín Mexicano de Derecho Comparado**, nº. 109, p. 72-110, 2004.

[128] Art. 5º - Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos.** Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://unesdoc.unesco.org/images/ 0013/001394/139423por.pdf>. Acesso em: 21 jan. 2017.)

[129] Art. 17. 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Pacto Internacional dos Direitos Civis e Políticos**. Adotado e aberto à assinatura, ratificação e adesão pela resolução 2200-A (XXI) da Assembleia Geral das Nações Unidas, de 16 de Dezembro de 1966. Disponível em: < http://www.cne.pt/ sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf>. Acesso em: 21 jan. 2017.)

[130] Art. 11. [...] 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou

Entretanto, aponta-se a Convenção de *Strasbourg* de 1981 como marco na configuração do direito à proteção dos dados pessoais como direito fundamental. A Convenção deixa claro que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais. A Carta dos Direitos Fundamentais da União Europeia, proclamada em 7 de dezembro de 2000, que dispõe no artigo 8º acerca da "proteção de dados pessoais", e inspira-se no artigo 8º da Convenção de *Strasbourg*, na Diretiva 95/46/CE e no artigo 286º do Tratado Instituidor da União Europeia. É o documento europeu que levou mais adiante a sistemática da proteção de dados pessoais e sua configuração como pressuposto do estado democrático presentes na Convenção de Strasbourg, Diretiva 95/46/CE e Convenção Europeia para os Direitos do Homem[132]. Nesse sentido também o Regulamento Geral sobre a Proteção de Dados da União Europeia 2016/679.

É na Declaração de Santa Cruz de La Sierra[133], documento final da XIII *Cumbre* Ibero-Americana[134] de Chefes de Estado e de Governo[135], firmada pelo governo brasileiro, em 15 de novembro de 2003, que se atribui o *status* de direito fundamental à matéria da proteção dos dados pessoais. No seu item 45 lê-se,

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela

---

reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção Americana de Direitos Humanos de 1969 (Pacto San José da Costa Rica)**. Assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de novembro de 1969. Disponível em: <http://www.planalto.gov.br/ccivil_ 03/decreto/D0678.htm>. Acesso em: 21 jan. 2017.).

[131] Sobre o valor jurídico da Declaração Universal ver: OLIVEIRA, Liziane Paixão Silva; FUMAGALI, E.. VALOR JURÍDICO DA DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM: NORMA JUS COGENS OU SOFT LAW?. In: PEDEMONTE, Iga Diaz; SANCHES, Samyra Haydêe Dal Farra Naspolini (Org.). **Direito internacional dos direitos humanos III**. 1. ed. FLORIANOPOLIS: CONPEDI, 2016, p.62-78.

[132] DONEDA, op. cit, 2011

[133] CONFERÊNCIA DAS AMÉRICAS. **Declaração de Santa Cruz de La Sierra.** Documento final da XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo, realizada em Santa Cruz de la Sierra em 14 e 15 de novembro de 2003. Disponível em: < http://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>. Acesso em: 21 jan. 2017.

[134] "O Sistema Ibero-Americano é constituído pelos vinte e dois países membros, a Secretaria-Geral Ibero-Americana, e os Organismos Ibero-Americanos Setoriais que são: a Organização de Estados Ibero-Americanos para a Educação, a Ciência e a Cultura, OEI; o Organismo Internacional de Juventude para Ibero-America, OIJ; a Organização Ibero-Americana de Segurança Social, OISS; e a Conferência de Ministros da Justiça dos Países Ibero-Americanos, COMJIB" (SECRETARÍA GENERAL IBEROAMERICANA. **Organismos Ibero-Americanos.** Disponível em: <http://segib.org/pt-br/organismos-ibero-americanos/>. Acesso em 15 dez. 2016).

[135] http://segib.org/pt-br/documento/declaracao-de-santa-cruz-de-la-sierra-3/ Fazer ainda referência.

> qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.[136]

Os documentos internacionais têm reconhecido o direito à proteção de dados pessoais como direito humano e instigando que se constitua como direito fundamental, a partir da conexão que este mantém com a promoção dos direitos humanos e das liberdades fundamentais. Dessa forma, considerando que o ordenamento jurídico estabelece a matéria dos direitos da personalidade como inerentes à dignidade humana, esta representando "elemento essencial dos direitos fundamentais"[137], resta concluir que o ordenamento jurídico pátrio há de convergir com os enunciados dos documentos internacionais, levando a matéria da proteção de dados pessoais a gozar do *status* de direito fundamental, decorrente do direito à privacidade estabelecido no art. 5º, X, CF88 ao tratar da inviolabilidade da intimidade e vida privada.

3.2 A INFLUÊNCIA DA LEGISLAÇÃO INTERNACIONAL

Nesta seção é traçada a evolução das leis de proteção de dados e examinado como os países europeus consolidaram a matéria de proteção de dados pessoais, assim como a Colômbia, a fim de compreender como o ordenamento jurídico brasileiro tem incorporado os dispositivos do direito interno de outros Estados que já avançaram na regulação da temática, formulado inclusive projetos de lei, objeto do capítulo seguinte.

3.2.1 As gerações de leis de proteção de dados pessoais

Conferir um tratamento autônomo ao direito à proteção de dados pessoais é uma tendência presente em diversos ordenamentos jurídicos. Isto influenciou diretamente a inclusão desse direito no rol dos direitos fundamentais, bem como a sua consolidação em diversos diplomas legais.

É incontestável que desde o surgimento do direito à proteção de dados pessoais muitos foram os enfoques dados à matéria. Observa-se esta assertiva na

---

[136] CONFERÊNCIA DAS AMÉRICAS, 2003.

[137] BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010, p. 252.

classificação evolutiva das leis de proteção de dados pessoais realizada por Viktor Mayer-Schonberger[138] e Doneda[139], que descrevem diferentes gerações de leis partindo desde um enfoque mais técnico e restrito, até a abertura a técnicas mais específicas, aplicáveis às tecnologias adotadas para o tratamento de dados.

A primeira das gerações de leis[140] se estruturava em torno do fenômeno computacional em si[141]. Naquele instante, a pretensão maior centrava-se na regulação de um cenário em que o processamento de dados de grande porte recaísse sobre a coleta e a gestão dos dados pessoais. Em regra, tais leis tratavam da concessão de autorizações para a criação de banco de dados e do seu controle por meio de órgãos públicos. Denota-se que as leis da primeira geração tinham como destinatário final e principal, o Estado, pois ressaltavam o controle do uso de informações pessoais por suas estruturas administrativas.

Com um imenso receio quanto ao tratamento de informações frente às tecnologias, substanciado na falta de experiência, e o desconhecimento quanto à possibilidade de uso indiscriminado da tecnologia, nessa primeira fase de leis, foram consagrados princípios de proteção amplos e genéricos, basicamente focados na atividade de processamento de dados, em que pese às leis de primeira geração terem se restringido à criação de banco de dados, controle e uso por entes públicos.

O enfoque dado por essas leis era previsível pelo simples fato de terem como motivação para sua elaboração, a ameaça representada pela tecnologia e, especificamente, pelos computadores[142]. Aspectos relevantes dessas leis repousavam na: a) ausência do emprego do termo privacidade, substituída por "banco de dados", em que pese à sua estruturação e elementos gramaticais estarem condicionados à informática; e b) ausência de previsão da participação do cidadão no processo que regulava a proteção de dados pessoais. Em síntese, trataram, na verdade, dos bancos de dados e não da privacidade.

---

[138] MAYER-SCHONBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (orgs.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997, pp. 219-242.

[139] DONEDA, op. cit., 2011.

[140] Cita-se a exemplo como leis de primeira geração a Lei do Land Alemão de Hesse, de 1970; a Primeira Lei Nacional de Proteção de Dados, sueca, que foi o Estatuto para Bancos de Dados de 1973 – Data Legen 289, ou Datalag, além do Privacy Act, norte-americano de 1974.

[141] DONEDA, op. cit., 2011.

[142] DONEDA, op. cit., 2011.

Com o passar dos anos, os centros de processamento de dados automatizados cresceram de uma forma significativa, multiplicando-se, ao passo que as leis de proteção de dados de primeira geração tornaram-se inefetivos, logo sendo ultrapassadas, em razão do controle, baseado em um regime de autorizações, como previa essas leis, daí terem se tornado inviáveis.

Rompendo com a concepção de que as leis de proteção de dados pessoais deveriam se estruturar em torno do fenômeno computacional em si, a segunda geração de leis sobre a matéria surgiu no final da década de 1970. A distinção elementar dessa geração em relação à anterior repousa no fato de que tais leis basearam-se "[...] na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão"[143].

No processo de evolução social e do próprio direito, novas condicionantes surgiram e, por força de novas exigências, surgiu a terceira geração de leis de proteção de dados pessoais. O surgimento dessa nova geração decorreu da percepção de que, para uma efetiva participação do cidadão na vida social, o fornecimento de dados pessoais havia se tornado um requisito indispensável. Com isso, houve uma inversão notória: o que era exceção tornou-se regra, basta observar as delimitações das leis de gerações anteriores.

Nesse sentido, observou-se que, assim como o Estado, os entes privados também se utilizavam do fluxo de informações pessoais para seu funcionamento. O problema concentrou-se no fato de que, com a intromissão dos indivíduos proprietários dos dados em questão, surgiu um obstáculo que interrompia e, às vezes, até excluía o indivíduo de algum aspecto da vida social, pois limitava o funcionamento do Estado e entes privados, decorrente da autonomia que os cidadãos passaram a possuir em detrimento do que previa a terceira geração de leis, que teve início na década de 1980.

O intuito era sofisticar a tutela dos dados pessoais, com foco no cidadão, porém em um nível de abrangência maior, o qual se preocupava muito além da liberdade de fornecer ou não os próprios dados pessoais, mas também em garantir a efetividade dessa liberdade[144].

A proteção de dados é considerada, por tais leis, como um processo complexo, que envolve direito de autotutela na gerência dos dados pessoais pelo

[143] DONEDA, op. cit., 2011, p. 98
[144] DONEDA, op. cit., 2011.

próprio indivíduo. A complexidade relaciona-se à participação do sujeito na sociedade e ao contexto no qual lhe é solicitado que revele seus dados, protegendo o particular das possíveis e prováveis situações em que lhes é imposta uma liberdade condicionante que cercearia o direito de decidir livremente sobre a disposição de suas informações pessoais propiciando, assim, o efetivo exercício da autodeterminação informativa.

Há relevantes mudanças nas estruturas das novas leis de terceira geração, a exemplo do surgimento da autodeterminação informativa representando uma extensão das liberdades constantes nas leis de segunda geração. A partir dessas leis foi reconhecido certo desequilíbrio entre a pessoa e as entidades que coletam e processam seus dados.

O modelo sólido de proteção de dados pessoais pode ser vislumbrado explicitamente nos países europeus que transcreveram para seus ordenamentos as Diretivas Europeias em matéria de proteção de dados, sendo elas a Diretiva 95/46 /CE[145] e a Diretiva 2002/58/CE[146], sobre a privacidade e as comunicações eletrônicas; e, em atual vigência o Regulamento Geral da União Europeia 2016/679[147] sobre proteção de dados pessoais.

3.2.2 A Contribuição de Portugal, Espanha, Alemanha e Colômbia

Portugal foi o primeiro país a estabelecer constitucionalmente um direito fundamental à proteção dos dados pessoais, disposto no artigo 35[148], da

[145] PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Diretiva 95/46/CE**, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < http://www.anacom.pt/render.jsp?categoryId=332397>. Acesso em: 21 jan. 2017.

[146] PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Directiva 2002/58/CE**, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponível em: < Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF >. Acesso em: 21 jan. 2017.

[147] PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Regulamento UE 2016/679,** de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://www.privacy-regulation.eu/pt/>. Acesso em: 21 jan. 2017.

[148] "Artigo 35º da Constituição:
1 - Todos os cidadãos têm o direito de acesso aos dados informatizados que lhe digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam nos termos da lei.

Constituição Portuguesa, cujo texto foi revisado em 1982, em 1989 e em 1997. Para Catarina Sarmento e Castro[149], juíza do Tribunal Constitucional de Portugal,

> O direito consagrado no artigo 35.º traduz-se num feixe de prerrogativas que pretendem garantir que cada um de nós não caminhe nu, desprovido de um manto de penumbra, numa sociedade que sabe cada vez mais acerca de cada indivíduo. É um direito a não viver num mundo com paredes de vidro, é um direito a não ser transparente, por isso, desenha-se como um direito de protecção, de sentido negativo. Visto deste prisma, o direito em causa permite que o indivíduo negue informação pessoal, se oponha à sua recolha, difusão, ou qualquer outro modo de tratamento. Neste sentido, ainda está próximo da ideia Americana de "privacy", enquanto direito de defesa face às agressões do Estado e terceiros às suas informações pessoais. Mas é mais. Longe de ser um mero direito contra as intrusões do Estado ou de outros indivíduos, que devem abster-se de proceder a tratamentos dos seus dados pessoais, é um direito a decidir até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam, construindo-se como uma liberdade, como um poder de determinar o uso dos seus dados pessoais. Assim, evita-se que o indivíduo se transforme em "simples objecto de informações" também na medida em que se lhe atribui um poder positivo de dispor sobre as suas informações pessoais, i.e., um poder de autotutela, de controlo, sobre os seus dados pessoais, que permite ao cidadão "preservar a sua própria identidade informática".

Diferente da Constituição Federal Brasileira de 1998, a Constituição Portuguesa retrata a preocupação com a regulação do uso dos dados pessoais, por meio da informática, refletindo a atual preocupação do indivíduo que, cada vez mais, tem seus dados disponibilizados na internet e armazenados em bancos de dados automatizados.

---

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". (PORTUGAL. **Constituição da República Portuguesa**. Disponível em: < http://www.fd.uc.pt/CI/CEE/OI/Constituicao_Portuguesa.htm> Acesso em: 10 maio 2016).

[149] CASTRO, C. S. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro. In: CONGRESO IBEROAMERICANO DE DERECHO CONSTITUCIONAL: DERECHO CONSTITUCIONAL PARA EL SIGILO XXI, 8, 2006, Sevilla (Epaña)/Universidad de Sevilla, **Actas**..., Navarra: Aranzadi, 2006, p. 1645.

A Constituição espanhola de 1978 garante, no seu art. 18, o direito à honra, à privacidade pessoal e familiar e à própria imagem, assemelhando-se ao disposto no art. 5º, X da Constituição Federal Brasileira de 1988. Distinguindo-se da CF88 que é omissa, a Constituição Espanhola[150] acentua o caráter danoso da informática com relação à proteção da privacidade e direitos fundamentais na realidade atual; por essa razão busca limitar o uso da informática[151].

A Sentença nº 254/1993, de 20 de julho de 1993[152] marca o primeiro pronunciamento do Tribunal Constitucional Espanhol sobre os limites da informática para proteção da intimidade pessoal e familiar. O caso tratou da solicitação relativa a dados pessoais existentes em bancos de dados automatizados sob a administração do Estado, com fundamento no art. 18, itens 1 e 4 da Constituição Espanhola de 1978[153], bem como na Convenção de *Strasbourg* de 1981 que entrou em vigor na Espanha em 01 de outubro de 1985. A pretensão foi no sentido de que a administração do Estado, ou qualquer organismo dela dependente, comunicasse se dispõe de banco de dados automatizados em que neles figurem dados pessoais do autor, e, caso existisse que fosse indicada a finalidade principal dos bancos de dados, assim como a autoridade que os controla, sua residência e quais dados pessoais encontram-se registrados.

O Tribunal Constitucional Espanhol entendeu que o uso da informática encontra um limite em respeito à honra e à intimidade das pessoas, em pleno exercício de seus direitos; e que, para a efetividade deste direito, é possível requerer garantia complementar que pode vir a ser suprida através do auxílio interpretativo de tratados e convenções internacionais, ratificados pela Espanha sobre a matéria. Decidiu-se, pois, que a garantia da intimidade adota um conteúdo positivo resultando no direito de controle do indivíduo sobre seus dados pessoais, e, por esse motivo, a liberdade informática deve também ser entendida como direito de

---

[150] ESPANHA. **Constituição Espanhola.** 29 de dezembro de 1978. Madrid, 1978. Disponível em: <http://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Acesso em: 21 jan. 2017.

[151] EFING, Antônio Carlos. **Bancos de dados e cadastro de consumidores**. São Paulo: Editora Revista dos Tribunais, 2002.

[152] ESPANHA. Tribunal Constitucional. **Recurso de Amparo núm. 1827/1990**. Sentencia 254/1993, de 20 de julho de 1993. Julgamento em 28 de julho de 1993. Madrid, 1993.

[153] "Artículo 18: 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. [...] 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." (ESPANHA, 1978; suprimimos).

controle do uso dos dados pessoais em programas informáticos, referenciando ainda o *habeas data.*

Para o Tribunal Constitucional Espanhol na Sentença nº 254/1993:

> [...] al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de caráter personal, así como los datos que le conciernen a él personalmente, la Administración demandada em este processo vulneró el contenido esencial del derecho a la intimidad del actor, al despojarlo de su necesaria protección[154].

O artigo 18.4 da Constituição Espanhola reconhece o direito à autodeterminação informática, ao passo que limita o uso das novas tecnologias em detrimento da honra, da intimidade do cidadão e de sua família e do pleno exercício de seus direitos. Não é à toa que a jurisprudência espanhola, pela primeira vez, através da Sentença nº 254/1993 menciona a liberdade informática como direito fundamental.

No tocante à Alemanha, o aspecto que se sobressai diz respeito à criação de cadastros informatizados e a coleta de dados. A legislação alemã sobre a proteção de dados pessoais segue o modelo das legislações de primeira geração que se ocupou dessa matéria. Exige a inscrição do cadastro informatizado que se deseja criar, como elemento constitutivo, para que se tenha a autorização a fim de criar um cadastro de dados; em suma, traz maior rigor na constituição de cadastros[155].

A principal contribuição para a configuração jurídica da "autodeterminação informativa" é a decisão de 15 de dezembro de 1983 do Tribunal Constitucional Alemão sobre a Lei do Censo da população[156] (*Volkszählungsgesetz*). O teor do julgado concebeu a "autodeterminação informativa" (*RechtaufinformationelleSelbstimmung*), como a autonomia que a pessoa tem de determinar quem, o quê, e em que ocasião (*wer, was, wann, beiwelchenGelegenheit*) pode conhecer e/ou utilizar dados que lhe afetam. O reconhecimento do direito à autodeterminação informativa decorreu da interpretação

[154]ESPANHA, 1993, p. 13.
[155] LIMBERGER, op. cit., 2007.
[156] O Tribunal afirmou que a autodeterminação informativa não é um direito absoluto, podendo ser restringido em razão de interesse público predominante. Isso pode ocorrer, na medida em que a informação representa um recorte da realidade social, da qual o próprio indivíduo faz parte e é interdependente. (MENDES, L. S. F. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Dissertação (Mestrado em Direito). Brasília, DF: Universidade de Brasília, 2008. Disponível em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp149028.pdf>. Acesso em 01 dez. 2016)

constitucional realizada pelo *Bundesverfassungsgericht* (art. 1.1 c/c art. 2.1, da Lei Fundamental), sobre o livre desenvolvimento da personalidade, o direito geral da personalidade e a dignidade da pessoa humana[157].

Atualmente, na Alemanha, a principal legislação de proteção de dados é o *Federal Data Protection Act* (*Bundesdatenschutzgesetz*) (BDSG)[158], alterado em 2009. Esse documento incorpora no direito alemão os requisitos da Diretiva de Proteção de Dados da União Europeia (95/46/CE)[159]. Dentre os princípios fundamentais que se aplicam ao tratamento de dados pessoais previstos na legislação alemã, estão a "transparência", sobressaindo a seção 4 (2)[160], que fixa como regra a necessidade de obtenção dos dados pessoais através do próprio titular, e como exceção nos casos exigidos por lei, por outras pessoas ou organismos administrativos em razão de suas atribuições ou propósitos, ou, ainda, quando a obtenção direta pela pessoa exigiria um esforço desproporcional, resultando assim numa coleta indireta. Segundo a seção 4 (3)[161], nos casos em que os dados pessoais são concedidos pelo indivíduo, a este devem ser informados: a identidade do responsável pelo tratamento dos dados, bem como a finalidade da obtenção, processamento e uso de seus dados.

Na sequência, consta na BDSG o princípio da limitação da finalidade, que pode ser lido na seção 28[162] que trata do recolhimento e registro de dados para fins comerciais, fixando que, nesses casos, o objetivo do processamento de dados

---

[157] CUEVA, op. cit., 2012, p. 230.

[158] ALEMANHA. **Federal Data Protection Act (BDSG)** In the version promulgated on 14 January 2003. Publicação: Federal Law Gazette I, p. 66. Last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009. Disponível em: < http://dzlp.mk/sites/default/files/ Dokumenti/EU%20zakoni%20zzlp/GERMANY.pdf>. Acesso em: 21 jan. 2017.

[159] TREACY, Bridget. Preparing for Change: Europe's Data Protection Reforms Now a Reality. In: HUNTON & WILLIAMS. **The International Comparative Legal Guide to: Data Protection 2016.** London, 2016, p. 92. Disponível em: <https://www.hunton.com/files/upload/ICLG_Data_Protection_2016.pdf>. Acesso em 19 jan. 2017.

[160] "(2) Personal data shall be collected from the data subject. They may be collected without the data subject's participation only if:
1. allowed or required by law, or
2. a) the data must be collected from other persons or bodies due to the nature of the administrative task to be performed or the commercial purpose, or
b) collecting the data from the data subject would require disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected." (ALEMANHA, 2009, p. 8).

[161] "(3) If personal data are collected from the data subject, the controller shall inform him/her as to
1. the identity of the controller,
2. the purposes of collection, processing or use, and [...]." (ALEMANHA, 2009, p. 8).

[162] "[...] When personal data are collected, the purposes for which the data are to be processed or used shall be specifically defined." (ALEMANHA, 2009, p. 30).

pessoais e a sua utilização devem ser determinados no momento da obtenção. Na seção 32 (1) resta também definido a limitação da finalidade quanto à coleta, processamento e uso de dados pessoais de empregados para fins de tomada de decisão sobre contratação ou após, em casos de cessação do contrato de trabalho, assim como para investigar crimes, neste último caso sendo necessária a existência de documento que possa acreditar que o indivíduo cometeu um crime na condição de empregado[163].

A legislação alemã sobre proteção de dados pessoais (BDSG) faz referência, ainda, aos princípios: i) da legalidade, ao passo que dispõe na seção 4 (1)[164] que a coleta, o processamento e a utilização dos dados pessoais somente serão possíveis se permitidos pela BDSG ou por outra lei que trate da matéria, ou por consentimento do indivíduo; ii) da proporcionalidade, observada em toda a BDSG, usado tanto em operações específicas, como na regra da seção 3 (A)[165], a qual remete à coleta, tratamento e utilização de dados em sistemas que devem ser organizados de acordo com a finalidade, em menor número possível de dados, e ainda sempre que possível, quando devem ser anônimos.

A BDSG garante aos indivíduos direito de acesso a informações sobre quem registrou os dados que lhes dizem respeito, os destinatários aos quais seus dados são transferidos e os propósitos para os quais estão sendo coletados, direitos estes previstos na seção 34[166]; bem como é garantido o direito de correção[167] quando se

---

[163] "(1) An employee's personal data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to investigate crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime, and the employee does not have an overriding legitimate interest in ruling out the possibility of collection, processing or use, and in particular the type and extent are not disproportionate to the reason." (ALEMANHA, 2009, p. 37).

[164] "(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consente." (ALEMANHA, 2009, p. 8).

[165] "Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection." (ALEMANHA, 2009, p. 7).

[166] "(1) The controller shall provide information to data subjects at their request concerning 1. recorded data relating to them, including information relating to the source of the data, 2. the recipients or categories of recipients to which the data are transferred, and 3. the purpose of recording the data." (ALEMANHA, 2009, p. 39).

[167] Seção 35: "(1) Personal data shall be rectified when they are inaccurate." (ALEMANHA, 2009, p. 41).

referirem a informações imprecisas, exclusão[168], nos casos em que tenham sido ilegalmente gravados, ou se refiram a dados sensíveis (origem racial ou étnica, opiniões políticas, religiosas ou crenças filosóficas, a filiação sindical, à saúde ou à vida sexual) ou quando se tornam desnecessários, bem como o direito ao bloqueio dos dados[169], quando a sua exclusão violaria o período de retenção definida por lei ou contrato, ou em casos em que a exclusão seria prejudicial para legitimar interesses do titular dos dados, e, por fim, quando a exclusão é impossível ou implica um esforço desproporcionado devido à categoria especial de gravação.

Denota-se que, apesar de todo o arcabouço protetivo trazido com a legislação portuguesa e alemã, não há previsão de qualquer instrumento processual apto a garantir os direitos materialmente assegurados, ao contrário do que ocorre no Brasil com a expressa disposição do *habeas data* como remédio constitucional que tutela o direito a proteção de dados pessoais.

Enquanto isso, na América Latina, cabe destacar a contribuição da Colômbia que em sua Constituição de 1991 reserva o capítulo I do seu título II para os direitos fundamentais. Sobressai o art. 15, que assegura o direito à intimidade e à proteção de dados pessoais:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantias consagradas en la Constitución.
> La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante

[168] Seção 35: "(2) Personal data may be erased at any time, except in the cases referred to in subsection 3 nos. 1 and 2. Personal data shall be erased if
1. unlawfully recorded, or
2. they concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, punishable actions or administrative offences, and the controller is unable to prove their accuracy,
3. they are processed for own purposes, as soon as knowledge of them is no longer needed to carry out the purpose for which they were recorded, or
4. they are commercially processed for the purpose of transfer and an examination at the end of the fourth calendar year from their initial recording shows that further retention is unnecessary." (ALEMANHA 2009, p. 41-42).

[169] Seção 35: "(3) Instead of being erased, data shall be blocked where
1. in the case of subsection 2 no. 3, erasure would violate retention periods set by law, statute or contract,
2. there is reason to believe that erasure would be detrimental to legitimate interests of the data subject, or
3. erasure would be impossible or would involve a disproportionate effort due to the special category of recording." (ALEMANHA, 2009, p. 42).

> orden judicial, en los casos y con las formalidades que establezca la ley.
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley[170].

Motivada pela proteção constitucional aos dados pessoais, a Constituição colombiana garante o direito de o individuo conhecer, atualizar e retificar informações que lhe digam respeito e que estejam em banco de dados e arquivos, sejam de entidade pública ou privada - destacando-se uma maior abrangência comparada à proteção conferida pela Constituição Brasileira que concebe o *habeas data* como instrumento oponível a bancos de dados de caráter público ou entidade governamental. Passados 21 anos, foi promulgada a Lei nº 1.581 de 2012[171] que dispõe sobre a proteção de dados pessoais, tendo como objetivo desenvolver o direito constitucional referidos no art. 15 e 20 da Constituição, regulamentada pelo Decreto nº 1.377 de 2013[172].

A Lei nº 1.581 de 2012 é a primeira lei colombiana específica para proteção de dados pessoais, mas não a única. Em 2008 foi promulgada a Lei nº 1.266 que trata do *habeas data* e regulamenta o manejo de informação contida em bases de dados pessoais, especialmente os que dizem respeito a informações financeiras, crédito, comerciais, de serviços e proveniente de outros países, da qual se destaca o arcabouço principiológico para administração de dados elencado no art. 4º que tem como objetivo auxiliar na interpretação e aplicação da lei, sendo eles,

> a) **Principio de veracidad o calidad de los registros o datos**. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;
> b) **Principio de finalidad**. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la

---

[170] COLOMBIA, **Constitución Política de Colombia**. Actualizada con los Actos Legislativos a 2015. p, 15. Disponível em: <http://www.corteconstitucional.gov.co/inicio/Constitucion% 20politica%20de%20Colombia %20-%202015.pdf>. Acesso em 22 jan. 2017.

[171] COLÔMBIA. **Ley Estatutaria 1581 de 2012** (Octubre 17). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013**. Por la cual se dictan disposiciones generales para la protección de datos personales.**
Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Acesso em: 22 jan. 2017.

[172] COLÔMBIA. **Decreto 1377** de 2013. (Junio 27) Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Disponível em: < http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf>. Acesso em 22 jan. 2017.

> Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;
> c) **Principio de circulación restringida**. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.
> Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;
> d) **Principio de temporalidad de la información**. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;
> e) **Principio de interpretación integral de derechos constitucionales**. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;
> f) **Principio de seguridad**. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;
> g) **Principio de confidencialidad**. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma[173].

A Lei nº 1.581 de 2012 acrescenta aos princípios já assegurados pela Lei nº 1.266 de 2008, como princípios orientadores para o tratamento de dados pessoais os princípios da legalidade em matéria de tratamento de dados, da liberdade, da

[173] COLÔMBIA. **Ley Estatutaria 1266** de 2008 (diciembre 31). por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488#0>. Acesso em 22 jan. 2017.

transparência e de acesso (art. 4º)[174]. Institui ainda como autoridade para proteção de dados pessoais a Superintendência de Indústria e Comércio por meio de uma Superintendência adjunta específica com poder de vigilância e sanção, a fim de que seja garantido o tratamento de dados pessoais em respeito aos princípios, direitos e garantias previsto na lei (arts. 19, 21).

Diante do exposto, tanto os países europeus citados, como a Colômbia, representante da América Latina, têm, cada vez mais, se preocupado com a proteção dos dados pessoais de seus cidadãos. A regulamentação é o primeiro e mais representativo passo que evidencia essa preocupação, através das leis de proteção de dados e da instituição de órgãos com atribuições específicas quanto à vigilância e aplicação de sanções junto àqueles que descumpram as referidas regras.

As consequências dessa onda de regulação acerca da proteção de dados pessoais já são sentidas pelas empresas. É o que informa uma pesquisa da OVUM encomendada pela *Intralinks*, ao apontar que mais de 70% das empresas que atuam na área de transformação digital preveem um aumento nos seus orçamentos para atender às exigências das novas regulamentações de dados, apontando ainda que

---

[174] "Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:
a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;
[...]
c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;
[...]
e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;
f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;
[...]." (COLÔMBIA, 2012).

os Estados Unidos, China e Rússia são os países menos confiáveis no quesito respeito aos direitos de privacidade[175].

[175] INFORME DE OVUN. Leyes de privacidad de los datos: simplificación de los trámites. **Intralinks.** 2017.
Disponivel em: <https://www2017..intralinks.com/es/resources/analyst-reports/ovum-report-data-privacy-laws-cutting-red-tape>. Acesso em 22 jan.

4 O MARCO LEGAL DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

No ordenamento jurídico brasileiro, o artigo 5º da Constituição de 1988 assegura o direito à informação, à liberdade de expressão, garante a inviolabilidade da intimidade e da vida privada e concebe o *habeas data* como instrumento de tutela para proteção dos dados pessoais, remédio constitucional reconhecido pelo Supremo Tribunal Federal para o fim de salvaguardar o direito à informação de dados pessoais.

Quando o tema discutido é o direito da personalidade, o Código Civil de 2002 disciplina a matéria em grupos: *direitos à integridade física* e *direitos à integridade moral.* No primeiro: situa-se o direito à vida, ao próprio corpo, enquanto no segundo, o direito à imagem, à privacidade, entre outros[176].

Acrescentando ao Código Civil, a legislação ordinária, ainda que de maneira reflexa, cuida da matéria de proteção aos dados pessoais: o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet.

Destarte, com o objetivo de conceber o marco regulatório do direito fundamental à proteção de dados pessoais no Brasil examinam-se, a seguir, os aspectos mais relevantes, no tocante à matéria, conferidos pela Constituição Federal de 1988, a legislação ordinária e, por fim, a elaboração de uma legislação específica em curso por meio de projeto de lei que tramita no Congresso Nacional.

4.1 O AMPARO CONSTITUCIONAL

O reconhecimento da proteção de dados como um direito autônomo e fundamental no direito brasileiro não é concebido de forma explícita, em face da não constatação literal das expressões “direito à autodeterminação informativa” ou “direito à proteção de dados pessoais” na Constituição Federal de 1988. Inobstante a ausência da previsão desse direito de maneira taxativa, importa destacar

[176] BARROSO, op. cit., 2010.

inicialmente as lições de Flávia Piovesan[177] segundo as quais "[...] a Constituição Brasileira de 1988 constitui o marco jurídico da transição democrática e da institucionalização dos direitos humanos no Brasil".

Com a consolidação do princípio da dignidade humana (art. 1º, III, CF88) é possível vislumbrar o tratamento da proteção da personalidade, mais precisamente no art. 5º, incisos X, XII, LXXII, CF88. Merece destaque o último que trata da previsão do *habeas data* como remédio constitucional que visa a garantir ao indivíduo o acesso e retificação dos seus dados pessoais constantes em bancos de dados de caráter público.

Dessa forma, considerando, a relevância da garantia constitucional do *habeas data*, o Supremo Tribunal Federal (STF) em cumprimento do seu dever em "divulgar aos jurisdicionados e aos cidadãos em geral, de maneira simples e didática, qual é a compreensão da Corte acerca dos distintos preceitos de nossa Lei Maior"[178] elaborou a obra "A Constituição e o Supremo"[179]. Nesta estão expostos os precedentes mais relevantes da sua jurisprudência, motivo pelo qual este texto irá analisar o pronunciamento desta Corte no recorte de julgamentos ali dispostos acerca do *habeas data*.

O STF elegeu, na 5ª edição de sua obra "A Constituição e o Supremo", já mencionada, nove decisões (HD 100 AgR; HD 90 AgR; HD 92 AgR; RMS 24.617; RHD 24; RHD 22; HD 87 AgR; RE 673.707; RE 165.304)[180] como sendo as mais representativas de todo seu arcabouço jurisprudencial para comentar o art. 5º, LXXII, CF88, que trata do *habeas data*. Por meio dessas decisões o Supremo Tribunal Federal estabelece o seu entendimento acerca do conceito e finalidade do *habeas data*, assim como reafirma os pressupostos processuais desta garantia com menção à Lei 9.507/97 que o regulamenta. Para o STF,

> O *habeas data* configura remédio jurídico-processual, de natureza constitucional, que se destina a garantir, em favor da pessoa interessada, o exercício de pretensão jurídica discernível em seu tríplice aspecto: (a) direito de acesso aos registros; (b) direito de

[177] PIOVESAN, Flávia. A constituição brasileira de 1988 e os tratados internacionais de proteção dos direitos humanos. **EOS - Revista Jurídica da Faculdade de Direito**. v. 2, n. 1, jan./jun. 2008. Curitiba: Dom Bosco, 2008, p. 25.
[178] BRASIL, Supremo Tribunal Federal. **A Constituição e o Supremo.** 5. ed. Brasília: STF, Secretaria de Documentação, 2016a, p. 5. Disponível em: <http://www.stf.jus.br/arquivo/cms/publicacaoLegislacaoAnotada/anexo/a_constituicao_e_o_supremo_5a_edicao.pdf>. Acesso em 5 jan. 2017.
[179] BRASIL, Supremo Tribunal Federal. op. cit., 2016a.
[180] BRASIL, Supremo Tribunal Federal. op. cit., 2016a, p. 343-344.

> retificação dos registros; e (c) direito de complementação dos registros. Trata-se de relevante instrumento de ativação da jurisdição constitucional das liberdades, a qual representa, no plano institucional, a mais expressiva reação jurídica do Estado às situações que lesem, efetiva ou potencialmente, os direitos fundamentais da pessoa, quaisquer que sejam as dimensões em que estes se projetem. O acesso ao *habeas data* pressupõe, entre outras condições de admissibilidade, a existência do interesse de agir. Ausente o interesse legitimador da ação, torna-se inviável o exercício desse remédio constitucional. A prova do anterior indeferimento do pedido de informação de dados pessoais, ou da omissão em atendê-lo, constitui requisito indispensável para que se concretize o interesse de agir no *habeas data*. Sem que se configure situação prévia de pretensão resistida, há carência da ação constitucional do *habeas data*.[181]

A partir deste tratamento conferido ao *habeas data*, em sede do Recurso em *Habeas Data* nº 22[182], reiterado no Agravo Regimental em *Habeas Data* nº 87, o Supremo concebeu a garantia constitucional expressa no art. 5º, LXXII, CF88 como instrumento que se presta a tutelar direitos fundamentais, e, adiante, realça o objeto de tutela desse remédio que recai sobre dados pessoais.

Ocorre que o *habeas data* foi, em sua maioria, utilizado para coibir atos arbitrários do Estado no tocante ao armazenamento de informações pessoais dos indivíduos, mantidas sob sigilo, objeto de enfrentamento pelo Supremo Tribunal Federal como se observa mediante os fundamentos do voto do Ministro Celso de Mello no Recurso em *Habeas Data* nº 22 para o qual:

> O sigilo dos atos estatais revela-se, pois, conflitante com a natureza pública ou ostensiva, de que se deve revestir o exercício do poder. O modelo político-jurídico, plasmado na nova ordem constitucional, rejeita (a) o poder que oculta e (b) o poder que se oculta. Com essa vedação, pretendeu o constituinte tornar efetivamente legítima, em face dos destinatários do poder, a prática das instituições do Estado.[183]

Explica-se o posicionamento retro, contextualizando-se historicamente o surgimento do *habeas data* na Constituição Federal de 1988. Na época o Brasil contava com o Serviço Nacional de Informações (SNI)[184]. Os *habeas data* eram

---

[181] BRASIL, Supremo Tribunal Federal, 2016a.

[182] BRASIL, Supremo Tribunal Federal. ***Habeas Data* 22**. *Habeas Data.* Natureza jurídica. Ministro Relator: Marco Aurélio. Órgão julgador: Tribunal Pleno. Data do Julgamento: 19 de setembro de 1991. Publicação: DJ 01-09-1995 PP-27378 EMENT VOL-01798-01 PP-00001. (1995b). Disponível em: < http://stf.jusbrasil.com.br/ jurisprudencia/14709849/recurso-em-habeas-data-rhd-22-df>. Acesso em: 21 jan. 2017.

[183] BRASIL. Supremo Tribunal Federal, 1995, p. 18

[184] "O SNI foi instituído pela Lei nº 4.341, de 13/06/1964, com a função de 'superintender e coordenar, em todo o território nacional, as atividades de Informações e Contra-Informações, em particular as

geralmente impetrados em face do SNI, conhecido também como "agência de espionagem da ditadura"[185]. O impetrante do RHD 22 pleiteou que lhe fosse assegurado o conhecimento de todas as informações relativas à sua pessoa, constantes dos registros do SNI. No julgamento do Recurso em *Habeas Data* 22, o Ministro Celso de Mello valeu-se do direito comparado ao tratar da institucionalização da garantia de acesso aos dados pessoais, mencionou o art. 35 da Constituição Portuguesa de 1976, o art. 105, b, da Constituição Espanhola, o "*Freedom of Information Act"* de 1974 e "*Freedom of Information Reform Act"* de 1986, ambos dos Estados Unidos, e, por fim, a França, que criou a Comissão Nacional de Informática, responsável por salvaguardar o direito de acesso às informações pessoais. Este repertório fundamentou seu posicionamento de que o direito de acesso às informações apesar de assegurado a todos, não é pleno, e sequer ilimitado, admitindo restrições quando se tratar de: (a) segurança e defesa do Estado, (b) investigação penal, ou (c) privacidade pessoal[186]. Explica o Ministro Celso de Mello, em seu voto no RDH 22, que "[...] a nova Constituição brasileira, ao

---

que interessem à Segurança Nacional'. O novo órgão era diretamente ligado à Presidência da República e atendia o presidente e o Conselho de Segurança Nacional. O chefe do Serviço tinha sua nomeação sujeita à aprovação prévia do Senado Federal e contava com prerrogativas de ministro. O SNI incorporou todo o acervo do Serviço Federal de Informações e Contra-Informações (SFICI), inclusive os funcionários civis e militares. A estrutura também era similar à de seu órgão antecessor. Uma série de inovações, entretanto, foram feitas. Uma das principais foi a instalação de uma Agência Central e de 12 Agências Regionais distribuídas pelo território nacional. A Agência Central contava com as áreas de Informações Externas, Informações Internas, Contra-Informação e Operações de Informações. O mesmo decreto que criou as Agências estabeleceu o 'Regulamento de Salvaguarda de Assuntos Sigilosos'(RSAS) – Decreto 60.417, de 11/3/1967. [...] O Brasil viveu, no início dos anos 1960, conjuntura política interna profundamente instável e influenciada pelo jogo geopolítico e estratégico que marcava a atuação das duas grandes potências mundiais à época da Guerra Fria – Estados Unidos e União Soviética. No mesmo período, era possível identificar conjunturas semelhantes de acirramento de conflito ideológico e de classes em diversos países da América Latina, com resultados diferentes: ora com o surgimento de movimentos autoritários e instalação de regimes de exceção, ora com o aparecimento de movimentos insurrecionais e revolucionários. No último cenário, estão incluídas, entre outras, independências de países africanos e a Revolução Cubana (1959). No primeiro cenário, insere-se a intervenção militar no processo político nacional em 1964. O SNI foi criado no mesmo ano." (BRASIL, Agência Brasileira de Inteligência. **1964 – Serviço Nacional de Informações (SNI).** Disponível em: < http://www.abin.gov.br/institucional/historico/1964-servico-nacional-de-informacoes-sni/>. Acesso em 13 jan. 2017, n.p)

[185] "No primeiro dia de seu governo [15 de março de 1990], o presidente Fernando Collor de Mello extingue o Serviço Nacional de Informações (SNI), criado logo depois do golpe de 1964 com o objetivo oficial de 'superintender e coordenar as atividades de informação e contrainformação em todo o território nacional'.Na prática, a criação do general Golbery do Couto e Silva tornou-se uma agência de espionagem dos governos militares que controlava a vida dos brasileiros, dos partidos, dos sindicatos e das organizações civis em geral. O SNI fichou militantes da resistência e forneceu informações aos organismos de repressão, como o Dops, o DOI-Codi e a Operação Bandeirante (Oban)." (EXTINTO o 'monstro' criado por Golbery. Disponível em: <http://memorialdademocracia.com.br/card/extinto-o-monstro-criado-por-golbery>. Acesso em 13 jan. 2017, n.p)

[186] BRASIL, Supremo Tribunal Federal, 1995.

instituir o habeas data, acentuou-lhe o caráter instrumental, em face do direito material cuja tutela visa a garantir"[187], concluindo o seu voto sob o fundamento de que, "[...] a garantia de acesso a informações de caráter pessoal, registradas em órgãos do Estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade"[188].

O *habeas data* é concebido, portanto, pelo Supremo Tribunal Federal como um "[...] relevante instrumento de ativação da jurisdição constitucional das liberdades [...]"[189], conectando-o ao direito à informação, direito público subjetivo. Inobstante o reconhecimento do *habeas data* como remédio constitucional que tutela o direito à informação de dados pessoais, não foi concedida a ordem pleiteada no RDH 22, sob o fundamento de que face à ausência de demonstração da recusa do SNI em fornecer as informações pessoais objeto da ação, restaria ausente o interesse legitimador da ação, pois se impõe ao autor que demonstre a existência de uma pretensão resistida[190].

A não positivação de um direito fundamental não implica a sua inexistência[191], ao passo que há direitos humanos fundamentais não inscritos no Texto Constitucional, embora não atendam ao aspecto formal[192], superam o "teste da fundamentalidade" sob o aspecto material. É indiscutível que a interpretação do art. 5º, § 2º da CF88 concebe uma interação entre o direito brasileiro e os tratados internacionais de direitos humanos. Isto implica a relevância dos tratados internacionais de direitos humanos que "[...] inovam significativamente o universo dos direitos nacionalmente consagrados – ora reforçando sua imperatividade jurídica, ora adicionando novos direitos"[193].

O art. 5º, § 2º, da CF88 tem o intento de viabilizar a inclusão de outros direitos fundamentais, pois nas palavras de Flávia Piovesan que "[...] a Constituição assume expressamente o conteúdo constitucional dos direitos constantes dos tratados

---

[187] BRASIL, Supremo Tribunal Federal, 1995, p. 21
[188] BRASIL, Supremo Tribunal Federal, 1995, p. 19
[189] BRASIL, Supremo Tribunal Federal, 1995, p. 22
[190] "Esta resistência, que se vê traduzida na ocorrência de obstáculo que impede o gozo de um direito pelo requerente, de manifestar-se na verificação real, prévia e concreta de um óbice oposto pela parte contrária, em ordem a evidenciar que a invocação da tutela jurisdicional se justifica e se torna necessária em face de impedimento, jurídico ou de fato, que inviabilize a satisfação de uma determinada pretensão de direito material." (BRASIL, Supremo Tribunal Federal, 1995b, p. 27).
[191] NAVARRO, op. cit. 2012, p. 15.
[192] CANOTILHO, J.J. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003, p. 379-380.
[193] PIOVESAN, op. cit., 2008, p. 32.

internacionais que Brasil é parte"[194]. Assim, nessa linha de pensamento, o direito fundamental à proteção dos dados pessoais, na lição de Jorge Bacelar Gouveia[195], seria um direito fundamental atípico, ou, na literatura de Ingo Sarlet[196], seria um direito fundamental implícito. Portanto, representa dizer que a previsão do princípio da não-tipicidade na esfera dos direitos fundamentais tem o condão de ampliar o rol desses direitos, inclusive incorporando os tratados internacionais dos quais o Brasil seja signatário[197].

Na classificação trazida por Flávia Piovesan, os direitos previstos pela Constituição situam-se em três grupos: i) direitos expressos no Texto Constitucional, ii) direitos expressos em tratados internacionais dos quais o Brasil seja parte, iii) direitos implícitos, que representam aqueles que estão subentendidos nas regras das garantias, bem como os decorrentes do regime e dos princípios adotados pela Constituição[198]. A partir dessa concepção, pode-se concluir que o direito à proteção de dados pessoais é um direito implícito, subentendido na garantia constitucional disposta no art. 5º, LXXII, CF88 que prevê o *habeas data*, disciplinado pela Lei nº 9.507/97[199], a qual regula o direito de acesso à informações e versa sobre o rito processual dessa garantia constitucional.

O que há de fundamental na consagração do *habeas data* são os direitos a que se presta tutelar: direito à informação e o direito contra a informação. Este remédio constitucional estaria incumbido de assegurar o direito à obtenção da informação, bem como garantir o direito contra a informação ou, seja, contra seu uso inadequado[200].

Além das finalidades previstas na Constituição Federal de 1988, a que se presta o *habeas data,* no tocante ao conhecimento de dados pessoais e sua

---

[194] PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 12. ed. São Paulo: Saraiva, 2011, p. 107.
[195] GOUVEIA, J. B. **Os direitos fundamentais atípicos**. Aequitas Editorial Notícias: Lisboa, 1995.
[196] SARLET, I. W. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 3. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2004.
[197] O direito à proteção de dados pessoais é referenciado no artigo 12 da Declaração Universal dos Direitos Humanos de 1948, no artigo 17 do Pacto Internacional dos Direitos Civis e Políticos 1966 (Decreto nº 592, de 06/07/19925); e no artigo 11 do Pacto de San José da Costa Rica de 1969 (Decreto n° 678, de 6/11/1992).
[198] PIOVESAN, op. cit., 2011, p. 110.
[199] BRASIL. Lei nº 9.507 de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: < https://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em 21 jan. 2017.
[200] SUNDFELD, Carlos Ari. "Habeas data" e mandado de segurança coletivo. **Doutrinas Essenciais de Direitos Humanos,** vol. 5, p. 169-186, Ago - 2011.

retificação, a Lei nº 9.507/97, além de disciplinar o rito processual dessa garantia, acrescenta uma terceira finalidade, que se refere "[...] a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável e que esteja sob pendência judicial ou amigável" (art. 7.º, III).[201]

No tocante aos dados sensíveis, em face da inviolabilidade da intimidade e da vida privada, as informações de caráter íntimo que possam colocar em risco a pessoa, faz com que o *habeas data* seja meio idôneo para apagá-la, esteja em banco de dados de um órgão público ou entidade qualquer, porque assim se estará retificando informações que não poderiam estar em banco de dados[202].

O Superior Tribunal de Justiça (STJ) no julgamento do Recurso Especial nº 1.457.199-RS, no caso "sistema *credit scoring*"[203], apesar de não se referir especificamente ao *habeas data*, tratou da vedação de utilização de dados sensíveis em bancos de dados para fins de formação de histórico de crédito, com fundamento no art. 43 do CDC e art. 3º da Lei nº 12.414/2011[204]. Para a Corte Superior, tal vedação:

> [...] busca evitar a utilização discriminatória da informação, conforme claramente definido pelo legislador como aqueles "pertinentes à origem social e étnica, à saúde, à informação genética, à orientação

[201] BRASIL, 1997.
[202] SUNDFELD, op. cit.,2011.
[203] "O chamado *credit scoring*, ou simplesmente *credscore,* é um sistema de pontuação do risco de concessão de crédito a determinado consumidor. Trata-se de um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis de decisão, com atribuição de uma nota ao consumidor avaliado conforme a natureza da operação a ser realizada. Aproveitando-se da facilidade contemporânea de acesso aos bancos de dados disponíveis no mercado via "internet", algumas empresas desenvolveram fórmulas matemáticas para avaliação do risco de crédito, a partir de modelos estatísticos, considerando diversas variáveis de decisão, atribuindo uma nota ao consumidor. As "variáveis de decisão" são fatores que a experiência empresarial denotou como relevantes para avaliação do risco de retorno do crédito concedido. Cada uma dessas variáveis recebe uma determinada pontuação, atribuída a partir de cálculos estatísticos, formando a nota final. Consideram-se informações acerca do adimplemento das obrigações (histórico de crédito), assim como dados pessoais do consumidor avaliado (idade, sexo, estado civil, profissão, renda, número de dependentes, endereço)." (BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.457.199 - RS** (2014/0126130-2). Direito do consumidor. Arquivos de crédito. sistema "credit scoring". Compatibilidade com o Direito brasileiro. Limites. Dano moral. Relator: Ministro Paulo de Tarso Sanseverino. Órgão julgador: Segunda Seção. Data do julgamento: 12 de dezembro de 2014. Data da publicação: 17 de dezembro de 2014b. Disponível em: < https://ww2.stj.jus.br/processo/revista/documento/mediado/? Componente =ITA&sequencial=1364998&num_registro=201401261302&data=20141217&formato=PDF>. Acesso em: 21 jan. 2017, p. 15-16,
[204] BRASIL. **Lei. 12.414** de 09 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: 21 jan. 2017.

> sexual e às convicções políticas, religiosas e filosóficas." Desse modo, no sistema jurídico brasileiro, encontram-se devidamente regulados tanto o dever de respeito à privacidade do consumidor (v.g. informações excessivas e sensíveis), como o dever de transparência nessas relações com o mercado de consumo (v.g. deveres de clareza, objetividade e veracidade)[205].

Cabe ressaltar que muito embora tenha reconhecida a vedação de utilização de dados sensíveis em bancos de dados para fins de formação de histórico de crédito, o STJ no caso concreto do *credit scoring,* entendeu que este sistema não constitui um cadastro ou banco de dados, mas um modelo estatístico, não se aplicando assim a exigência de obtenção de consentimento prévio e expresso do consumidor consultado (art. 4º da Lei n. 12.414/2011). Para a Corte Superior, o *credit scoring* constitui segredo da atividade empresarial, e, por esta razão, com fundamento no art. 5º IV, da Lei 12.414/2011[206], suas fórmulas matemáticas e modelos estatísticos não são passiveis de divulgação.

Defende Eduardo Talamini que "[...] o interessado terá sempre direito ao conhecimento dos dados atinentes à sua pessoa, ainda que o sigilo destes seja imprescindível à segurança da sociedade e do Estado"[207]. Portanto, o catálogo dos direitos fundamentais não está restrito à Constituição, admitindo-se a incorporação de outros direitos decorrente da cláusula aberta inserida no § 2º do art. 5º da CF88, bem como pelo conteúdo materialmente constitucional de que determinados direitos se revestem, como é observado no conteúdo do direito à proteção de dados pessoais que tem como finalidade assegurar a inviolabilidade da intimidade e vida privada do indivíduo.

4.2 O CÓDIGO CIVIL DE 2002

Com a finalidade de resguardar a dignidade humana, protegendo-a dos atentados que pode sofrer por parte de outros indivíduos, os direitos da personalidade se firmam enquanto direitos personalíssimos e essenciais ao desenvolvimento da pessoa humana[208].

---

[205]BRASIL, Superior Tribunal de Justiça, 2014, p. 41
[206] BRASIL. **Lei. 12.414** 2011.
[207] TALAMINI, Eduardo. O processo do *habeas data*: breve exame. **Revista de Processo,** vol. 101, p. 88-99, Jan – Mar 2001, p. 5.
[208] GOMES, Orlando. **Introdução ao direito civil**. 11. ed. Rio de Janeiro: Forense, 1996.

Dada à relevância e à necessidade de se assegurarem os direitos à personalidade do individuo, a Lei nº 10.406/02[209] que instituiu o Código Civil elegeu, no seu capítulo II (arts. 11 a 21), os direitos da personalidade como sendo intransmissíveis e irrenunciáveis, complementando no art. 11 que o exercício desses direitos não pode sofrer limitação voluntária. O Código Civil de 2002 dispõe que é exigível pelo titular que cesse a ameaça ou a lesão a direito da personalidade[210], podendo este reclamar perdas e danos sem prejuízos de outras sanções previstas em lei (art. 12), acatando o direito à indenização por dano material ou moral decorrente da violação à intimidade, à vida privada, à honra e à imagem anteriormente assegurado no art. 5º, X, CF/1988.

Ao individuo é assegurado o direito de proibir, mediante requerimento, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem que se referirem à sua pessoa, garantindo novamente o direito à indenização quando lhe for atingida a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais, estabelecendo, no entanto, exceções para essa regra que é mitigada: a) no caso de autorização da pessoa envolvida, b) quando a divulgação seja necessária à administração da justiça ou, ii) à manutenção da ordem pública (art. 20).

Ainda, nesse diploma legal, há expressa menção à inviolabilidade da vida privada (art. 21), por isso, a requerimento do interessado, o juiz pode adotar as providências necessárias para impedir ou fazer cessar ato contrário a essa garantia. Observa-se que o referido dispositivo, ao deixar a cargo do juiz decidir quais serão as 'providências necessárias' a serem adotadas, realça a necessidade de que haja

---

[209] BRASIL. **Lei 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 20 jan. 2017.

[210] O Superior Tribunal de Justiça por meio do julgamento do REsp 1195995 / SP, em 22/03/2011, cujo acórdão foi relatado pelo Ministro Massami Uyeda, entende que "[...] o direito à intimidade, não é absoluto, aliás, como todo e qualquer direito individual. Na verdade, é de se admitir, excepcionalmente, a tangibilidade ao direito à intimidade, em hipóteses em que esta se revela necessária à preservação de um direito maior, seja sob o prisma individual, seja sob o enfoque do interesse público. Tal exame, é certo, não prescinde, em hipótese alguma, da adoção do princípio da dignidade da pessoa humana, como princípio basilar e norteador do Estado Democrático de Direito, e da razoabilidade, como critério axiológico." (BRASIL. Superior Tribunal de Justiça. **REsp 1195995/SP**. Danos morais e materiais decorrentes de exame de HIV não solicitado. Relatora: Ministra Nancy Andrighi, Rel. p/ Acórdão: Ministro Massami Uyeda. Órgão Julgador: Terceira Turma. Data do julgamento: 22/03/2011.Publicação: DJe 06/04/2011. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento https://ww2.stj.jus.br/processo/revista/documento>. Acesso em: 28 nov. 2016)

uma atuação específica de todo o ordenamento na proteção da privacidade da pessoa humana, que resulte em uma resposta eficaz aos riscos que hoje corre[211].

O Superior Tribunal de Justiça, no julgamento do caso *scoring*, em sede de recursos repetitivos (tema 710)[212], que discutiu a natureza dos sistemas de *scoring* e a possibilidade de violação a princípios e regras do Código de Defesa do Consumidor, capazes de gerar indenização por dano moral, menciona os direitos da personalidade, referenciando os dispositivos do Código Civil (arts. 11 a 21), argumentou o STJ que,

> Por serem direitos inerentes à própria personalidade, apresentam como características a instransmissibilidade, a indisponibilidade e a irrenunciabilidade, consoante expresso no art. 11 do CC/2002. Constituem "direitos essenciais", sem os quais a personalidade restaria uma suscetibilidade completamente irrealizada e sem os quais os demais direitos subjetivos perderiam interesse para o indivíduo, tendo sido qualificados como direitos inatos ou naturais pela Declaração dos Direitos do Homem e do Cidadão, de 1789[213].

Diante do exposto, fica evidente a importância dos direitos da personalidade na vida do indivíduo, uma vez que assegura a sua integridade física e moral. A promoção desses direitos confere ao indivíduo o direito de decidir sobre a extensão de sua exposição, bem como o direito subjetivo contra terceiros e o próprio Estado, nos casos em que tiver violada a sua vida privada, podendo exigir que seja reparado, através de indenização.

4.3 O CÓDIGO DE DEFESA DO CONSUMIDOR

A Constituição Federal de 1988 estabelece, em seu artigo 5º, que ao Estado cabe promover a defesa do consumidor. Adiante, ao tratar da ordem econômica, assegura a todos existência digna, conforme os ditames da justiça social, considera a defesa do consumidor como um dos princípios a serem observados (art. 170, V). Por fim, a CF88 incumbiu ao Congresso Nacional a elaboração de um código de defesa do consumidor (art. 48), surgindo, nesse contexto, a Lei nº 8.078, de 11 de

---

[211] DONEDA, Danilo. Os direitos da personalidade no código civil. **Revista da Faculdade de Direito de Campos**, ano VI, nº 6, Jun. 2005.
[212] BRASIL. Superior Tribunal de Justiça, 2014.
[213] BRASIL. Superior Tribunal de Justiça, 2014, p. 30.

setembro de 1990, que passou a viger a partir de 12 de março de 1991 que instituiu o Código de Defesa do Consumidor (CDC)[214].

É partindo da precípua finalidade do Código de Defesa do Consumidor, que repousa em conferir uma máxima proteção ao indivíduo frente às relações de consumo, que os arquivos de consumo passaram a ser regulamentados pela Lei nº 8.078/90, com destaque aos artigos 43, primeiro dispositivo legal do ordenamento jurídico brasileiro que dispõe sobre banco de dados e cadastros, e, apesar de se referir a consumidores, disciplina uma série de requisitos aos quais os bancos de dados e cadastros devem respeitar, dentre eles, serem objetivos, claros, verdadeiros e em linguagem de fácil compreensão (§ 1°, art. 43, CDC), exigindo o consentimento expresso, mediante a forma escrita, do consumidor para que, somente a partir disso, possam ser abertos bancos de dados (§2º, art. 43, CDC), considerando ainda esses bancos de dados como entidades de caráter público, atraindo assim a incidência da proteção prevista no art. 5º, LXXII, a, CF88 que trata do *habeas data*.

Na configuração do direito à proteção de dados pessoais, Doneda[215] faz referência aos *Fair Information Principles* que consistem nos princípios específicos ao tratamento desse direito: a) princípio da publicidade (ou da transparência), para o qual a existência de um banco de dados com dados pessoais demanda conhecimento público; b) princípio da exatidão, os dados armazenados devem ser fiéis à realidade; c) princípio da finalidade, segundo o qual qualquer utilização de dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados; d) princípio do livre acesso, ao indivíduo deve ser garantido o acesso ao banco de dados no qual suas informações estão armazenadas; e) princípio da segurança física e lógica, os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. Para o autor, a aplicação de tais princípios representa uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua afirmação como um direito fundamental nos ordenamentos jurídicos.

Os *Fair Information Principles* constam nas orientações da OCDE sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais. Eles representam diretrizes cuja finalidade é harmonizar as legislações nacionais sobre privacidade e o respeito aos direitos humanos, ao passo que reconhecem o

[214] BRASIL. Lei 8.078, 1990.
[215] DONEDA, op. cit., 2011, p. 101.

interesse comum em proteger a privacidade e as liberdades individuais. São princípios básicos elaborados em setembro de 1980 pelos países membros da OCDE[216].

No Brasil os *Fair Information Principles* podem ser lidos no artigo 43 da Lei nº 8.078, de 11/09/1990 (CDC): no §4° (princípio da publicidade), ao passo que atribui o caráter público aos bancos de dados e cadastros relativos a consumidores, e tal princípio refere-se a obtenção pelo indivíduo de todas as informações referente aos responsáveis pelo tratamento dos dados, ou seja, garante a obtenção de todas informações sobre seus dados sem esforços; no §3° (princípio da exatidão) que garante o direito a imediata correção de informações incorretas, para esse principio segundo as orientações da OCDE os dados pessoais em tratamento devem ser exatos, exaustivos e atuais; no *caput* e no §1° (princípio do livre acesso); no §3º (princípio da segurança física e lógica), que impõe limitações no uso e divulgação dos dados, onde segundo orientações da OCDE exige-se medidas de segurança física, organizacionais e informativas. O princípio da finalidade pode ser lido via interpretação sistemática e teleológica desses enunciados normativos, esse princípio tem como condão impedir que novos propósitos sejam introduzidos de forma arbitrária e assegurar que as mudanças que eventualmente ocorram sejam compatíveis com os propósitos iniciais. Assim, tem-se aqui outro elemento que evidencia a afirmação implícita do direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro.

4.4 A LEI DO CADASTRO POSITIVO

A Lei nº 12.414, de 09 de junho de 2011, conhecida como Lei do Cadastro Positivo (LCP), 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, sendo regulamentado pelo Decreto nº 7.829 de 17/10/2012[217].

---

[216] OECD. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,** 23 set. 1980, atualização em 2013. Disponível em: < http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 10 fev. 2017.

[217] BRASIL. **Decreto nº 7.829** de 17de outubro de 2012. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento,

Acerca do conceito de cadastro positivo Carlos Orcesi da Costa refere que,

> Cadastro de adimplemento é, pois, um complexo conjunto de dados e informações, abrangente apanhado do comportamento, da vida, e do histórico de consumo do cidadão, que permitirá ao concedente de crédito analisar a conveniência ou não de assumir o risco do financiamento. Supondo que a maioria das pessoas ainda pague em dia os seus compromissos, virá para premiar os bons, a médio prazo, com menores taxas de juros (como acontece, por exemplo, no mercado de seguros), e provavelmente dificultar ou segregar os maus[218].

Conforme consta da Lei nº 12.414/2011, banco de dados representa um conjunto de dados relativo a pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro (art. 2º, I); disciplina que somente poderão ser armazenadas informações: i) objetivas, aquelas descritivas dos fatos e que não envolvam juízo de valor, ii) claras, aquelas que possibilitem o imediato entendimento do cadastrado independentemente de remissão a anexos, fórmulas, siglas, símbolos, termos técnicos ou nomenclatura específica, iii) verdadeiras, aquelas exatas, completas e sujeitas à comprovação nos termos da LCP, e iv) de fácil compreensão, aquelas em sentido comum que assegurem ao cadastrado o pleno conhecimento do conteúdo, do sentido e do alcance dos dados sobre ele anotados; que sejam necessárias para avaliar a situação econômica do cadastrado (art. 3º, §§ 1º e 2º). Em síntese, o banco de dados disposto na LCP tem por finalidade o armazenamento de informações de adimplemento do cadastrado, para a formação do histórico de crédito.[219]

Ao regulamentar a formação de banco de dados de consumidores para fins de concessão de crédito, a Lei nº 12.414/11 proíbe que sejam armazenadas informações excessivas, ou seja, aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor (art. 3º, § 3º, I) e informações sensíveis, aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (art. 3º, § 3º, II). [220]

---

de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: < http://www.planalto.gov.br/ ccivil_03/_Ato2011-2014/2012/Decreto/D7829.htm>. Acesso em: 21 jan. 2017.

[218] COSTA, Carlos Celso Orcesi da, **Cadastro positivo** – Lei n. 12.414/2011 comentada artigo por artigo. São Paulo: Saraiva, 2012, p. 31.

[219] BRASIL, **Lei 12.414,** 2011b.

[220] BRASIL, **Lei 12.414,** 2011b.

A autorização prévia do consumidor, por meio de consentimento informado através de assinatura em instrumento específico ou em cláusula apartada, é requisito indispensável para a abertura de cadastro (art. 4º), devendo ressaltar que tal exigência refere-se à abertura do cadastro e não de anotação de informação em banco de dados, pois, para a LCP, uma vez autorizada a abertura do cadastro pelo cadastrado, as anotações em banco de dados independem de qualquer autorização e de comunicação ao individuo.[221]

Assim como anteriormente analisado com dispositivos do CDC, os *Fair Information Principles* podem ser observados em diversos dispositivos da Lei do Cadastro Positivo: no art. 5º, IV, V (princípio da publicidade); nos §§ 1° e 2º do art. 3º (princípio da exatidão); no arts. 5º, II, e 6º (princípio do livre acesso); no §3º (princípio da segurança física e lógica), no § 3º do art. 3º, e art. 5º, VII (princípio da finalidade).

Ao se avançar no exame da legislação e doutrina que cuidam da matéria de proteção de dados pessoais, observa-se que os princípios específicos surgem como um dos instrumentos norteadores da regulação, tornando-se indispensáveis para a busca de um efetiva proteção de dados pessoais.

Assim, a partir do ensinamentos de Humberto Ávila, segundo o qual, os "princípios não são necessariamente meras razões ou simples argumentos afastáveis, mas também estruturas e condições inafastáveis"[222], evidencia-se que os princípios podem não representar única e incontestável solução para o problema da efetividade da proteção de dados pessoais, mas como visto aqui, o arcabouço principiológico específico que gravita sobre as regras e exigências para coleta, tratamento e usos dos dados pessoais, no contexto do *big data*, por certo, são o ponto de partida para que as estratégias pensadas na atualidade - que serão abordadas no item 4.8.1 - sejam repensadas a fim de que se possa falar em efetiva proteção dos dados pessoais diante do *big data.*

[221] BRASIL, **Lei 12.414,** 2011b.
[222] ÁVILA, Humberto. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. 16. ed. São Paulo: Malheiros Editores, 2015, p. 158-159.

4.5 A LEI DE ACESSO À INFORMAÇÃO

A Lei nº 12.527, de 18 de novembro 2011[223], também conhecida como Lei de Acesso à Informação (LAI), trata sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso à informação, conforme previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; ao regime dessa lei estão subordinados os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público e as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios, e até as entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.

Importa destacar da LAI, no tocante à proteção de dados pessoais, que apesar de estabelecer diretrizes que deverão ser respeitadas a fim de assegurar o direito fundamental de acesso à informação, como observância da publicidade como preceito geral e do sigilo como exceção, divulgação de informações de interesse público, independentemente de solicitações (art. 3º, I, II), incumbe aos órgãos e entidades do poder público assegurar a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso (art. 6º, III), ou seja, inobstante a finalidade precípua de promover o acesso à informação que consubstancia um efetivo controle social pelos indivíduos, deve ser respeitada a intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais (art. 31) quando do tratamento das informações pessoais. [224]

Ao tratar das informações pessoais no seu art. 31, a LAI institui que o acesso às informações pessoais será restrito a agentes públicos legalmente autorizados e à

---

[223] BRASIL. **Lei 12.527**, de 18 de novembro 2011c. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 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: 21 jan. 2017.
[224] BRASIL. **Lei 12.527**, 2011c.

pessoa a que elas se referirem, independente de classificação de sigilo e pelo prazo de 100 (cem) anos a contar de sua produção (art. 31, § 1º, I), somente podendo ser divulgadas ou acessadas por terceiros em duas hipóteses: i) diante de previsão legal, ou ii) mediante consentimento expresso da pessoa a que se referirem (art. 31, § 1º, II).[225]

Quando se refere à hipótese de divulgação ou acesso por terceiros às informações pessoais, mediante consentimento expresso da pessoa, a Lei nº 12.527/2011 traz um rol de exceções a esta regra (art. 31, § 3º), dispensando tal consentimento, quando as informações forem necessárias: a) à prevenção e diagnóstico médico, nos casos em que a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico, b) para 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, restando aqui presente a obrigatoriedade da anonimização do indivíduo, c) ao cumprimento de ordem judicial, d) à defesa de direitos humanos, e) à proteção do interesse público e geral preponderante.[226]

Um aspecto que chama atenção da Lei de Acesso à Informação é que não poderá ser invocada a restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa 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 (art. 31, § 4º), em que o direito a ter restringido o acesso às suas informações pessoais é mitigado.[227]

A LAI prevê a responsabilização daquele que fizer uso indevido de informações pessoais a que tiver acesso (art. 31, § 2º), constituindo no rol das condutas ilícitas que ensejam responsabilidade do agente público o ato de divulgar ou permitir a divulgação, ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal (art. 32, IV).[228]

---

[225] BRASIL. **Lei 12.527**, 2011c.
[226] BRASIL. **Lei 12.527**, 2011c.
[227] BRASIL. **Lei 12.527**, 2011c.
[228] BRASIL. **Lei 12.527**, 2011c.

4.6 O MARCO CIVIL DA INTERNET

Seja para trazer uma segurança jurídica para os usuários da internet, ou ainda para garantir a proteção de direitos fundamentais na internet, a Lei nº 12.965, de 23 de abril de 2014, que recebeu o título de Marco Civil da Internet (MCI)[229], foi aprovada, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil, daí ser considerada como uma lei principiológica, o que, deveras, parece ser mais adequado, posto que tem como objeto regular um espaço em constante modificação no universo das tecnologias, como no caso a internet.

Apesar de disciplinar o uso da internet no Brasil, a Lei nº 12.965/14 declina alguns de seus dispositivos para proteção dos dados pessoais, a começar por estabelecer o desenvolvimento da personalidade como um dos fundamentos que disciplinam uso da internet no Brasil (art. 2º, II), bem como elege entre seus princípios a proteção da privacidade e proteção dos dados pessoais (art. 3º, II, III).[230]

No capítulo II, que trata dos direitos e garantias dos usuários, o Marco Civil da Internet, assegura aos usuários da rede (art. 7º, I, VII, VIII, IX, X) a proteção da privacidade e de seus dados pessoais: a) a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; b) 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; c) informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais; d) a necessidade de consentimento expresso do individuo sobre a coleta, uso, armazenamento e tratamento de seus dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; e) exclusão definitiva dos dados pessoais[231] que tiver fornecido a determinada aplicação de internet, a seu

---

[229] BRASIL. **Lei 12.965**, de 23 de abril de 2014a. 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 21 jan. 2017.

[230] BRASIL. **Lei 12.965,** 2014a.

[231] Do ponto de vista de Cristina Sílvia Alves Lourenço e Maurício Sullivan Balhe Guedes, apesar de o art. 7º, X, do Marco Civil assegurar ao usuário um direito público subjetivo de exclusão definitiva dos dados pessoais, não há uma preocupação acerca de que modo será realizada essa exclusão, entendem que a exclusão não se pode dar somente do sistema operacional da plataforma acessível conectada à internet, mas sim do servidor principal, a fim de evitar que sejam restaurados ou novamente utilizados, esclarecem que a exclusão deve ser definitiva e não mera exclusão. (LOURENÇO, Cristina Sílvia Alves; GUEDES, Maurício Sullivan Balhe. A internet e o direito à

requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas no MCI.[232]

Adiante, ao dispor sobre a proteção aos registros, aos dados pessoais e às comunicações privada, o MCI estabelece que a guarda e a disponibilização de dados pessoais devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (art. 10), estabelecendo que o provedor responsável pela guarda somente será obrigado a disponibilizar os dados pessoais ou informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial (art. 10, § 1º), determinando ainda que 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 (art. 11).[233]

O Decreto nº 8.771, de 11 de maio de 2016 que regulamenta o Marco Civil[234] trata das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicando procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, bem como aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações.

É no capítulo III do Decreto nº 8.771/16 que é abordada a proteção aos registros, aos dados pessoais e às comunicações privadas, especificando o que considera dados cadastrais[235] (art. 11), sendo aqueles que se referem a filiação,

---

exclusão definitiva de dados pessoais na experiência brasileira. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** São Paulo: Atlas, 2014, pp. 559-573.)

[232] BRASIL. **Lei 12.965**, 2014a.

[233] BRASIL. **Lei 12.965**, 2014a.

[234] BRASIL. **Decreto nº 8.771,** de 11 de maio de 2016. Regulamenta a Lei nº 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: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 21 jan. 2017.

[235] Ao tratar sobre o Decreto nº 8.771/16 no Seminário sobre Privacidade e Proteção de Dados Pessoais, promovido pelo Comitê Gestor da Internet no Brasil (CGI.BR), Renato Leite Monteiro afirma que apesar de haver um tratamento diferenciado para dados cadastrais, esses dados não deixam de ser pessoais. A única diferença entre eles está nos meios para obtenção desses dados. Enquanto os

endereço e qualificação pessoal (nome, prenome, estado civil e profissão), e define dados pessoais[236] como sendo aqueles relacionados à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (art. 14, I) e o que venha a ser tratamento de dados pessoais, considerando ser 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 (art. 14, II).[237]

4.7 AS PROPOSIÇÕES LEGISLATIVAS PARA PROTEÇÃO DE DADOS PESSOAIS

No ordenamento jurídico brasileiro ainda não existe lei específica que trate da proteção de dados pessoais. Como visto anteriormente, a matéria encontra-se distribuída de maneira esparsa e singela em alguns diplomas, demandando, por vezes, um esforço hermenêutico para situar a proteção dos dados pessoais, seja a partir do art. 5º, X, XII, LXXII, § 2º, CF88, Lei nº 9.507/97, art. 21 do Código Civil, art. 43 do Código de Defesa do Consumidor, Lei nº 12.414 (LCP), Lei nº 12.527 (LAI) ou Marco Civil da Internet, não sendo este um rol exaustivo de legislação esparsa que possa conceber a proteção de dados pessoais.

Em razão da ausência de uma legislação específica e considerando a importância de ver protegidos os dados pessoais na rede e fora dela é que

---

pessoais exigem ordem judicial, os dados cadastrais podem ser requisitados diretamente pelas autoridades administrativas, sem ordem judicial. (ROVER, Tadeu. **Decreto falhou ao regulamentar sanções do Marco Civil da Internet,** 25 ago. 2016. Disponível em: <http://www.conjur.com.br/2016-ago-25/decreto-falhou-regulamentar-sancoes-marco-civil-internet>. Acesso em 27 nov. 2016.)

[236] Os conceitos de dado pessoal e tratamento de dados pessoais previstos no Decreto nº 8.771/16 foram incorporados pelo Projeto de Lei (PL) nº 5276/2016 - apensado ao PL 4060/2012 - que trata especificamente sobre a proteção de dados pessoais (art. 5º, I, II), se assemelhando aos conceitos também utilizados pelo PL nº 4060/2012 que considera dado pessoal "[...] qualquer informação que permita a identificação exata e precisa de uma pessoa determinada" e tratamento de dados "toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados que permitam o armazenamento, ordenamento, conservação, atualização, comparação, avaliação, organização, seleção, extração de dados pessoais" (art. 7º, I, II). (BRASIL, **Projeto de Lei nº 4060/2012**, p. 2-3. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra; jsessionid= 0CFA5ADBBA 5E762EB8 E42924B7AB7842.proposicoesWebExterno1?codteor=1001750&filename=PL+4060/2012>. Acesso em 5 fev. 2017).

[237] BRASIL. **Lei 12.965**, 2014a.

propostas legislativas tramitam no Congresso Nacional a fim de sanar essa lacuna e aproximar o Brasil das legislações de países que avançam no tema e consolidam a proteção de dados pessoais. Não é ir muito longe: a Colômbia (já reportada) e o Uruguai, em agosto de 2008, promulgou a Lei nº 18.331 – proteção de dados pessoais e ação de *habeas data*[238].

O Projeto de Lei nº 5.276/2016 apresentado pelo Poder Executivo em 13 de maio de 2016 dispõe sobre tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, é resultado de um amplo debate[239] promovido pelo Ministério da Justiça, tendo seu texto sido elaborado em parceria com o Centro de Estudos sobre Tecnologias Web (Ceweb), vinculado ao Núcleo de Informação e Coordenação do Ponto BR (Nic.br) e com o Instituto Nacional de Ciência e Tecnologia para a Web (InWeb), da Universidade Federal de Minas Gerais, conforme aponta mensagem da Presidência[240], tendo sido influenciado pelo contexto internacional, notadamente a Resolução da ONU 25 de novembro de 2013 sobre "Direito à Privacidade na Era Digital"[241], estando o Brasil atrás de 109 países que já possuem normas específicas sobre o tema.

Com regime de prioridade na sua tramitação, o PL nº 5.276/2016, apensado ao PL nº 4060/2012 trata do mesmo objeto e de autoria do deputado Milton Monti (PR/SP). Lista no seu art. 6º dez princípios cujas atividades de tratamento de dados pessoais deverão observar, sendo eles, a boa-fé, a finalidade, adequação,

---

[238] URUGUAI. **Lei nº 18.331** - protección de datos personales y acción de "habeas data", 6 ago. 2008. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp6739900.htm>. Acesso em 15 nov. 2016.

[239] Para mais informações ver o relatório final da consulta pública sobre o anteprojeto de Lei de Proteção de Dados Pessoais (ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNLOGIA. **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, 2016. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 27 nov. 2016.)

[240] BRASIL **Projeto de Lei nº 5.276/2016**c. 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/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em 27 nov. 2016.

[241] A mencionada resolução "[...]ressalta que o direito à privacidade é um direito humano e afirma, pela primeira vez, que as pessoas têm os mesmos direitos tanto *offline* quanto online. Ele reconhece que a segurança pública pode justificar a coleta de determinadas informações, mas reafirma que os países devem cumprir suas obrigações para com o direito internacional. O texto pede que os Estados estabeleçam ou mantenham uma fiscalização independente, uma vigilância nacional que assegure a transparência e a prestação de contas quanto a fiscalização, recolhimento de dados e/ou intercepção de comunicações." (ASSEMBLEIA Geral da ONU aprova resolução de Brasil e Alemanha sobre direito à privacidade, 19 dez. 2013. Disponível em: <https://nacoesunidas.org/assembleia-geral-da-onu-aprova-resolucao-de-brasil-e-alemanha-sobre-direito-a-privacidade/>. Acesso em: 27 nov. 2016.)

necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação.[242]

O PL 5.276/2016 estabelece as hipóteses que permitem o tratamento de dados pessoais, estando presente no art. 7º a necessidade de consentimento livre, informado e inequívoco pelo titular, por escrito por qualquer outro meio que o certifique (art. 9º), para cumprimento de uma obrigação legal pelo responsável, pela administração pública em caso de execução de políticas públicas, para realização de pesquisa histórica, científica ou estatísticas, garantindo, sempre que possível, a anonimização dos dados pessoais, na hipótese de execução de um contrato do qual é parte o titular, para o exercício regular de direitos em processo judicial ou administrativo, para proteção da vida ou da incolumidade física do titular ou de terceiro, para tutela da saúde, quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto quando prevalecerem interesses ou direitos do titular, em especial se for menor de idade.[243]

É assegurado ao titular dos dados pessoais, nos casos de tratamento de seus dados, o acesso facilitado às informações de forma clara, adequada e ostensiva sobre a finalidade específica, forma e duração do tratamento, a identificação e contato do responsável, assim como a quem podem ser comunicados os seus dados e o âmbito dessa difusão, as responsabilidades dos agentes que realizarão o tratamento e direito do titular à acessar os dados, retificá-los ou revogar o consentimento, denunciar ao órgão competente o descumprimento das disposições da lei.

Um dos aspectos relevantes do PL 5.276/2016 é a exigência do consentimento do titular para o tratamento de dados pessoais e dados sensíveis, em que para a primeira categoria de dados o consentimento deve ser livre, informado e inequívoco, já para os dados sensíveis o consentimento deve ser livre, inequívoco, informado, expresso e específico (art. 11, I), ou seja, para os dados sensíveis que segundo o PL considera aqueles dados pessoais que recaem sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos (art. 5º, III), além das características

[242] BRASIL. Projeto de Lei nº 5.276/2016c.
[243] BRASIL. Projeto de Lei nº 5.276/2016c.

do consentimento para os dados pessoais, deve ser expresso e específico; dispõe ainda que o consentimento pode ser revogado a qualquer momento (art. 9º, § 5º).[244]

Questão emblemática no PL 5.276/2016 reside quanto ao tratamento de dados anonimizados aos quais não é conferida proteção, salvo quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido (art. 13). Ocorre que o avanço tecnológico muda os conceitos de dados anônimos e sensíveis, nesse cenário tem-se o *big data*[245], que, em razão do aumento de quantidade e variedade de informações, facilita a reidentificação[246].

Durante a consulta pública sobre o anteprojeto de proteção de dados pessoais que deu origem ao PL 5.276/2016, realizada entre 28 de janeiro e 05 de julho de 2015, foi questionado se os dados anônimos deveriam ser considerados dados pessoais, o relatório final dessa consulta pública sintetizou as posições daqueles que defendem que sim, como Joana Varon, sob o argumento de que:

> [...] adicionar dados anônimos como novo inciso é inconcebível. Dados anônimos também são dados pessoais e, portanto, dentro do escopo da lei, inclusive porque a "autoridade de proteção de dados" deve fiscalizar técnicas de anonimização de acordo com o estado da arte e padrão tecnológico, ou seja, aquele que não seguir a forma correta de anonimização será responsabilizado[247].

Em contraponto, a ABRANET, Claro, IAB, CNseg, Câmara BR e Vivo defendem posição contrária à inclusão dos dados anônimos no âmbito de proteção da lei sobre dados pessoais, argumentando que a anonimização dos dados permite

---

[244] BRASIL. Projeto de Lei nº 5.276/2016c.

[245] "O termo que se refere a gigantescas massas de dados armazenados em sistemas, agregando inúmeras informações de variadas fontes. Esses gigantes bancos de dados podem ser analisados e estudados de maneiras inovadoras, facilitando a extração de informações e correlações antes indisponíveis ou de difícil acesso". (ABREU, Jacqueline de Souza. **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, 08 jul. 2016. Disponível em: < http://jota.info/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016>. Acesso em: 27 nov. 2016.)

[246] Exemplo da impossibilidade de anonimização perfeita é o caso da Netflix que em outubro de 2006 ao lançar o "Prêmio Netflix", disponibilizou 100 milhões de registros de locação de filmes de quase 500 mil usuários, oferecendo um prêmio de US$ 1 milhão para a equipe que conseguisse melhor em pelo menos 10% o sistema de recomendação de filmes para seus usuários. A Netflix anonimizou os dados, retirando a identificação pessoal dos usuários, porém, um usuário acabou sendo identificado, uma mãe e lésbica não assumida na conservadora região do Meio-Oeste dos Estados Unidos, que por causa disso processou a Netflix sob o pseudônimo "Jane Doe". (MAYER-SCHONBERGER; CUKIER, 2013.)

[247] ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNLOGIA, op. cit., 2016, p. 58.

com que decisões e resultados sejam conseguidos sem que os indivíduos envolvidos sejam identificados[248].

Sendo o processo de anonimização de dados pessoais reversível, na medida em que as informações podem ser reidentificadas a partir das análises de *big data*, não se pode afastar dos dados anônimos a proteção que se busca conferir aos dados pessoais.

A simples possibilidade de um dado anonimizado levar à identificação de um individuo em decorrência dos avanços tecnológicos, por si, já sinaliza que a legislação específica que tanto se advoga ser necessária não pode quedar-se inerte a essa questão, sob pena de antes mesmo de entrar em vigência, já estar fadada à inefetividade.

Ressalta-se que conferir aos dados anônimos a mesma proteção dada aos dados pessoais, incluindo no escopo da legislação específica sobre a matéria, não significa proibir que o Brasil faça uso da tecnologia do *big data*, do contrário, apenas representa que, ao tratar dados para usufruir das vantagens dessa nova tecnologia, que o faça sob a égide das regras que tem como finalidade proteger a intimidade, a vida privada e o livre desenvolvimento do indivíduo, em atenção aos princípios que devem ser observados nas atividades de tratamento de dados pessoais, principalmente aqui o da finalidade, transparência e segurança.

O PL 5.276/2016 cria ainda a figura de um órgão competente designado para zelar pela implementação e pela fiscalização da lei de proteção de dados pessoais (art. 53), que dentre suas atribuições estaria a aplicação de sanções administrativas àqueles que cometessem infrações às normas prevista pela lei, sanções essas escalonadas que vão desde multa simples a suspensão de funcionamento de banco de dados (art. 52), que não substituem a aplicação de outras sanções administrativas, civis ou penais (art. 52, § 2º), bem como, elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, realizar auditoria nos tratamentos de dados pessoais, editar normas sobre proteção de dados pessoais e privacidade, entre outras (art. 53).[249]

Ocorre que o PL 5.276/2016 não define com especificidade como será esse órgão competente. Em razão disso, tem-se discutido o formato desse órgão que terá como finalidade colocar em prática a Lei de Proteção de Dados Pessoais; nesse

[248] ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNLOGIA, op. cit., 2016.
[249] BRASIL. Projeto de Lei nº 5.276/2016c.

sentido, Marcel Leonardi defende a criação de uma autoridade federal independente, destacando como principais vantagens “[...] a consistência das interpretações, a especialização técnico-jurídica sobre o tema, a certeza regulatória e a independência necessárias para atuar de modo eficaz”[250].

O posicionamento de Laura Schertel Mendes acerca do controle e fiscalização da atividade de processamento de dados por autoridade administrativa é condição para a efetivação do direito fundamental à proteção de dados, referindo-se como exemplo o Conselho Administrativo de Defesa Econômica (CADE), autarquia federal, vinculada ao Ministério da Justiça com autonomia administrativa e política, órgão que no seu ponto de vista é um modelo a espelhar o órgão competente previsto no PL 5276/2016[251].

Destarte, ante a necessidade de proteger os dados pessoais e diante da ausência de lei específica sobre a matéria, os projetos de lei 4.060/2012 e 5.276/2016, que tratam especificamente sobre dados pessoais são medidas imprescindíveis.

Entretanto, várias foram as discussões acerca de algumas falhas encontradas nos projetos de lei, especificamente no último, mais detalhado, ressaltada aqui a questão da proteção jurídica aos dados anônimos da mesma forma conferida aos dados pessoais, pois, ao descuidar e negligenciar a proteção dos dados anônimos, corre-se o risco de tornar-se uma lei inefetiva, haja vista todo o contexto das novas tecnologias no qual os dados pessoais estão inseridos e são diariamente coletados para tratamento e análises.

4.8 A EFETIVIDADE DO ATUAL MODELO REGULATÓRIO PARA A PROTEÇÃO DE DADOS PESSOAIS

Hodiernamente, a regulamentação visando à proteção de dados pessoais tornou-se essencial para reverter a vulnerabilidade do indivíduo em face das novas tecnologias. A legislação tem sido utilizada pelos países que consolidaram a matéria, como ponto de partida para disciplinar direitos, deveres, instituir

---

[250] ANTONIALLI, Dennys et al. **[especial] Fiscalização:** como deve ser o “órgão competente”?, 15 jul. 2016. Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-fiscalizacao-como-deve-ser-o-orgao-competente-2/>. Acesso em: 27 nov. 2016, n.p.

[251] ANTONIALLI, op. cit., 2016, n.p.

responsabilidades e criar mecanismos a fim de tutelar a privacidade e os dados pessoais de cada indivíduo. É fundamental uma regulamentação que seja efetiva, tanto no sentido de precaver quanto de reparar eventuais danos, tendo em vista o estado de perigo que os riscos podem gerar, bem como a incerteza e a insegurança trazidos com as inovações tecnológicas.

No campo em que estão inseridos direito, ciência e tecnologia, é inevitável abordar os riscos. Regina Linden Ruaro e Carlos Alberto Molinaro explicam que,

> Todo o risco produz uma situação de perigo, de incerteza e de insegurança, reclama, pois, um tratamento jurídico fundado na prevenção ou na precaução. Em qualquer caso reclama regulação. [...] O direito pode cooperar para a solução. Risco implica responsabilidade, responsabilidade enquanto obrigação de responder pelo dano produzido tenha este como origem causa natural ou antrópica[252].

Nesse contexto, o direito ao regular a coleta, tratamento e uso dos dados pessoais, especialmente no cenário do *big data,* somente poderá cooperar de fato com a solução para os riscos à privacidade do indivíduo quando de fato vislumbrar mecanismos eficazes para proteção dos dados pessoais. Assim, impõe-se o exame das estratégias e mecanismos pensados pelo direito a fim de salvaguardar as liberdades individuais, os direitos da personalidade e a dignidade humana.

A partir do marco regulatório sobre a proteção de dados pessoais, evidencia-se algumas estratégias tradicionais utilizadas para garantir a privacidade dos indivíduos: a) consentimento individual, b) opção de exclusão e c) anonimização; estas, por sua vez, nas lições de Viktor Mayer-Schonberger e Kenneth Cukier[253] restam ineficientes considerando a prática do *big data*.

No relatório "*Big data and privacy: a technological perspective*"[254] emitido em maio de 2014 ao Presidente dos Estados Unidos o *President's council of advisors on science and technology*[255] (PCAST) se examina a natureza da tecnologia atual de

---

[252] RUARO; MOLINARO, op. cit., 2014, p. 54-55.
[253] MAYER-SCHONBERGER; CUKIER, op. cit., 2013.
[254] USA, President's Council of Advisors on Science and Technology (PDCAST). **Big data and privacy:** a technological perspective, maio 2014. Disponível em: < https://www.whitehouse.gov/sites/default/files/ microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em 29 dez. 2016.
[255] É um grupo formado por cientistas e engenheiros que prestam consultoria sobre tecnologia ao presidente dos Estados Unidos e demais departamentos e agencias federais, realiza recomendações referente a ciência, tecnologia e inovação e influência pontencial destas nas escolhas da presidência. Para maiores informações consultar o endereço www.whitehouse.gov/ostp/pcast (USA, President's Council of Advisors on Science and Technology (PDCAST). **Big data and privacy:** a technological

gerenciamento e análise de *big data,* principalmente a sua evolução, a capacidade e tendências que implicam na concepção e execução de políticas públicas para proteção da privacidade no contexto dessa nova tecnologia. A PCAST acredita que os benefícios da tecnologia de *big data* são maiores do que quaisquer novos danos.

Ao tratar das estratégias de proteção dos dados pessoais, o relatório "*Big data and privacy: a technological perspective*" demonstra que a anonimização, o consentimento individual e a opção de exclusão no cenário do *big data* tornam-se ineficazes na proteção dos dados pessoais. Isto porque, conforme aponta o relatório no tocante ao processo de anonimização, à medida que se eleva o tamanho e a diversidade dos dados disponíveis levadas a efeito pelas características do *big data:* volume e variedade, abordadas no item 2.3.1, aumenta-se a probabilidade de se re-identificar indivíduos (ou seja, re-associar seus registros com seus nomes). Embora a anonimização possa continuar a ser útil como uma salvaguarda, não é, por si só, suficiente para uma proteção eficaz dos dados pessoais no contexto do *big data,* nesse sentido Viktor Mayer-Schönberger e Kenneth Cukier explicam que,

> A anonimização se refere à exclusão de quaisquer dados pessoais de um banco de dados, como nome, endereço, número do cartão de crédito, data de nascimento ou identidade. Os dados resultantes podem, então, ser analisados e compartilhados sem comprometer a privacidade de ninguém. A prática funciona num mundo de pequenos dados. Mas o big data, com o aumento de quantidade e variedade de informações, facilitam a reidentificação[256].

O relatório da PDCAST trata ainda da notificação e consentimento individual como a prática de exigir dos indivíduos a autorização de forma positiva para o acesso e tratamento de seus dados pessoais às práticas de coleta de suas informações pessoais seja por meio de aplicativos, programa ou serviço da *Web*, afirma que somente em algum mundo de fantasia os usuários realmente leem esses avisos e compreendem suas implicações antes de clicar para consentir.

O problema conceitual com a notificação e o consentimento segundo o PDCAST é que ele coloca fundamentalmente a carga da privacidade e proteção dos dados sobre o indivíduo. A notificação e o consentimento criam uma situação de

---

perspective, maio 2014. Disponível em: < https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>. Acesso em 29 dez. 2016).

[256] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013, p. 108.

desigualdade de condições na negociação entre provedor e usuário. O indivíduo se depara com um conjunto de termos mediante adesão, sem possibilidade de negociação, em que dispõe de apenas alguns segundos para processar, analisar e dispor sobre seus dados. A PCAST acredita que a responsabilidade pela utilização de dados pessoais de acordo com as preferências do utilizador deve recair sobre o provedor e não com o usuário.

Somados estes argumentos, conclui-se que o consentimento individual é mecanismo insuficiente para proteção de dados pessoais. Laura Schertel Mendes sugere ainda que:

> [...] o consentimento informado e consciente do titular dos dados apesar de ser indispensável gera alguns problemas: i) o problema do não consentimento excluir o titular do mercado de consumo e da sociedade; ii) o problema da violação da proteção de dados pessoais, após o tratamento ter sido consentido pelo titular dos dados; iii) a questão do consentimento aplicado ao tratamento dos dados sensíveis que ora são restringidos ou proibidos total ou parcialmente pelas legislações. Em razão das dificuldades acima mencionadas, entende-se melhor evitar a transposição do consentimento negocial, aplicado aos mecanismos contratuais tradicionais, à disciplina da proteção de dados. De outro lado, como exercício da autodeterminação do indivíduo este tem a prerrogativa de revogar o consentimento tanto em relação à autorização para o tratamento (coleta e processamento de dados), quanto em relação à circulação dos dados.[257]

Nesse mesmo sentido, ao tratar do consentimento para as condições de uso e políticas de privacidade nas redes sociais, Pablo Schiavi adverte que,

> Como criterio general, cabe señalar que las redes sociales y plataformas colaborativas disponen de avisos legales, condiciones de uso y políticas de privacidad, aunque en ocasiones, redactadas en um lenguaje de difícil comprensión para el usuario. De esta forma, y a pesar de encontrarse recogidas en el sitio web, no alcanzan su finalidad última: que el usuario comprenda el objeto, la finalidad y el plazo para el que son recabados y tratados sus datos personales.[258]

Dessa forma, o consentimento concebido como estratégia que visa à proteção de dados pessoais é insuficiente, pois onera o indivíduo transportando para este a responsabilidade quanto à disponibilização de suas informações pessoais sem que detenha o livre e necessário esclarecimento de quais informações estão

---

[257] SCHIAVI, Pablo. La protección de los datos personales en las redes sociales, **AeC - Revista de Direito Administrativo e Constitucional**, Belo Horizonte, ano 13, n. 52, abr. / jun. 2013, p. 12. Disponível em: < http://www.revistaaec.com/index.php/revistaaec/article/view/137>. Acesso em 11 fev. 2017. Traduzimos.

[258] SCHIAVI, 2013, p. 12.

sendo cedidas e para quais fins. Ademais, assegurar ao indivíduo o direito de somente ter coletados e analisados seus dados pessoais, mediante seu consentimento faz com que, quando se depare com situação na qual discorde dos termos de coleta e uso e políticas de privacidade, esteja privado do uso das ferramentas da sociedade da informação, levando à sua exclusão como individuo que se coloca na condição de 'invisível' e 'desconectado'. A ideia de consentimento é fictícia, ao passo que não há poder de controle do individuo, mas simplesmente poder de delegar a outrem autorização para coletar e fazer uso de seus dados independente da finalidade.

A opção de exclusão que confere ao indivíduo o direito de não deixar rastro eliminando informações pessoais que estejam em bancos de dados também torna-se inefetiva no cenário do *big data*, pois acabam por excluir o indivíduo considerando que suas informações o representam como integrante da sociedade da informação, ou por coloca-lo em risco, como no caso do Street View, da Google:

> Os carros coletam imagens de estradas e casas em muitos países. Na Alemanha, a Google enfrentou protestos do público e da mídia. As pessoas temiam que as imagens de suas casas e jardins pudessem ajudar quadrilhas de ladrões na escolha de alvo lucrativos. Sob pressão regulatória, a Google concordou em permitir que as imagens das casas fossem embaçadas. Mas a opção de exclusão é visível no Street View - você nota as casas ofuscas -, e os ladrões podem interpretar o sinal como indício de alvos especialmente bons[259].

Neste sentido, diante de todo o contexto dissertado neste trabalho, pode-se afirmar que o atual modelo regulatório para a proteção de dados pessoais é inefetivo, a partir da concepção de efetividade (eficácia social) distinguida da eficácia jurídica vislumbrada nas lições de Sarlet:

> [...] eficácia jurídica como a possibilidade (no sentido de aptidão) de a norma vigente (juridicamente existente) ser aplicada aos casos concretos e de – na medida de sua aplicabilidade – gerar efeitos jurídicos, ao passo que a eficácia social (ou efetividade) pode ser considerada como englobando tanto a decisão pela efetiva aplicação da norma (juridicamente eficaz), quanto o resultado concreto decorrente – ou não – desta aplicação.[260]

---

[259] MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana. Tradução Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013, p. 107.

[260] SARLET, op. cit., 2011, p. 240

Tampouco é efetivo tal modelo regulatório na definição de efetividade presente na doutrina de Luís Roberto Barroso, para o qual,

> "[...] significa a realização do Direito, o desempenho concreto de sua função social. [...] a materialização, no mundo dos fatos, dos preceitos legais e simboliza a aproximação, tão íntima quanto possível, entre o *dever-ser* e o *ser* da realidade"[261]

A legislação brasileira, assim como as iniciativas de leis que preveem a necessidade do consentimento expresso do individuo sobre a coleta, uso, armazenamento e tratamento dos dados pessoais diferenciam dados anônimos de dados pessoais, conferindo proteção jurídica somente para a segunda categoria, assegurando o direito de exclusão dos dados pessoais de forma literal sem atentar ao contexto das novas tecnologias e especificamente do *big data*; considera-se, porém, que elas são despidas de efetividade, pois, apesar de serem dotadas de eficácia jurídica, regulamentando o tratamento de dados pessoais, não atingem o resultado emanado pela norma, que se refere à 'proteção dos dados pessoais' ou 'à privacidade', como se queira dizer.

Apesar de todos os esforços, o indivíduo estará vulnerável ao processo de reidentificação dos dados anônimos que revelarão informações pessoais, à coleta desenfreada de dados disponibilizados *online* e *off-line* nas mais variadas fontes de coleta, e, por fim, a condição refém das ferramentas da sociedade da informação sob a qual impõe consentir às grandes empresas a coleta, tratamento e uso de seus dados sob pena de ver excluído dos bens e serviços por elas oferecidos.

A maior conclusão a que pode-se vislumbrar é que o direito fundamental à proteção de dados pessoais no Brasil é violado, é inefetivo, possui um déficit legiferante e está pendente de uma resposta jurídico-normativa que desenvolva a sua importância na Sociedade da Informação.

[261] BARROSO, op. cit., 2010, p. 221; suprimimos; grifos do autor.

5 CONCLUSÕES

Diante do que foi exposto no presente trabalho, os objetivos delineados no início desta pesquisa tem o fim de contribuir para os estudos sobre uma efetiva proteção jurídica dos dados pessoais, no cenário das novas tecnologias, especificamente do *big data.* Todo e qualquer dado pode ser pessoal, a partir das análises de correlação e processo de reidentificação que tornam insuficiente a técnica de anonimização do indivíduo.

Evidenciou-se que as inovações tecnológicas trazem consigo valores econômicos, sociais e científicos para a sociedade, materializadas principalmente a partir da produção de bens e serviços. O *big data,* como visto, surgiu nesse contexto como ferramenta com aptidão para extrair e revelar novas ideias a partir da grande quantidade de dados que são disponibilizadas em escalas sem precedentes na internet, à disposição das grandes corporações. Tem-se que não somente é crescente o uso da internet pelas pessoas, como estas são cada vez mais vulneráveis, em decorrência da ausência de conhecimento sobre quais informações diariamente são disponibilizadas *online,* direta ou indiretamente, ao utilizar os serviços *online,* ao mover-se na sociedade da informação. Emerge, portanto, a necessidade de uma tutela efetiva dos dados pessoais, apta a produzir no mundo dos fatos os efeitos pretendidos pela legislação, aproximando o normativo e a realidade social.

Com a transição da sociedade disciplinar para sociedade de controle, respectivamente objeto dos estudos de Michel Foucault e Gilles Deleuze, foi possível demonstrar que ambas compartilham o atributo da ‘vigilância’ do individuo, diferenciando-se apenas nos mecanismos como cada um procede, estando para a sociedade de controle - a que vivemos - os bancos de dados automatizados como o projeto arquitetônico de vigilância pós-moderno, uma reinvenção do panóptico utilizado por Michel Foucalt para descrever a sociedade disciplinar.

Os bancos de dados automatizados, devido ao avanço tecnológico, tornaram possível a transição da informação dispersa para organizada; atrelado a isso, através do *big data,* que tem como características o volume, a variedade e velocidade, no processo de armazenamento, coleta e tratamento, respectivamente,

o individuo tem sido colocado em uma situação de vulnerabilidade representada pela ausência de controle sobre suas informações pessoais.

A partir da concepção que defende um sistema de direitos fundamentais aberto e flexível na Carta Magna de 1988, considerando ainda o direito à proteção de dados pessoais como desdobramento do direito à privacidade - este último consagrado no art. 5º, X, CF88 que salvaguarda a intimidade e vida privada - inserido no rol dos direitos da personalidade, aliado ao fundamento de que a proteção de dados pessoais encontra-se diretamente ligada à proteção dos direitos humanos e das liberdades individuais levados a efeito pelos documentos internacionais, e, por fim, reafirmados os direitos da personalidade com base constitucional fundada no pressuposto da dignidade humana, resta atribuir o *status* de direito fundamental à matéria de proteção de dados pessoais.

Inobstante o Brasil não possuir legislação específica sobre a proteção de dados pessoais, a matéria encontra guarida a partir da interpretação da Constituição Federal de 1988 e da legislação ordinária, como abordado no presente trabalho o Código Civil de 2002, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, Lei de Acesso à Informação e o Marco Civil da Internet, ainda que de forma reflexa. Assim, conclui-se que, apesar de o tratamento de dados pessoais ser abordado com a atenção que requer, apenas nos Projetos de Lei nº 4.060/2012 e 5.276/2016, que tramitam no Congresso Nacional, o individuo pode recorrer à Constituição Federal e legislação ordinária, pois, com esforço mútuo, esses instrumentos asseguram: (i) a inviolabilidade da intimidade e vida privada, (ii) instrumento jurídico-processual cuja finalidade é permitir o acesso e retificação dos dados pessoais em bancos de dados de caráter público, (iii) máxima proteção aos dados pessoais do consumidor, (iv) proteção jurídica aos dados sensíveis em bancos de dados, (iv) proteção a informação pessoal em detrimento do direito fundamental de acesso à informação, (v) proteção de dados pessoais como princípio que disciplinam o uso da internet no Brasil e informações claras e completas sobre coleta, uso, armazenamento e proteção dos dados pessoais e necessidade de consentimento expresso do indivíduo para as mesmas atividades já mencionadas.

A questão que sobressai nestas conclusões, a partir do marco regulatório do direito à proteção de dados pessoais no ordenamento jurídico brasileiro, é que os dispositivos legais que cuidam da matéria, no contexto das novas tecnologias,

especificamente do *big data,* não podem conferir uma solução para os problemas a que se destinam. O direito fundamental à proteção de dados pessoais no Brasil é violado, inefetivo, possui um déficit legiferante e está pendente de uma resposta jurídico-normativa que desenvolva a sua importância na Sociedade em Rede.

A necessidade de consentimento individual e expresso, as técnicas de anonimização e opções de exclusão no cenário do *big data* não são suficientes para que tenhamos uma efetiva proteção jurídica aos dados pessoais. Nesse sentido, o trabalho conclui pela necessidade de uma regulação que se baseie num arcabouço principiológico, em razão do processo tecnológico ser dinâmico, evolutivo e imprevisível. Engessar a legislação com mecanismos reversíveis e muitas vezes insuficientes e até inviáveis no contexto das novas tecnologias, como é o caso de pensar na obrigatoriedade de se exigir do individuo o consentimento a cada disponibilização de informação pessoal que coloca na rede, sendo que, como visto, os dados armazenados representam a pessoa na sociedade que passou a adotar a posição de membro-usuário-produto, torna-a inefetiva.

Em face da demanda por proteção advinda dos dados pessoais no contexto da sociedade da informação, tem-se que a noção de risco deve ser o norte para o enquadramento dos dados, devendo a regulação privilegiar os princípios da finalidade, responsabilidade e segurança. Representa dizer que há de se refletir sobre: qual a finalidade para coletar determinados dados, sejam eles pessoais ou não? Existe uma análise dos riscos na gestão dos dados que considere os impactos da coleta, tratamento e uso dessas informações? Há transparência na coleta e usos primários e secundários no processo de análises dos dados coletados? As respostas a estas reflexões por certo guiarão na elaboração de uma regulação que poderá surtir efeitos pretendidos na tutela da privacidade, trazendo à luz o direito do individuo de se dar conta do que está acontecendo, assim ele poderá ser o protagonista no processo de *big data* deixando a posição que se reduz a delegar às grandes empresas a coleta e tratamento de seus dados, como ocorre com a exigência do ‘consentimento’.

Portanto, constatou-se, que os princípios envoltos nesta temática e discorridos no texto têm papel fundamental para a efetividade da proteção de dados pessoais frente ao *big data*, tendo em vista que uma regulamentação que os considere e se desprenda das ‘velhas’ estratégias de consentimento, anonimização

e opção de exclusão, consideradas como suficientes para proteção dos dados, é mais adequada e eficaz. Os princípios da publicidade, da exatidão, da finalidade, do livre acesso, da segurança física, e especialmente da finalidade, responsabilidade e segurança quando considerados levarão a constatação da autonomia da proteção de dados pessoais.

REFERÊNCIAS

ABREU, Jacqueline de Souza. **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, 08 jul. 2016. Disponível em: < http://jota.info/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro-08072016>. Acesso em: 27 nov. 2016.

ALEMANHA, Lei Fundamental da República Federal da Alemanha, 1919, atualizada até 2011. Disponível em: <http://www.brasil.diplo.de/contentblob/3160404/ Daten/ 1330556/ Gundgesetz_pt.pdf>. Acesso em 04 fev. 2017, p. 18.

ALEMANHA. **Federal Data Protection Act (BDSG)** In the version promulgated on 14 January 2003. Publicação: Federal Law Gazette I, p. 66. Last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009. Disponível em: < http://dzlp.mk/sites/default/files/Dokumenti/ EU%20zakoni%20zzlp/ GERMANY.pdf>. Acesso em: 21 jan. 2017.

ALEXY, Robert. Direitos fundamentais, ponderação e racionalidade. **Revista de Direito Privado,** vol. 24, out - dez, 2005, p. 334-344.

ANTONIALLI, Dennys et al. **[especial] Fiscalização:** como deve ser o “órgão competente”?, 15 jul. 2016. Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-fiscalizacao-como-deve-ser-o-orgao-competente-2/>. Acesso em: 27 nov. 2016.

ASSEMBLEIA Geral da ONU aprova resolução de Brasil e Alemanha sobre direito à privacidade, 19 dez. 2013. Disponível em: <https://nacoesunidas.org/assembleia-geral-da-onu-aprova-resolucao-de-brasil-e-alemanha-sobre-direito-a-privacidade/>. Acesso em: 27 nov. 2016.

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNLOGIA. **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, 2016. Disponível em: <http://www.internetlab.org.br/wp-content/uploads/ 2016/05/ reporta_apl_dados_pessoais_final.pdf>. Acesso em: 27 nov. 2016.)

ÁVILA, Humberto. **Teoria dos princípios:** da definição à aplicação dos princípios jurídicos. 16. ed. São Paulo: Malheiros Editores, 2015.

BARRIENTOS-PARRA, J. D.; BORGES MELO, E. C. O Direito à intimidade na sociedade técnica: rumo a uma política pública em matéria de tratamento de dados pessoais. **Revista de Informação Legislativa**, ano 45, v. 180, p. 197-214, out./dez. 2008

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. 2. ed. São Paulo: Saraiva, 2010.

BAUMAN, Zygmunt. **Globalização:** as consequências humanas. Rio de Janeiro: Jorge Zahar Ed., 1999.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2014.

BERNERS-LEE, Tim. Tim Berners-Lee: I invented the web. Here are three things we need to change to save it, 12 mar. 2017, **The Guardian**. Disponível em: <https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet?CMP=share_btn_fb>. Acesso em 15 mar. 2017.

BRAGA, S. ; VLACH, V.. Os usos políticos da tecnologia, o biopoder e a sociedade de controle: considerações preliminares. **Scripta Nova. Revista electrónica de geografía y ciencias sociales.** Barcelona: Universidad de Barcelona, 1 de agosto de 2004, vol. VIII, nº 170(42). Disponível em: <http://www.ub.es/geocrit/sn/sn-170-42.htm>. Acesso em: 5 maio 2016.

BRASIL, Agência Brasileira de Inteligência. **1964 – Serviço Nacional de Informações (SNI).** Disponível em: < http://www.abin.gov.br/institucional/historico/1964-servico-nacional-de-informacoes-sni/>. Acesso em 13 jan. 2017.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

BRASIL. **Lei 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < http://www.casadoempresario.org.br/wp-content/uploads/2013/04/CDC.pdf>. Acesso em: 20 jan. 2017.

BRASIL, Supremo Tribunal Federal. ***Habeas Data* 22**. *Habeas Data.* Natureza jurídica. Ministro Relator: Marco Aurélio. Órgão julgador: Tribunal Pleno. Data do Julgamento: 19 de setembro de 1991. Publicação: DJ 01-09-1995 PP-27378 EMENT VOL-01798-01 PP-00001. (1995b). Disponível em: < http://stf.jusbrasil.com.br/ jurisprudencia/14709849/recurso-em-habeas-data-rhd-22-df>. Acesso em: 21 jan. 2017.

BRASIL, Superior Tribunal de Justiça, **Recurso Especial 22.337-RS**. Inserção de dados pessoais do cidadão em bancos de informações. Relator: Ministro Rui Rosado de Aguiar Júnior. Turma Julgadora: Quarta Turma. Data do julgamento: 13 de fevereiro de 1995; publicação: DJ 20/03/1995. Disponível em: < https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=>. Acesso em 15 jan. 2017.

BRASIL. **Lei nº 9.507,** de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: < https://www.planalto.gov.br/ ccivil_03/Leis/L9507.htm>. Acesso em 21 jan. 2017.

BRASIL. **Lei 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 20 jan. 2017.

BRASIL. Superior Tribunal de Justiça. **REsp 1195995/SP**. Danos morais e materiais decorrentes de exame de HIV não solicitado. Relatora: Ministra Nancy Andrighi, Rel. p/ Acórdão: Ministro Massami Uyeda. Órgão Julgador: Terceira Turma. Data do julgamento: 22/03/2011a. Publicação: DJe 06/04/2011. Disponível em: <https://ww2.stj.jus.br/ processo/revista/documento https://ww2.stj.jus.br/processo/revista/documento>. Acesso em: 28 nov. 2016.

BRASIL. **Lei. 12.414** de 09 de junho de 2011b. 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: 21 jan. 2017.

BRASIL. **Decreto nº 7.829** de 17de outubro de 2012. Regulamenta a Lei nº 12.414, de 9 de junho de 2011b, que 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/ 2012/ Decreto/D7829.htm>. Acesso em: 21 jan. 2017.

BRASIL, **Projeto de Lei nº 4060/2012**, p. 2-3. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: <http://www.camara.gov.br/proposicoesWeb/ prop_mostrarintegra; jsessionid=0CFA5ADBBA5E762EB8E42924B7AB7842. proposicoes WebExterno1?codteor=1001750&filename=PL+4060/2012>. Acesso em 5 fev. 2017.

BRASIL. **Lei 12.527**, de 18 de novembro 2011c. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 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: 21 jan. 2017.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.457.199 - RS** (2014/0126130-2). Direito do consumidor. Arquivos de crédito. sistema “credit scoring”. Compatibilidade com o Direito brasileiro. Limites. Dano moral. Relator: Ministro Paulo de Tarso Sanseverino. Órgão julgador: Segunda Seção. Data do julgamento: 12 de dezembro de 2014b. Data da publicação: 17 de dezembro de 2014b. Disponível em: < https://ww2.stj.jus.br/ processo/revista/documento/mediado/? Componente =ITA&sequencial= 1364998&num _registro =201401261302&data=20141217&formato=PDF>. Acesso em: 21 jan. 2017.

BRASIL. **Lei 12.965**, de 23 de abril de 2014a. 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 21 jan. 2017.

BRASIL, Supremo Tribunal Federal. **A Constituição e o Supremo.** 5. ed. Brasília: STF, Secretaria de Documentação, 2016a. Disponível em: <http://www.stf.jus.br/arquivo/ cms/publicacaoLegislacaoAnotada/anexo/a_constituicao_e_o_supremo_5a_edicao.pdf>. Acesso em 5 jan. 2017.

BRASIL. **Decreto nº 8.771,** de 11 de maio de 2016b. Regulamenta a Lei nº 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: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 21 jan. 2017.

BRASIL **Projeto de Lei nº 5.276/2016**c. 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/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em 27 nov. 2016.

CANOTILHO, J.J. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

CANOTILHO, J.J; MOREIRA, V. **Constituição da República Portuguesa anotada**. 4. ed., vol. I. Coimbra: Coimbra Editora, 2007.

CARVALHO, A. P. G. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de direito do consumidor** (RT), ano 12, n. 46, p. 77-119, abril/jun. 2003.

CASTELLS, Manuel. **A sociedade em rede.** 9. ed. São Paulo: Paz e Terra, 2006.

CASTRO, C. S. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro. In: CONGRESO IBEROAMERICANO DE DERECHO CONSTITUCIONAL: DERECHO CONSTITUCIONAL PARA EL SIGILO XXI, 8, 2006, Sevilla (Epaña)/Universidad de Sevilla, **Actas**..., Navarra: Aranzadi, 2006.

CERCA de 48% dos brasileiros usam internet regularmente **Portal Brasil,.** 19 dez. 2014. Disponível em: < http://www.brasil.gov.br/governo/2014/12/cerca-de-48-dos-brasileiros-usam-internet-regularmente>. Acesso em 15 maio 2016.

CHEN, C.L, Philip; ZANG, Chun-Yang. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, **Inform. Sci.**, v. 275, 10 ago. 2014, p. 3, traduzimos. Disponível em: <http://dx.doi.org/10.1016/j.ins.2014.01.015>. Acesso em: 15 jan. 2017.

CHEVITARESE, Leandro; PEDRO, Rosa Maria Leite Ribeiro. Da sociedade disciplinar à sociedade de controle: a questão da liberdade por uma alegoria de Franz Kafka, em O Processo, e de Phillip Dick, em Minority Report. **Estudos de Sociologia. Rev. do Prog de Pós-graduação em Sociologia da UFPE**, v. 8, n. 12. 2002.

COLÔMBIA. **Ley Estatutaria 1266** de 2008 (diciembre 31). por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponível em: <http://www.alcaldiabogota.gov.co/ sisjur/normas/Norma1.jsp?i=34488#0>. Acesso em 22 jan. 2017.

COLÔMBIA. **Ley Estatutaria 1581** de 2012 (Octubre 17). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013**. Por la cual se dictan disposiciones generales para la protección de datos personales.** Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Acesso em: 22 jan. 2017.

COLÔMBIA. **Decreto 1377** de 2013. (Junio 27) Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Disponível em: < http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf>. Acesso em 22 jan. 2017.

COLOMBIA, **Constitución Política de Colombia**. Actualizada con los Actos Legislativos a 2015. Disponível em: <http://www.corteconstitucional.gov.co/inicio/Constitucion% 20politica%20de%20Colombia %20-%202015.pdf>. Acesso em 22 jan. 2017.

CONFERÊNCIA DAS AMÉRICAS. **Declaração de Santa Cruz de La Sierra.** Documento final da XIII Cimeira Ibero-Americana de Chefes de Estado e de Governo, realizada em Santa Cruz de la Sierra em 14 e 15 de novembro de 2003. Disponível em: < http://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>. Acesso em: 21 jan. 2017.

CONVERGÊNCIA DIGITAL. **Brasileiros reagem à espionagem e rejeitam repasse de dados por empresas de tecnologia**, 18 mar. 2015a. Disponível em: <http://convergenciadigital.uol.com.br/ cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39185&sid=18#.VRvP H7kU-9I>. Acesso em 15 maio 2016.

CONVERGÊNCIA DIGITAL. **Pesquisa diz que 31% dos brasileiros aceitam compartilhar dados pessoais**, 28 out. 2015b. Disponível em: < http://convergenciadigital.uol.com.br/cgi/cgilua.exe/ sys/start.htm?UserActiveTemplate=site&infoid=40999#.V0s3-hjgozm>. Acesso em 15 maio 2016.

COSTA, Carlos Celso Orcesi da, **Cadastro positivo** – Lei n. 12.414/2011 comentada artigo por artigo. São Paulo: Saraiva, 2012.

COSTA, Rogério da. Sociedade de controle. **São Paulo Perspec.** São Paulo, v. 18, n. 1, p. 161-167, mar. 2004. Disponível em <http://www.scielo.br/scielo .php?script=sci _arttext& pid=S0102-88392004000100019&lng=pt&nrm=iso>. Acesso em 10 jun. 2016.

CRESWELL, J. W. **Projeto de pesquisa:** método qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010.

CUEVA, R. V. B. Há um direito a autodeterminação informativa no Brasil? In: MUSSI, J.; SALOMÃO, L. F.; MAIA FILHO, N. N. (Org.). **Estudos jurídicos em homenagem ao Ministro Cesar Asfor Rocha.** Ribeirão Preto: Migalhas, 2012, v.3, p. 220-241.

CUNHA E CRUZ, Marco Aurélio Rodrigues da; SOUSA, Jéffson Menezes de; COSTA, C. . Proteção de dados pessoais ou autodeterminação informativa no Brasil?. In: OLIVEIRA, Rafael Santos de; SILVA, Rosane Leal da. (Org.). **Direito e novas mídias**. Curitiba: Ithala, 2015, p. 179-193.

DAVENPORT, Thomas H.. **Big data no trabalho:** derrubando mitos e descobrindo oportunidades. Tradução Cristina Yamagami. Rio de Janeiro: Elsevier, 2014.

DELEUZE, G. *Post-scriptum* sobre as sociedades de controle. In: _____. **Conversações (1972-1990).** São Paulo: Ed. 34, 1992

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

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

ECO, Umberto. **Apocalípticos e integrados**. São Paulo: Perspectiva, 2001.

EFING, Antônio Carlos. **Bancos de dados e cadastro de consumidores**. São Paulo: Editora Revista dos Tribunais, 2002.

ESPANHA. **Constituição Espanhola.** 29 de dezembro de 1978. Madrid, 1978. Disponível em: <http://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Acesso em: 21 jan. 2017.

ESPANHA. Tribunal Constitucional. **Recurso de Amparo núm. 1827/1990**. Sentencia 254/1993, de 20 de julho de 1993. Julgamento em 28 de julho de 1993. Madrid, 1993.

EXTINTO o ‘monstro’ criado por Golbery. Disponível em: <http://memorialdademocracia.com.br/card/extinto-o-monstro-criado-por-golbery>. Acesso em 13 jan. 2017.

FEIJÓ, Bruno Vieira. A revolução dos dados. **Revista Exame PME – Pequenas e Médias Empresas**, São Paulo, p. 30-43, set. 2013.

FOUCAULT, M. **Vigiar e punir:** nascimento da prisão. 38. ed. Petrópolis (RJ): Vozes, 2010.

GEDIEL, J. A. P; CORRÊA, A. E. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. **Revista da Faculdade de Direito** (UFPR), Curitiba, v. 47, p. 141-153, 2008.

GERMAN PARLIAMENT. **Federal Data Protection Act**. **(*Bundesdatenschutzgesetz*** (BDSG)). [s.d.] [on line] Disponível em: <http://www.bfd.bund.de>. Acesso em: 20 jan. 2017.

GOMES, Orlando. **Introdução ao direito civil**. 11. ed. Rio de Janeiro: Forense, 1996.

GOUVEIA, J. B. **Os direitos fundamentais atípicos**. Aequitas Editorial Notícias: Lisboa, 1995.

HENRIQUES, Daniela Aparecida; COSTA, Helder Rodrigues. **Big data** – como utilizar a extraordinária quantidade de informações coletadas por novas tecnologias para obter vantagens competitivas. Disponível em: <http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a72.pdf> Acesso em 25 abr. 2016.

HURWITZ, Judith et al. **Big data for dummies.** Rio de Janeiro, Alta Books, 2015.

INFORME DE OVUN. Leyes de privacidad de los datos: simplificación de los trámites. **Intralinks.** 2017. Disponivel em: <https://www2017..intralinks.com/es/resources/ analyst-reports/ovum-report-data-privacy-laws-cutting-red-tape>. Acesso em 22 jan.

LAUDATI, Laraine. **Summaries of EU Court decisions relating to data protection 2000-2015**. OLAF Data Protection Officer, 28 January, 2016, p. 6. Disponível em: <https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf>. Acesso em 20 jan. 2017.

LEMOS, Ronaldo. Proposta de Doria de vender os dados do Bilhete Único é ilegal, 20 fev. 2017, **Folha de São Paulo**. Disponível em: < http://www1.folha.uol.com.br/colunas/ronaldolemos/2017/02/1860214-proposta-de-doria-de-vender-os-dados-do-bilhete-unico-e-ilegal.shtml>. Acesso em 15 mar. 2017.

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

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

MAYER-SCÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (orgs.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997, pp. 219-242.

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

MARCACINI, Augusto Tavares Rosa **Direito e informática**: uma abordagem jurídica sobre criptografia, São Paulo: Forense, 2002.

MENDES, L. S. F. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. Dissertação (Mestrado em Direito). Brasília, DF: Universidade de Brasília, 2008. Disponível em: <http://www.dominiopublico.gov.br/ download/teste/arqs/cp149028.pdf>. Acesso em: 01 dez. 2016

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 181-182.

MOREY, Timothy; FORBATH, Theodore; SCHOOP, Alisson, Dados dos consumidores: modelos de transparência e confiança. **Harvard Business Review Brasil,** São Paulo, fevereiro 2016.

MURILLO DE LA CUEVA, P. L. **El derecho a la autodeterminación informativa**. Tecnos: Madrid, 1990.

MURILLO DE LA CUEVA, P. L. La construcción del derecho a la autodeterminación informativa. **Revista de estudios políticos**, nº 104, p. 35-60, 1999.

MURILLO DE LA CUEVA, P. L. La primera jurisprudencia sobre el derecho a la autodeterminación informativa.**Datospersonales.org**: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, ISSN-e 1988-1797, Nº. 1, 2003. Disponível em: < https://www.researchgate.net/publication/28060693_La_primera_jurisprudencia_sobre_el_derecho_a_la_autodeterminacion_informativa>. Acesso em: 20 maio 2016.

MURILLO DE LA CUEVA, P. L. Derechos fundamentales y avances tecnológicos: Los riesgos del progreso. **Boletín Mexicano de Derecho Comparado**, nº. 109, p. 72-110, 2004.

MURILLO DE LA CUEVA, P. L. Perspectivas del derecho a la autodeterminación informativa. **IDP**: revista de Internet, derecho y política = revista d'Internet, dret i política, nº. 5, 2007. Disponível em: <http://www.uoc.edu/idp/5/dt/esp/lucas.pdf>. Acesso em: 20 maio 2016.

MURILLO DE LA CUEVA, P. L. La protección de los datos de carácter personal en el horizonte de 2010, **Anuario de la Facultad de Derecho (Universidad de Alcalá)**, nº. 2, p. 131-142, 2009.

NAVARRO, A. M. N. P. O direito fundamental à autodeterminação Informativa. In: NASPOLINI SANCHES, S. H D. F.; DUARTE, F.; ALENCAR, M. L. P. (Coord.). CONPEDI/UFF. (Org.). Direitos fundamentais e democracia II. CONGRESSO NACIONAL DO CONPEDI, XXI. **Anais...** FUNJAB, 2012, p. 429-458.

NEVES, Cláudia E. Abbês Baêta. Sociedade de Controle, o neoliberalismo e os efeitos de subjetivação. In: SILVA, André do et al. (Org.). **Subjetividade:** questões contemporâneas. São Paulo: Hucitec, 1997.

OLIVA, Afonso Carvalho de. **O direito fundamental à proteção de dados pessoais do consumidor brasileiro:** do código de defesa do consumidor ao caso “score”. Dissertação (Mestrado em Direitos Humanos). Aracaju, SE: Universidade Tiradentes, 2016.

OLIVEIRA, Liziane Paixão Silva; FUMAGALI, E.. VALOR JURÍDICO DA DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM: NORMA JUS COGENS OU SOFT LAW?. In: PEDEMONTE, lga Diaz; SANCHES, Samyra Haydêe Dal Farra Naspolini (Org.). **Direito internacional dos direitos humanos III**. 1. ed. FLORIANOPOLIS: CONPEDI, 2016, p.62-78.

Organisation for Economic Co-operation and Development (OECD). **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,** 23 set. 1980, atualização em 2013. Disponível em: < http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. Acesso em: 10 fev. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos.** Adotada e proclamada pela resolução 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://unesdoc.unesco.org/images/ 0013/001394/139423por.pdf>. Acesso em: 21 jan. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Pacto Internacional dos Direitos Civis e Políticos**. Adotado e aberto à assinatura, ratificação e adesão pela resolução 2200-A (XXI) da Assembleia Geral das Nações Unidas, de 16 de Dezembro de 1966. Disponível em: < http://www.cne.pt/ sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf>. Acesso em: 21 jan. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção Americana de Direitos Humanos de 1969 (Pacto San José da Costa Rica)**. Assinada na Conferência Especializada Interamericana sobre Direitos Humanos, San José, Costa Rica, em 22 de novembro de 1969. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm>. Acesso em: 21 jan. 2017.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Diretiva 95/46/CE**, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: < http://www.anacom.pt/render.jsp?categoryId=332397>. Acesso em: 21 jan. 2017.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Directiva 2002/58/CE**, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponível em: < Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF >. Acesso em: 21 jan. 2017.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Regulamento UE 2016/679,** de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <http://www.privacy-regulation.eu/pt/>. Acesso em: 21 jan. 2017.

PATI, Camila. **Conheça o data center do Google em que empregados não entram**, 29 mar. 2016. Disponível em: < http://exame.abril.com.br/tecnologia/noticias/conheca-o-data-center-do-google-que-nem-funcionarios-entram>. Acesso em 15 maio 2016.
PÉREZ LUÑO, A-E. Informática y libertad: Comentario al artículo 18.4 de la Constitución. **Revista de estudios políticos**, nº 24, p. 31-54, 1981.

PÉREZ LUÑO, A-E. **Derechos Humanos, Estado de Derecho y Constitución**. Madrid: Tecnos, 2005.

PÉREZ LUÑO, A-E. **La terceira generación de derechos humanos**. Cizur Menor (Navarra): Thomson-Aranzadi, 2006..

PÉREZ LUÑO, A-E. La protección de los datos personales del menor en internet. **Anuario Facultad de Derecho** (Universidad de Alcalá), n 2, p. 143-175, 2009.

PIOVESAN, Flávia. A constituição brasileira de 1988 e os tratados internacionais de proteção dos direitos humanos. **EOS - Revista Jurídica da Faculdade de Direito**. v. 2, n. 1, jan./jun. 2008. Curitiba: Dom Bosco, 2008.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 12. ed. São Paulo: Saraiva, 2011.

PORTUGAL. **Constituição da República Portuguesa**. Disponível em: < http://www.fd.uc.pt/CI/CEE/OI/Constituicao_Portuguesa.htm> Acesso em 10 maio 2016.

PORTUGAL, Constituição da República Portuguesa, 1976, VII Revisão Constitucional [2005], n.p. Disponível em: <http://www.parlamento.pt/Legislacao/ Paginas/ Constituicao RepublicaPortuguesa.aspx>. Acesso em 04 fev. 2017.

REINALDO FILHO, D. A privacidade na sociedade da informação. In: REINALDO FILHO D. (Coord.). **Direito da Informática, temas polêmicos**. Bauru, SP: Edipro, 2002, p. 25-40.

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

ROVER, Tadeu. **Decreto falhou ao regulamentar sanções do Marco Civil da Internet,** 25 ago. 2016. Disponível em: <http://www.conjur.com.br/2016-ago-25/decreto-falhou-regulamentar-sancoes-marco-civil-internet>. Acesso em 27 nov. 2016.

RUARO, Regina Linden; MOLINARO, Carlos Alberto. Acoplamento entre internet e sociedade. **Revista da AGU**, Brasília-DF, ano XIII, n. 40, abr./jun. 2014.

RUARO, R.; RODRIGUEZ, D.; FINGER, B.. O direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito da UFPR**, n° 53, p. 45-66, 2011. Disponível em: <http://ojs.c3sl.ufpr.br/ojs2/index.php/direito/article/view/30768/19876>. Acesso em: 20 de mar. 2016.

SARLET, Ingo Wolfgang. Direitos fundamentais e direito privado: algumas considerações em torno da vinculação dos particulares aos direitos fundamentais, **Revista de Direito do Consumidor**, vol. 36, out - dez, 2000, p. 54 - 104.

SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 3. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2004.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

SCHIAVI, Pablo. La protección de los datos personales en las redes sociales, **AeC - Revista de Direito Administrativo e Constitucional**, Belo Horizonte, ano 13, n. 52, abr. / jun. 2013, p. 12. Disponível em: < http://www.revistaaec.com/index.php/revistaaec/article/view/137>. Acesso em 11 fev. 2017.

SIBILIA, Paula. **O homem pós-orgânico:** o corpo, subjetividade e tecnologias digitais. Rio de Janeiro: Relume Dumará, 2002.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 29. ed. São Paulo: Malheiros, 2008.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 35. ed. São Paulo: Malheiros, 2012.

SOUZA, V. R. C. O acesso à informação na legislação brasileira. **Revista da Seção Judiciária do Rio de Janeiro**, v. 19, p. 161-181, 2011.

STÜRMER, Bertram Antônio. Banco de dados e “habeas data” no código do consumidor. **Revista de Direito do Consumidor,** vol. 1, p. 55-94, Jan – Mar/1992.

SUNDFELD, Carlos Ari. “Habeas data” e mandado de segurança coletivo. **Doutrinas Essenciais de Direitos Humanos,** vol. 5, p. 169-186, Ago - 2011.

SYMANTEC. **Glossário.** Disponível em: <www.symantec.compt/br/security_response/glossary/define.jsp?letter=p&word=petabyte>.Acesso em 20 fev. 2017.

TALAMINI, Eduardo. O processo do *habeas data*: breve exame. **Revista de Processo,** vol. 101, p. 88-99, Jan – Mar 2001

TÓTORA, Silvana. Democracia e sociedade de controle. **Verve**, 10: 237-261, 2006, p. 239. Disponível em: < http://revistas.pucsp.br/index.php/verve/article/viewFile/5441/3888>. Acesso em 15 maio 2016.

TREACY, Bridget. Preparing for Change: Europe’s Data Protection Reforms Now a Reality. In: HUNTON & WILLIAMS. **The International Comparative Legal Guide to: Data Protection 2016.** London, 2016, p. 92. Disponível em: <https://www.hunton.com/files/upload/ICLG_Data_Protection_2016.pdf>. Acesso em 19 jan. 2017.

TRINDADE, Rafael. **Foucault** – panóptico [ou, “a visibilidade é uma armadilha”], 2014. Disponível em: < https://goo.gl/images/baOdKf>. Acesso em: 18 jan. 2017.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679**, 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. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em 17 dez. 2016).

URUGUAI. **Lei nº 18.331** - protección de datos personales y acción de "habeas data", 6 ago. 2008. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp6739900.htm>. Acesso em 15 nov. 2016.

USA, President’s Council of Advisors on Science and Technology (PDCAST). **Big data and privacy:** a technological perspective, maio 2014. Disponível em: <https://www.whitehouse.gov / ites/ default/files/ microsites/ostp/PCAST/pcast_big _data_and_privacy_-_may_2014.pdf>. Acesso em 29 dez. 2016.

VERZELLO, Robert J.; REUTTER III, John. **Processamento de dados**. Tradução Regina Szwarcfiter, Heraldo Luiz Marin. São Paulo: McGraw-Hill do Brasil, 1984.

ZIKOPOULOS, P; DE ROOS, D; PARASURAMAN, K; DEUTSCH, T; GILES, J; CORRIGAN, D. **Harness the power of Big Data-** The IBM Big Data Platform. Emeryville: McGraw-Hill Osborne Media, 2012.