

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

A ERA DA VIGILÂNCIA NO CIBERESPAÇO E OS IMPACTOS DA NOVA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL:
Reflexos no direito à privacidade

MARIANA MONTEIRO DA COSTA

Rio de Janeiro
2018/2º SEMESTRE

MARIANA MONTEIRO DA COSTA

A ERA DA VIGILÂNCIA NO CIBERESPAÇO E OS IMPACTOS DA NOVA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL:

Reflexos no direito à privacidade

Monografia apresentada à Faculdade de
Direito da Universidade Federal do Rio de
Janeiro, como requisito parcial para obtenção
do título de Bacharel em Direito, sob a
orientação da **Professora Dra. Juliana Gomes
Lage**.

Rio de Janeiro
2018/2º SEMESTRE

CIP - Catalogação na Publicação

C837e Costa, Mariana Monteiro da
A ERA DA VIGILÂNCIA NO CIBERESPAÇO E OS IMPACTOS
DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO
BRASIL: Reflexos no direito à privacidade / Mariana
Monteiro da Costa. -- Rio de Janeiro, 2018.
93 f.

Orientadora: Juliana Gomes Lage.
Trabalho de conclusão de curso (graduação) -
Universidade Federal do Rio de Janeiro, Faculdade
de Direito, Bacharel em Direito, 2018.

1. Dados Pessoais. 2. Controle. 3. Privacidade.
4. Internet. I. Lage, Juliana Gomes, orient. II.
Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

MARIANA MONTEIRO DA COSTA

A ERA DA VIGILÂNCIA NO CIBERESPAÇO E OS IMPACTOS DA NOVA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL:

Reflexos no direito à privacidade

Monografia apresentada à Faculdade de
Direito da Universidade Federal do Rio de
Janeiro, como requisito parcial para obtenção
do título de Bacharel em Direito, sob a
orientação da **Professora Dra. Juliana Gomes
Lage**.

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

Juliana Gomes Lage - Orientadora

XXX - Membro da Banca

XXX - Membro da Banca

XXX - Membro da Banca

Rio de Janeiro
2018/2º SEMESTRE

AGRADECIMENTOS

Agradeço em primeiro lugar à minha família de sangue, aqueles que me acompanharam e me apoiaram em toda a jornada até aqui. Sem todo o carinho e estímulo não teria conseguido completar mais esse sonho. Graças à força e determinação da minha querida mãe, Paula, ao carinho e ombro amigo do meu pai, Evandro, à amizade dos meus irmãos, Eduardo e Amanda, bem como ao amor de meus queridos avós e demais parentes, mesmo os que já se foram, pude chegar até esse momento de forma atenta e forte.

O fechamento deste ciclo representa uma jornada de grande enriquecimento moral, afetivo, cultural e intelectual que travei dentro da gloriosa FND, principalmente, graças aos grandes amigos que encontrei e aos projetos e sonhos que concretizamos no decorrer desses cinco anos. Desde a primeira semana de aula sabia que meu lugar era com os companheiros do Coletivo Direito de Resistência, esses que me mostraram que um novo modelo de universidade e de sociedade era possível. Sempre acreditei que o Direito pode ser utilizado como um importante instrumento de transformação social e é nesse sentido que pretendo levar minha vida profissional de agora em diante.

Por fim, agradeço ao Direito de Resistência, aos Desviados da Nacional, às Empenadas e às amigas da eterna Turma C, em especial Gabriel, Guilherme, Jordana, Carolina, Robson, Humberto, Ilana, Nathália, Mariana, Romulo, Tainá, Raissa, Camila, Jean, Julia, Luís, Raiza, Isabela, Bruna, Jamila, Luísa, Alice e Thizá, amigos que levo da Nacional para o restante de minha vida.

*“O medo mimético provocado por uma fantasia literária revela a natureza
de medos sociais reais.”*

- Norbert Elias

RESUMO

O presente trabalho tem como objetivo analisar as questões relativas à privacidade e ao tratamento de dados pessoais na internet. Para tanto, nesta pesquisa, busca-se, no primeiro capítulo, abordar de forma ampla as implicações sociais, econômicas e políticas da manipulação das informações com a disrupção de novas tecnologias, bem como no tocante às formas de controle propiciadas pelas mesmas. No segundo capítulo, são abordadas as questões relativas aos direitos de personalidade na era da informação, com especial enfoque para o direito à privacidade, direito à autodeterminação informativa e para o princípio de proteção da dignidade da pessoa humana. Traça-se também um panorama sobre a consideração dos dados pessoais como novo direito de personalidade, com vistas à proteção destes em face de abusos por partes de plataformas e provedores. Por fim, no último capítulo, são abordados mais especificamente os dispositivos constitucionais e infraconstitucionais brasileiros, bem como a atual legislação europeia e brasileira sobre a matéria.

Palavras-chave: Dados pessoais; *Internet*; Controle; Privacidade; RGPD; LGPD.

ABSTRACT

The present work aims at analyzing issues related to privacy and the processing of personal data on the Internet. For this purpose, in this research, we seek, in the first chapter, to broadly address the social, economic and political implications of the manipulation of information with the disruption of new technologies, as well as the forms of control provided by them. In the second chapter, issues of personality rights in the information age are addressed, with a special focus on the right to privacy, the right to self-determination and the principle of protection of the dignity of the human person. It also provides an overview of the consideration of personal data as a new personality right, with a view to protecting them in the face of abuse by platforms and providers. Lastly, in the last chapter, the Brazilian constitutional and common provisions, as well as the current European and Brazilian legislation on the subject, are more specifically addressed.

Keywords: Personal Data; Internet; Control; Privacy; GDPR; LGPD.

SUMÁRIO

INTRODUÇÃO.....	7
1. VIGILÂNCIA E INTELIGÊNCIA ARTIFICIAL NO CIBERESPAÇO.....	9
1.1. Sociedade em rede e economia da informação	10
1.2. A vigilância líquida como pós-pan-óptico	12
1.3. Espetacularização da vida e o papel das redes sociais	14
1.4. A distopia na arte: Da ficção para a realidade	17
1.5. Tecnologia como meio de controle da população: " <i>A Smart Machine</i> "	22
1.5.1. Big Data e o imperativo da vigilância	24
1.5.2. Social Big Data e a delegação da escolha às máquinas	27
1.6. Internet das Coisas (IoF): O advento da Web 4.0	32
2. DIREITO À PRIVACIDADE E OS DADOS PESSOAIS COMO NOVO DIREITO DE PERSONALIDADE.....	35
2.1. Privacidade, Intimidade e Vida Privada	36
2.2. Proteção da dignidade da pessoa humana e a autodeterminação informativa	41
2.3. Dados pessoais como direito de personalidade	43
2.3.1. Princípios norteadores	45
2.4. Abuso por parte das plataformas	50
2.4.1. Consentimento como ficção jurídica	51
2.4.2. Comercialização de dados	54
2.4.3. Uso de dados para reprodução de padrões discriminatórios	55
3. MODELO BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS E O CONTEXTO DA LEI 13.709/18.....	59
3.1. O Marco Civil da Internet: Lei 12.965/14	60
3.1.1. Dados pessoais no Marco Civil	62
3.2. A inspiração da Lei 13.709/18 na Regulação Europeia (RGPD)	65
3.3 Principais pontos da Lei 13.709/18 no tocante à privacidade.....	72
CONCLUSÃO.....	82
REFERÊNCIAS BIBLIOGRÁFICAS.....	84

INTRODUÇÃO

Com o advento da Era da Vigilância no ciberespaço e fora dele, principalmente por conta do advento da *internet* e do aumento exponencial do valor de mercado das informações dos indivíduos, começou a surgir, na atualidade, um novo patamar de desafios jurídicos. Com o aprimoramento da tecnologia são produzidas problemáticas antes inexistente, pois com a técnica surge também algo que foge ao controle do homem.

Muito próximo de um futuro distópico apresentado na literatura, em filmes e séries de televisão, em que a tecnologia, através da manipulação de informações, é capaz de promover decisões automatizadas e criar perfis de usuários e consumidores; a realidade é cada vez mais parecida com a ficção. Mesmo que se tenha em consideração os inúmeros aspectos positivos do tratamento de dados pessoais, importante se faz atentar para as possibilidades de discriminações de grupos e indivíduos propiciadas pela tecnologia.

Cumprе ressaltar que o aumento do controle sobre os usuários por meio da tecnologia representa um dos mais intensos debates da atualidade, tendo em vista as grandes propensões de mau uso das informações por conta de interesses escusos daqueles que os manipulam. A partir de superprocessadores de Big Data, ou seja, de um massivo conjunto de dados pessoais correlacionados, podem ser sentidas influências de ordem social, econômica, política e, inclusive, no tocante às escolhas íntimas dos usuários.

Nesse sentido, para a devida proteção de direitos fundamentais, como o direito à privacidade e os demais direitos da personalidade, faz-se necessária verdadeira releitura do momento presente. Aprimoram-se, dessa forma, as técnicas e métodos de controle do tratamento de dados pessoais no mundo, bem como a edição de legislações voltadas exclusivamente para a proteção de informações. Nesse contexto, em 2018, é implementado o

Regulamento Geral de Proteção de Dados 2016/679¹ europeu e publicada a Lei Geral de Proteção de Dados Pessoais brasileira, Lei 13.709/2018².

Por fim, diante da impossibilidade de se negar a realidade que está posta, cabe a reflexão acerca da real utilidade das tecnologias emergentes e sobre que ética desejamos inserir nas coisas inteligentes. Também se faz necessário debate acerca do empoderamento do titular de dados e de sua participação individual e coletiva no ambiente da *internet*, tendo em vista que este espaço representa hoje parte estrutural de uma série de espécies de interações, construindo-as e moldando-as.

Nesse sentido, para que se possibilite a formação de verdadeiras cidadanias eletrônicas, exige-se uma construção social da noção de privacidade. De acordo com Rodotà, “da amplitude e da efetividade das garantias asseguradas à privacidade, como momento constitutivo da esfera pública e da esfera privada, depende, em grande parte, a possibilidade de que a sociedade da informação evolua para uma sociedade ‘do conhecimento e do saber’, e não para uma sociedade da vigilância, da classificação e do controle”.³

¹ EUROPA. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L119, 59º ano, de 4 de maio de 2016. Disponível em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>. Acesso em: 29 nov. 2018.

² BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

³ RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 137.

1. VIGILÂNCIA E INTELIGÊNCIA ARTIFICIAL NO CIBERESPAÇO

O preço a pagar para que se possa fruir da Sociedade da Informação, ou da Vigilância, pode ser descrito como a disponibilização de nossos dados pessoais. Dessa forma, em troca de se obter um serviço ou um bem, são cedidas informações pessoais. O ponto chave é a informação e seu valor crescente de aspecto central nesse novo sistema.

Mesmo que não queiramos, ao fazer uso das plataformas e aplicativos, involuntariamente deixamos uma série de rastros eletrônicos que combinam nossas ações passadas de forma a prever nossos passos futuros. Dessa forma, a vigilância é líquida, está presente em todos os lugares, tende a dominar todo o sistema e a ele impor suas características.

Os riscos que daí se podem afluír se conectam ao uso político, econômico e social que pode ser feito de tais dados, estes que, quando usados para o controle de determinados cidadãos, revelam seu caráter autoritário e ditatorial. Stefano Rodotà cita a imagem do “homem de vidro”, proveniente do período de ascensão do nazismo, que seria o verdadeiro cidadão deste novo mundo calcado pela tecnologia, tendo em vista a pretensão do Estado de tudo saber, mesmo os aspectos mais íntimos do cidadão.⁴

Nesse sentido, passaria de Sociedade da Informação para Sociedade da Vigilância, que tudo e a todos controla através da manipulação das informações. Todavia, essa nova forma de controle diverge dos regimes totalitários do século XX, característicos de uma modernidade sólida. No mundo atual, a vigilância não mais se limita a impedir ou desencorajar determinados comportamentos.⁵

Pelo contrário, a vigilância, em sua forma líquida, incentiva que determinados comportamentos, como os de consumo, sejam repetidos tanto quanto possível, classificando e

4 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 147-148.

5 Ibidem, p. 112-113.

criando perfis daqueles que fazem uso dos dispositivos, através de cruzamento de dados. A passagem abaixo do romance *O Círculo* pode ilustrar esse contexto:

“Você acha isso certo?”, perguntou Mercer. “Sabe como foi que me abordaram? Com a visão utópica de sempre. Dessa vez disseram que assim eu ia reduzir o desperdício. Se as lojas sabem o que os clientes querem, não precisam produzir demais, não transportam produtos demais, não precisam jogar coisas fora quando não são compradas. Veja, como tudo o mais que vocês ficam empurrando para a gente, dito assim parece perfeito, progressista, mas acarreta mais controle, mais rastreamento de tudo o que fazemos”.⁶

Como consequência disso, existem inúmeras possibilidades de exclusão de determinados indivíduos e de práticas discriminatórias contra grupos marginalizados nesta embrionária “Sociedade da Classificação”⁷, dessa forma, faz-se mister verdadeira tutela com intuito de se permitir um movimento de resistência e de empoderamento dos usuários, bem como sejam estruturadas as bases de uma real cidadania eletrônica.

1.1. Sociedade em rede e economia da informação

Existe uma série de nomenclaturas passíveis de serem utilizadas para definir a forma social que estamos vivenciando, dentre elas, sociedade pós-industrial, sociedade informática, sociedade do conhecimento, sociedade tecnizada ou sociedade em rede.

Podemos caracterizar a passagem do século vinte para o século vinte e um como um importante marco de alteração nas estruturais sociais vigentes até então, estando, neste novo século, as sociedades contemporâneas sujeitas a transformações constantes tanto em seu sentido tecnológico quanto em seu sentido econômico, social e cultural.

O conhecimento e a informação passaram a representar um aspecto de extrema relevância nas sociedades modernas, apresentando cada vez mais alto valor econômico e relevância social. Em uma economia pautada na informação, sedimentada nos pilares da tecnização, informatização e globalização, é de suma importância que possamos compreender

6 EGGERS, Dave. *O Círculo*. São Paulo. Companhia das Letras, 2014. p. 277.

7 RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 114.

seus aspectos de funcionamento para que saibamos nos salvaguardar de suas novas ameaças, principalmente no que tange à violação da privacidade e à proteção de dados pessoais.

Nesse sentido, é importante frisar a contribuição do sociólogo Castells para que possamos compreender esses marcos históricos e sua relação com as estruturas de poder na sociedade contemporânea. Segundo o autor, “as sociedades são organizadas em processos estruturados por relações historicamente determinadas de produção, experiência e poder”.⁸ Por esse ângulo, Castells observa que a tecnologia da informação guarda estreito vínculo com o processo de reestruturação do sistema capitalista, que pôde se adaptar aos novos moldes econômicos e sociais.

Assim, a nova estrutura social estaria vinculada ao surgimento de um novo modelo de desenvolvimento, o *informacionalismo*. Esta sociedade moderna pautada na informação é disposta pela lógica da organização em redes, ou seja, da *sociedade em rede*, estando a economia estruturada ao redor destas redes globais de capital, gerenciamento e informação. De acordo com o sociólogo:

“(...) redes são estruturas abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação (por exemplo, valores ou objetivos de desempenho). Uma estrutura social com base em redes é um sistema aberto altamente dinâmico suscetível de inovação sem ameaças ao seu equilíbrio.”⁹

Por fim, Castells nos apresenta cinco quesitos centrais do atual sistema de meios de comunicação e, conseqüentemente, de produção: a informação vista como matéria-prima; as novas tecnologias trespassando por praticamente todas as atividades humanas; a dinâmica de redes presente nos sistemas e relações em que consta a nova tecnologia; a maleabilidade de organização e reorganização de processos, organizações e instituições; e, por fim, haveria uma tendência para a convergência e integração do sistema como um todo, acarretando em uma interdependência entre biologia e microeletrônica.¹⁰

8 CASTELLS, M. A sociedade em rede: Vol.1. A era da informação: Economia, sociedade e cultura (2 ed.). São Paulo: Paz e Terra, 1999. p. 33.

9 Ibidem, p. 499.

10 Ibidem, p. 78-79.

Destarte, necessário se faz analisar a sociedade em rede, que hoje domina as formas de comunicação social, econômica e política; em consonância com a possibilidade de controle dos indivíduos gerada por esses meios tecnológicos. É certo que, atualmente, para que seja possível compreender as novas relações propiciadas pela tecnologia, faz-se ímpar compreender as novas dinâmicas em que a sociedade global se encontra inserida.¹¹

1.2. A vigilância líquida como pós-pan-óptico

O diálogo através de mensagens de e-mail entre os sociólogos Zygmunt Bauman e David Lyon deu origem ao livro *Vigilância Líquida*¹², este que aborda como tema central a vigilância na sociedade pós-moderna e suas diversificadas formas. Categorias consagradas no pensamento de Bauman, a liquidez e a fluidez não deixam de perpassar a obra em questão, representando característica marcante da sociedade pós-moderna em que vivemos.

Inicialmente, cumpre conceituar o termo pan-óptico (“o olho que tudo vê”) utilizado por Michel Foucault em *Vigiar e Punir*¹³ e por Gilles Deleuze em *Post-Scriptum sobre a sociedade de controle*¹⁴. Esse conceito faz referência a um projeto arquitetônico de prisão criado pelo filósofo e jurista Jeremy Bentham¹⁵. Nesta prisão haveria uma torre central que permitiria aos vigilantes observar todos os presos em cada uma de suas celas, porém estes não saberiam se estariam ou não sendo observados.

Este modelo designaria uma penitenciária ideal, visto que ocasionaria um sentimento de constante vigilância, de vigilância ininterrupta. Cumpre ressaltar, todavia, que “a visibilidade é uma armadilha” (FOUCAULT, 2009, p. 190), culminando em um exponencialmente crescente controle sobre os corpos em questão. O pan-óptico, portanto, não é simplesmente uma estrutura física, mas sim uma *tecnologia de poder*, com o intuito de produzir um estado

¹¹ DOS SANTOS, Marcos Moura Baptista. Sociedade em rede e modo de desenvolvimento informacional: descrições sociológicas da sociedade contemporânea. Disponível em: <http://www.unisc.br/cursos/enade/docs/curso_enade/Sociedade_Rede_paradigma_informacional.doc>. Acesso em: 23 nov. 2018.

¹² BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014.

¹³ FOUCAULT, M. *Vigiar e punir*. Petrópolis: Vozes, 2000.

¹⁴ DELEUZE, Gilles. *Postscript on the societies of control*. October, n. 59, 1992.

¹⁵ BENTHAM, J. *O panóptico*. Belo Horizonte: Autêntica Editora, 2008.

consciente de alerta em razão de inabalável visibilidade. Desta feita, por ser também flexível e maleável, poderia perfeitamente se adequar a outros ambientes que não a prisão.

Todavia, apesar de serem obras basilares e de relevância histórica singular, segundo Bauman, não são suficientes para pensarmos a vigilância hoje, visto que esta assumiu diversas formas que não mais se explicam pelos conceitos de sociedades disciplinares formulados no século passado.¹⁶ Não se trata mais somente da questão da disciplina, mas também do controle, este que representa a vigilância também a céu aberto. Deleuze faz uso de uma metáfora para se referir a estes dois ambientes, ao formular que “os anéis de uma serpente [sociedade de controle] são ainda mais complicados que os buracos de uma toupeira [sociedade disciplinar]” (DELEUZE, 2013, p. 230).

Nesse sentido, a fase atual pode ser descrita como a modernidade “tardia”, “pós-modernidade” ou modernidade “líquida”. Segundo o autor, Marx e Engels, em 1848, já haviam premeditado tal momento no momento de transição para o século XX, em seu *Manifesto Comunista*¹⁷:

“Tudo o que era sólido se desmancha no ar, tudo o que era sagrado é profanado, e as pessoas são finalmente forçadas a encarar com serenidade sua posição social e suas relações recíprocas”.

Nesse contexto, a vigilância, inicialmente sólida e estável, acaba por adentrar e se infiltrar em praticamente todas as áreas da vida, onde antes sua influência era sutil, crescendo, dessa forma, como ervas daninhas, e não mais como árvores.¹⁸

Há de se ressaltar, contudo, que o panoptismo, este aparato físico de vigilância, não resta inteiramente superado. Para Bauman, muito pelo contrário, está “armado de músculos eletronicamente reforçados, “*ciborguizados*””.¹⁹ Todavia, deixou de ser o padrão de controle,

16 LEOPOLDO, Rafael. Vigilância Líquida: Variações sobre o Panoptismo. Sapere Aude – Revista de Filosofia, Belo Horizonte, v. 6, n. 12, jan. 2016. p. 894-902. Disponível em: <<http://periodicos.pucminas.br/index.php/SapereAude/article/view/11261/9115>>. Acesso em: 23 nov. 2018.

¹⁷ MARX, Karl; ENGELS, Friedrich. O Manifesto comunista. 14 ed. São Paulo: Paz e Terra, 2004.

¹⁸ DELEUZE, Gilles. Postscript on the societies of control. October, n. 59, 1992. p. 3-7.

¹⁹ BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. p. 58.

limitando-se às instituições totais, como os presídios e clínicas psiquiátricas, em que se encontrem aqueles “excluídos” em débito com a sociedade.

No mundo pós-pan-óptico, em uma sociedade pós-disciplinar, o indivíduo introjetaria esta sociedade de controle, a lógica da vigilância. Dessa forma, o indivíduo não precisaria do antigo pan-óptico, pois já teria em si mesmo sua autovigilância e a vigilância do outro, em uma tarefa do tipo “faça você mesmo”:

“Em suma, tal como os caramujos transportam suas casas, os empregados do admirável novo mundo líquido moderno precisam crescer e transportar sobre os próprios corpos seus pan-ópticos pessoais”.²⁰

Com a proliferação de dispositivos móveis pessoais, portanto, acaba-se por criar uma série de pequenos pan-ópticos, nos quais é voluntária a produção da base de dados pessoais, matéria-prima deste novo mercado. Por conseguinte, “podem ser tudo menos os vigilantes de estilo antigo, zelando pela monotonia da rotina obrigatória; são antes rastreadores ou perseguidores obsessivos dos padrões intensamente mutáveis dos desejos e da conduta inspirada por esses desejos voláteis”.²¹

1.3. Espetacularização da vida e o papel das redes sociais

Segundo David Lyon, “o anonimato já está em processo de autoerosão no *Facebook* e em outras mídias sociais. O privado é público, é algo a ser celebrado e consumido tanto por incontáveis “amigos” quanto por “usuários” casuais”.²²

Seguindo no contexto da sociedade contemporânea, podemos constatar que a informação exerce importante poder de organização e mediação social, promovendo *trocas simbólicas* entre os usuários. Dessa forma, no ambiente do ciberespaço é que se estabelecem grande parte das interações comunicativas atualmente.

Todavia, essas trocas que compõem a comunicação estão se tornando cada vez mais imediatistas e efêmeras. Com o advento da *cibercultura*, nova cultura gerada pela

20 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 61.

21 *Ibidem*, p. 74.

22 *Ibidem*, p. 21.

interconexão de vários grupos por meio da tecnologia, é possível compreender a dimensão do avanço da presença da *Internet* no cotidiano social. Dessa forma, a *Internet* surge como espaço de criação e expressão de particularidades, na qual as redes sociais apresentam papel estruturante.

Atualmente, as mídias sociais são capazes de esculpir opiniões, incitar comportamentos, bem como influenciar na personalidade e constituição dos sujeitos, transfigurando-se, dessa forma, em palco da *espetacularização* da vida cotidiana, através de uma abundância de imagens compartilhadas instantaneamente via computadores e dispositivos móveis.

Nesse sentido, ao passo em que a *Internet* facilita a comunicação entre os usuários, através do acesso e compartilhamento de dados e informações, traz consigo uma série de ameaças à segurança do sujeito. Por conseguinte, podemos observar reflexos diretos em sua esfera de privacidade.²³ Dessa forma, há genuína inversão da vida privada, em prol da exposição, tendo como palco as redes sociais. Segundo Bauman:

“A condição de ser observado e visto, portanto, foi reclassificada de ameaça para tentação. A promessa de maior visibilidade, a perspectiva de “estar exposto” para que todo mundo veja e observe, combina bem com a prova de reconhecimento social mais avidamente desejada, e, portanto, de uma existência valorizada – “significativa”.”²⁴

Entende Bauman que “o aspecto mais notável da edição contemporânea da vigilância é que ela conseguiu, de alguma maneira, forçar e persuadir opositores a trabalhar em uníssono e fazê-los funcionar de comum acordo, a serviço de uma mesma realidade. Por um lado, o velho estrategema pan-óptico (“Você nunca vai saber quando é observado em carne e osso, portanto, nunca imagine que não está sendo espionado”) é implementado aos poucos, mas de modo consistente e aparentemente inevitável, em escala quase universal. Por outro, com o velho pesadelo pan-óptico (“Nunca estou sozinho”) agora transformado na esperança de “Nunca mais vou ficar sozinho” (abandonado, ignorado e desprezado, banido e excluído), o medo da exposição foi abafado pela alegria de ser notado.”²⁵

²³ DOS SANTOS, Sara Gomes. Era do espelho: A captura do olhar nas redes sociais. Campina Grande: 2016. Disponível em:< <http://dSPACE.bc.uepb.edu.br/jspui/bitstream/123456789/11696/1/PDF%20-%20Sara%20Gomes%20dos%20Santos.pdf>>. Acesso em: 25 nov. 2018.

²⁴ BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. p. 30.
²⁵ Ibidem, p. 29-30.

A vida real, fruto de relações externas, foi substituída em parte pela vida virtual, ou *virtual life*, esta que coloca o sujeito como protagonista na construção de seu próprio eu. Nossa identidade, portanto, é criada através de interação contínua com as máquinas, que se conectam por meio de emaranhados de redes. O homem, neste contexto, é ser interativo, recebendo e fornecendo grande quantidade de conteúdo rotineiramente. Nesse mundo, pois, a perda de *status* na internet pode ocasionar sérias privações na vida real.²⁶

Ganhamos, portanto, um corpo eletrônico, este que adquire forma nas redes e que, ao mesmo tempo, pode se dividir entre identidades variáveis construídas na internet. Segundo Rodotà, “o computador e a internet levam a crise de identidade que a psicologia já havia feito emergir a uma consequência extrema.”²⁷

Todavia, as dinâmicas próprias da “vida na tela”, o *black mirror*, ao mesmo tempo em que geram um sério risco de isolamento do indivíduo que deixa de se relacionar de outras formas, limitando-se única e exclusivamente às trocas com o computador; também proporcionam a formação de comunidades ou vínculos sociais que seriam antes impossíveis sem o auxílio da tecnologia.

Apesar disso, ressalta Rodotà que “a crescente possibilidade de o indivíduo fechar-se na fortaleza eletrônica parece oferecer apenas a ilusão de um fortalecimento e enriquecimento da esfera privada. Mais do que se subtrair ao controle social, o indivíduo se encontra na situação de ver rompido o liame social com os seus semelhantes, que se tenta reconstruir com base somente na comunicação eletrônica. Na aldeia global aumenta a sensação de autossuficiência, mas também a separação em relação aos demais. Deterioram-se as tradicionais formas de controle social, cujo lugar é assumido, no entanto, por controles mais penetrantes e globais, tornados possíveis pelo tratamento eletrônico das informações.”²⁸

26 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 119.

27 Ibidem, p. 120.

28 Ibidem, p. 94-95.

Um reflexo das consequências que nos aguardam, principalmente por conta da Inteligência Artificial, é ilustrada de uma maneira extremamente sensível no filme *Her*²⁹, dirigido por Spike Jonze. No filme, o escritor solitário Theodore desenvolve uma relação de amor com o novo sistema operacional de seu computador, chamada Samantha, criando laços com a máquina que não é capaz de estabelecer com outras pessoas. Por conta dos avanços da IA, a própria máquina também adquire seus próprios *sentimentos* em relação a Theodore.

Esta é a realidade que nos é posta no momento, distanciando-se cada vez mais da ficção e aproximando-se com maior afinco de um futuro tangível, acometendo toda a organização social. Devemos, diante disso, buscar formas de permear essa dimensão com uma lógica de liberdade, e não de controle, visto que não é mais possível ignorar sua existência no mundo moderno.

1.4. A distopia na arte: Da ficção para a realidade

No momento presente, as séries de televisão, romances e filmes parecem confirmar que estamos em uma era de ouro das distopias. O termo distopia é costumeiramente utilizado na literatura de ficção científica e, como o nome sugere, é o pensamento, filosofia ou processo contrário à utopia.

Em um futuro distópico, o lugar ou estado imaginário é vivenciado em condições de extrema opressão ou privação, onde habitualmente é caracterizado pelo totalitarismo, autoritarismo e por um opressivo controle da sociedade.³⁰

De maneira oposta à literatura utópica, como, por exemplo, *Utopia*³¹ de Thomas More, a literatura distópica começou a se difundir no século XX, entre outras causas, pela eclosão de diversos conflitos bélicos, ao mesmo tempo em que se afirmavam sistemas de governo totalitários e crises econômicas agudas ao redor do globo. Esse sentimento de profundo

²⁹ HER. Direção: Spike Jonze. Estados Unidos da América: Warner Bros. Pictures, 2013. 1 DVD (125 minutos).

³⁰ ROCHA, Camila. Por que é fácil confundir realidade e distopia nos dias atuais. Nexo Jornal, 03.08.2017. Disponível em: < <https://www.nexojornal.com.br/expresso/2017/08/03/Por-que-%C3%A9-f%C3%A1cil-confundir-realidade-e-distopia-nos-dias-atuais> >. Acesso em: 23 nov. 2018.

³¹ MORE, Sir. Thomas. Utopia. Tradução (da versão em inglês) de Jefferson Luiz Camargo e Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 1999.

desespero e de preocupação com o futuro que se instalou no período foi a base de obras canônicas para a literatura mundial como *1984*³² de George Orwell e *Admirável Mundo Novo*³³ de Aldous Huxley.

Todavia, suas narrativas são distintas, em *Admirável Mundo Novo*, vive-se numa Londres futura no ano de 2540, segregada em estratos hierárquicos e composta de uma série de regras e condicionamentos de comportamentos, onde tudo foi padronizado e “fordizado”³⁴. O romance pessimista é capaz de antecipar desenvolvimentos em tecnologia em nome da modernidade, que acabam por gerar mudanças catastróficas na forma de organização da sociedade.³⁵

Já em *1984*, é descrita uma sociedade totalitária completamente vigiada por um aparato estatal (*Big Brother* ou o Grande Irmão) que a todos vigia e controla, visando coibir qualquer forma de livre pensamento e dissidência. O regime chega até a recriar a própria história, que é contada de acordo com os interesses estatais momentâneos, e a criar uma nova língua e teoria moral que a cada vez exijam menor intelectualidade por partes dos cidadãos para sua compreensão.

O controle é tão grande que se vive com medo de se estar infringindo alguma regra, mesmo que durante o sono. Esta compulsoriedade se dá por meio dos mais diversos mecanismos, desde o controle da imprensa até a prisão, tortura e assassinato. Segundo passagem do livro:

“A ordem dos antigos despotismos era: ‘Não farás’. A ordem dos totalitários era: ‘Farás’. Nossa ordem é: ‘Es’. Ninguém que seja trazido para este lugar se rebela contra nós. Todos passam por uma lavagem completa. (...) Quando acabamos com eles, estavam reduzidos a uma casca. Não havia mais nada dentro deles, exceto o arrependimento pelo que tinham feito e o amor pelo Grande Irmão”.³⁶

³² ORWELL, George. 1984. São Paulo: Companhia das Letras, 2009.

³³ HUXLEY, A. Admirável mundo Novo. Rio de Janeiro: Editora Globo, 1932.

³⁴ Fordismo: Sistema de produção e gestão em massa idealizado, em 1913, pelo empresário estadunidense Henry Ford.

³⁵ RAMONET, Ignacio. A atualidade chocante de ‘Admirável Mundo Novo’. Revista Fórum, 26.07.2015. Disponível em:< <https://www.revistaforum.com.br/a-atualidade-chocante-de-admiravel-mundo-novo/>>. Acesso em: 23 nov. 2018.

³⁶ ORWELL, George. 1984. São Paulo: Companhia das Letras, 2009. p. 299.

Portanto, no início do século XX, a partir do fim da fé cega no progresso, pudemos assistir a migração das literaturas utópicas para as pessimistas distopias. Nesse sentido, diante da impossibilidade de deter o progresso técnico, vimos surgir temores difusos. Conforme expõe Rodotà, o surgimento dessa angústia se dá justamente por conta da velocidade do progresso técnico-científico da época, ao mesmo tempo em que permanece lenta nossa capacidade de amadurecer o controle sobre os processos sociais decorrentes desse.³⁷

A metáfora de controle total do Grande Irmão, embora seja convincente e se aproxime dos governos totalitários que romperam e ainda rompem nas democracias ocidentais, não é a única possível. O *panóptico* de Bentham e o *Big Brother* de George Orwell não são os únicos modelos possíveis de controle. Hoje, o controlado pode também ser tornar o controlador. Rodotà atenta para o fato de que “a imagem de tantos ‘Pequenos Irmãos’ [*Small Brothers*] tende a se substituir àquela *orwelliana* do ‘*Big Brother*’”.³⁸

Tanto as metáforas de Franz Kafka sobre os poderes obscuros que exercem controle sem que saibamos ao certo como funcionam³⁹, tanto os romances do século XXI que retratam o controle da tecnologia sobre os indivíduos, ilustram modelos que superam a modernidade sólida e sua arquitetura fixa.⁴⁰

O renomado autor Daniel J. Solove, na obra publicada em 2004, *The Digital Person*⁴¹, aborda que a metáfora não é simplesmente uma descrição de algo, mas sim a forma como conceituamos alguma coisa. Dessa forma, não são importantes por oferecerem uma descrição precisa e real das coisas, mas sim por direcionarem nosso foco para certos fenômenos políticos e sociais, especialmente nossas preocupações com a privacidade.⁴²

37 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 42.

38 Ibidem, p. 146.

39 Dentre as obras do autor, cita-se O Processo. O romance conta a história de Joseph K., que acorda certa manhã e descobre que é processado e sujeito a um longo e incompreensível processo por um crime não especificado pelas autoridades.

40 BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. p. 18.

41 SOLOVE, Daniel J. The Digital Person: Technology and Privacy in the Information Age: NYU Press, 2004.

42 Ibidem, p. 27-28.

Em sua obra, ao analisar a metáfora constantemente utilizada do *Big Brother* de George Orwell, contudo, entende que a vigilância por meio dos dados pessoais é totalmente nova, o método de controle não se dá mais através de olhos ou câmeras de vigilância, mas sim através da coleta de fatos e de dados. Dessa forma, a metáfora correta deveria também abordar formas de autocontrole.⁴³

Hoje, dissolveu-se a fixidez rígida das formas em um modelo pós-pan-óptico mais ardiloso, em que, segundo Bauman, “o poder pode se mover com a velocidade do sinal eletrônico – e assim o tempo requerido para o movimento de seus ingredientes essenciais se reduziu à instantaneidade”.⁴⁴ Cumpre ressaltar que a transparência promovida não se dá para ambos os lados, visto que continua obscura a forma de atuação das organizações de vigilância.

Nesse sentido, dentre as obras atuais que retratam a sociedade da vigilância, podemos citar o livro *O Círculo* de Dave Eggers. No mundo distópico retratado no livro, é apresentada uma realidade já muito próxima à atual. Na fábula, uma poderosa empresa de tecnologia passa a controlar todos os cidadãos do país, sobrelevando-se, inclusive, ao próprio Estado. Para exercer esse controle, são utilizadas as redes sociais e o tratamento incessante de dados pessoais dos usuários, em uma escala superabundante e de hipercapilaridade.⁴⁵

Da mesma forma, séries como *3%*^{46 47} e *Black Mirror*⁴⁸, demonstram que a crença em um progresso tecnológico e científico só poderia ser vivenciada por uma pequena minoria privilegiada. Em um contexto global, portanto, demonstram-se intangíveis as benesses tecnológicas para toda a população, acarretando não em qualidade de vida ampliada, mas sim em incremento das formas de controle. Segundo Lyon:

43 SOLOVE, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*: NYU Press, 2004. p. 32-33.

44 BAUMAN, Zygmunt. *Modernidade Líquida*. Rio de Janeiro: Zahar. p. 18.

45 EGGERS, Dave. *O Círculo*. São Paulo. Companhia das Letras, 2014.

46 *3%* [Seriado]. Direção: César Charlone et al. Produção: César Charlone et al. Brasil: Boutique Filmes, 2016.

47 *3%* é uma série de televisão brasileira de ficção científica que retrata um mundo pós-apocalíptico em que a maior parte da população habita um local miserável (*Continente*), enquanto uma minoria (3%) mora no *Maralto*, local com elevada qualidade de vida. Para habitar o *Maralto* é necessário passar por um processo seletivo que atesta algumas habilidades específicas dos cidadãos.

48 *BLACK MIRROR* [Seriado]. Direção: Joe Wright et al. Produção: Barney Reisz. Reino Unido: Zeppotron, 2011.

“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”.⁴⁹

Como exemplo de série de televisão obscura e satírica, podemos citar a aclamada série *Black Mirror*, que foi responsável por um levante de debates acerca da ingerência da tecnologia em nosso cotidiano. Os distintos capítulos, à primeira vista, representam cenários futuros repletos de dispositivos ultra tecnológicos que, aplicados à rotina das comunidades, tornaram-se catastróficos para a sociedade como um todo.

Através da análise dos episódios, podemos perceber panoramas comuns das distopias, como é o caso da espetacularização da mídia e o papel das redes sociais, a dependência e o controle da tecnologia sobre o homem, abusos de poder, solidão, violência legitimada, vigilância extrema e assim por diante.

Black Mirror, contudo, não nos descreve um cenário futuro e longínquo que poderíamos por ventura, remota e desgraçadamente, habitar, mas, pelo contrário, somente metaforiza o mundo que já se coloca para nós como uma realidade tangível. Como bem explicitado pelo criador da série Charlie Brooker:

“Cada episódio tem um elenco diferente, um cenário diferente e até uma realidade diferente, mas todos eles são sobre a forma como vivemos hoje - e a forma como nós poderemos estar vivendo em 10 minutos se não tomarmos cuidado.”⁵⁰

O episódio intitulado *Nosevide*⁵¹, da série de televisão supracitada, retrata uma realidade não muito distante da nossa, em que o que importa não é meramente a felicidade, mas sim o status apresentado perante a sociedade. No episódio, cada indivíduo apresenta uma nota baseada em diversos fatores de sua existência social e que influenciam diretamente nas suas possibilidades e limitações cotidianas.

49 BAUMAN, Zygmunt. *Modernidade Líquida*. Rio de Janeiro: Zahar. p. 108.

50 BROOKER, Charlie. *The dark side of our gadget addiction*. *The Guardian*, 01.12.2011. Disponível em: <<https://www.theguardian.com/technology/2011/dec/01/charlie-brooker-dark-side-gadget-addiction-black-mirror>>. Acesso em: 23 nov. 2018.

51 NOSEVIDE (Temporada 3, ep. 1). *Black Mirror* [Seriado]. Direção: Joe Wright et al. Produção: Barney Reisz. Reino Unido: Zeppotron, 2016. 1 DVD (63 min.), son., color.

Uma nota baixa pode significar a exclusão de determinados serviços ou ambientes, bem como de relações com determinadas pessoas com notas mais elevadas. Portanto, essa interligação, expressa de modo *exagerado* pela série, assemelha-se muito da atual realidade, especialmente em países autoritários como a China, em que este tipo de controle é mapeado e concretizado pelo próprio Estado.

Além do fato dessa atribuição de notas representar verdadeira “*gamificação do autoritarismo*”, ou seja, a aplicação de elementos e mecânicas de *design* de jogos em um contexto de repressão, os critérios subjetivos empregados revelam um mundo de opacidade em que nunca nos é possível saber exatamente como estamos sendo avaliados.

O filme de ficção científica *Minority Report*⁵² (2002), bem como o romance homônimo de Philip K. Dick⁵³, tratam de uma sociedade no ano de 2054 em que os crimes são evitados em razão da possibilidade de prever, com antecedência razoável, como, onde e quando esses viriam a ser cometidos. Dessa forma, os criminosos já eram apreendidos antes mesmo de cometer o crime, com base no depoimento de três videntes, os “*precogs*”.

No mundo real, através do emprego de técnicas tecnológicas e de raciocínio estatístico, também torna-se cada vez mais possível monitorar o futuro. A vigilância acompanha nossas informações a todo tempo, podendo ocasionar processos de ações repetitivas e medidas de exclusão daqueles “indesejados”.⁵⁴

Nesse sentido, a manipulação de dados por parte da inteligência artificial, através de sua replicação e fragmentação, pode acabar por inspirar mais confiança que a própria pessoa, como acontece na ficção em análise.

1.5. Tecnologia como meio de controle da população: “*A Smart Machine*”

⁵² MINORITY REPORT. Direção: Steven Spielberg. Estados Unidos da América: Cruise/ Wagner Productions et al, 2002. 1 DVD (2h 26 minutos).

⁵³ DICK, Philip K. *Minority Report – A nova lei*. Brasil: RECORD, 2002.

⁵⁴ BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 13.

Segundo Shoshana Zuboff no artigo *Big other: surveillance capitalism and the prospects of an information civilization*⁵⁵, as perspectivas de constante transformação da *Internet* mantêm, todavia, certas características inerentes aos seus mecanismos de controle, como as relações de dominação e alienação que continuam a permear seu meio. A autora vai, através de seus apontamentos, destacar a *nova lógica de acumulação baseada na vigilância massiva*, cujo resultado é o desenvolvimento de um capitalismo de vigilância e de uma nova era de civilização.

Como tratado anteriormente, a sociedade contemporânea pode ser classificada como uma sociedade da informação, em que esta apresenta peso relevante, tanto econômico quanto social. Dessa forma, através de análises concretas, a autora pode observar alarmante geração de valor sobre as informações e dados dos usuários de serviços e produtos na internet, como no caso dos usuários da empresa Google.

No caso supracitado, os dados de seus usuários são massivamente extraídos, armazenados e processados em torno de uma dinâmica que explora e incorpora valor ao que antes representavam esparsas informações. Esta nova forma de trabalho automatizado por tecnologias de informação, como os computadores, é inteiramente baseada no conhecimento. A partir do registro dos dados coletados, os próprios mecanismos passam a automatizar e aprimorar cada vez mais sua produtividade, em conformidade com o aumento da quantidade de dados processados.

A empresa, logo, é capaz de não cobrar diretamente o usuário final pela disponibilização do serviço, porém, extraíndo sua fonte de riqueza diretamente dos dados e informações disponibilizados pelos mesmos. Desta forma, comercializa as informações em troca de compensações financeiras.

Um dos exemplos mais característicos dessa conversão das informações em valor econômico se dá através do algoritmo *AdWord*, que orienta a disposição da propaganda dos clientes da empresa *Google* em suas páginas no navegador da rede, com apoio em palavras-

⁵⁵ ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of na information civilization. Journal of Information Technology, 2015.

chave utilizadas pelo usuário na pesquisa. Resta salientar que a possibilidade publicitária não se limita a este algoritmo, apresentando, ainda, uma série de outras modalidades a serem exploradas.

Como visto, atualmente, nossas trocas sociais são em grande parte mediadas por dispositivos em rede, ocasionando uma extração quase infinda de informações. A consequência prática disso é o permanente monitoramento e vigilância de dados. Todavia, há quem defenda um aspecto positivo desta vigilância, que poderia ser revertida em comodidade e bem-estar para os usuários. A formação de perfis de comportamento poderia de certa forma antecipar as ações dos usuários de modo a dirimir riscos na tomada de decisões política ou econômica.

Entretanto, Zuboff atenta para o fato dessa imprevisibilidade ser parte componente da autonomia do indivíduo, sendo duvidoso seu desejo de eliminação. Um dos aspectos mais preocupantes dessa anulação da autonomia se dá através da tentativa de controle explícito sobre o comportamento do usuário, modulando-o através da identificação de padrões.⁵⁶

O alarme se justifica pelo fato de determinados agentes econômicos políticos poderem fazer uso deste controle para beneficiar seus próprios interesses. Hoje, a governança algorítmica é capaz de exercer um poderio velado sobre o comportamento das pessoas, tema no qual nos aprofundaremos mais adiante.

1.5.1. *Big Data* e o imperativo da vigilância

Retomando, a sociedade contemporânea, característica por seu mercado competitivo e inovação tecnológica constante, induziram as empresas e órgãos públicos a uma ininterrupta busca pela informação. Apresentando, para aqueles que dominam estas tecnologias, uma imensa vantagem no tocante à sobrevivência dos próprios institutos e instituições.

⁵⁶ ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of na information civilization. *Journal of Information Technology*, 2015. p. 75-89.

Neste diapasão, os sujeitos renegam as suas informações pessoais em troca de disponibilização de serviços e vantagens econômicas. Por conseguinte, a quantidade de dados disponíveis sobre os usuários e processados com o intuito de obter vantagens competitivas no mercado já se expande a níveis colossais.

O imperativo de vigilância é tamanho no tocante à coleta de dados pessoais hoje que não se trata mais somente dos dados em si e do significado que carregam, mas também da obtenção de informações completamente novas a partir da combinação destes dados quando analisados em conjunto. Estes modernos métodos tecnológicos de associação de dados fizeram surgir o que conhecemos hoje como “*Metadados*” ou “*Big Data*”.

Ao passo em que os *Metadados* podem ser conceituados como dados sobre outros dados, acrescentando novas informações aos dados pessoais e tornando mais acessível sua organização; o *Big Data* pode ser descrito como o gigantesco volume de dados, estruturados ou não, que, após serem localizados, analisados e processados em tempo hábil, são utilizados para a elaboração de ações estratégicas, políticas ou de negócios.

Em contraponto aos benefícios que podem advir desta nova tecnologia como, por exemplo, a promoção de políticas públicas adequadas e a interpretação de tendências de eventos de ordem econômica, de aceitação de produtos, de tráfego público e de ordem climática; podem ser percebidas as consequências sociais negativas frutos da má utilização dos dados pessoais em prol de interesses escusos.

De acordo com Zygmunt Bauman, no livro *Vigilância Líquida*, a Sociedade da Informação, por ter tornado os dados pessoais bens valiosos para elaboração de estratégias de *marketing* e publicidade, acaba por promover reiteradas violações de direitos fundamentais em uma constante vigilância de seus usuários. Segundo o autor, na era digital, em que o status do consumidor se altera a cada novo bit de informação transacional, suas chances de tornar-se alvo de alguma forma variam de acordo com os níveis de tráfego e a trilha de rastros mais recente que deixou pra trás.⁵⁷

57 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 20-25.

No decorrer de nossas vidas cotidianas deixamos, em diversos dispositivos, uma série de rastros eletrônicos que são capazes de nos identificar, influenciar em nossos relacionamentos amorosos, reconstruir nossos trajetos, revelar nossas escolhas e desejos mais íntimos. Dessa forma, a vigilância é perpétua enquanto estivermos inseridos nesta rede, tornando-nos alvos de observadores por trás dessas fechaduras digitais que compõem a internet, ao mesmo tempo em que aumenta nossa vulnerabilidade frente as empresas ou ao próprio governo.⁵⁸

Para ilustrar esse contexto, podemos analisar a realidade chinesa atual, que muito se aproxima do episódio anteriormente analisado da série *Black Mirror, Nosevide*⁵⁹. No ano de 2014 o governo chinês anunciou os planos para criação de um sistema de crédito social, o *Social Ranking Score*, até o ano de 2020. Este sistema, todavia, já está sendo implementado através de empresas privadas que, por meio de um complexo sistema de algoritmos, determinam pontuações para cada indivíduo, colocando-os em ranking de acordo com essas notas.

Esses algoritmos dialogam com uma série de dados pessoais de cada indivíduo e se combinam para gerar a referida pontuação. O caso é tão emblemático que notas baixas nesses rankings significam a exclusão de, por exemplo, uma gama de serviços privados e públicos; enquanto notas elevadas representam vantagens das mais variadas formas. Lucy Peng, CEO da *Ant Financial* (filiada da *Alibaba* e maior empresa de serviços financeiros online da China), afirmou que o sistema “vai garantir que as pessoas más na sociedade não vão ter para onde ir, enquanto as boas pessoas podem mover-se livremente, sem restrições”.⁶⁰

58 GHISLENI, Eduardo Steffenello. Vigilância na sociedade em rede: A coleta de dados pessoais na internet e suas implicações ao direito à privacidade. 2015. 60 f. Trabalho de Conclusão de Curso (Graduação em Direito)-UFSM, Santa Maria, 2015. Disponível em:<<https://repositorio.ufsm.br/bitstream/handle/1/11518/MONOGRAFIA%20EDUARDO%20S%20GHISLENI.pdf?sequence=1&isAllowed=y>>. Acesso em: 25 nov. 2018.

⁵⁹ NOSEVIDE (Temporada 3, ep. 1). *Black Mirror* [Seriado]. Direção: Joe Wright et al. Produção: Barney Reisz. Reino Unido: Zeppotron, 2016. 1 DVD (63 min.), son., color.
60 RR. “Black Mirror” ou vida real? China começa a “avaliar” pessoas em aplicação. *Renascença*, 20.03.2018. Disponível em: <https://rr.sapo.pt/noticia/108659/black-mirror-ou-vida-real-china-comeca-a-avaliar-pessoas-em-aplicacao>. Acesso em: 23 nov. 2018.

A *Alibaba*⁶¹, uma das companhias responsáveis pela formulação de *rankings* de crédito social, não divulgou, até o presente momento, o “complexo algoritmo” que utiliza para o cálculo da pontuação de cada cidadão, contudo, apresentou os cinco fatores que são levados em conta: o histórico financeiro do utilizador; a capacidade do utilizador cumprir suas obrigações contratuais; suas características pessoais, como endereço e número de telefone; o comportamento e a preferência do investigado, podendo classificá-lo como pessoa produtiva ou não e; por último, suas relações interpessoais, como o fato de falar positivamente ou negativamente do governo chinês em redes sociais.

Nesse sentido, a distópica realidade chinesa atual, representada pelo *Social Ranking Score*, digitalizou os métodos de vigilância do Estado em uma desenfreada e cada vez mais profunda tentativa de controle sobre a população através de seus dados pessoais. Em uma análise mais profunda, é possível perceber que a formação de perfis visa categorizar condutas que ocasionam, em último caso, a simulação e até a determinação de comportamentos futuros.

Todavia, essas consequências temerárias não se limitam ao Estado Chinês, no mundo todo vem se tornando possível manipular as escolhas e a própria vida dos usuários, como consequência indireta dos novos e preocupantes usos que se dão ao instrumento do *Big Data*, sobre os quais nos aprofundaremos mais adiante, principalmente no tocante aos seus aspectos discriminatórios.

1.5.2. *Social Big Data* e a delegação da escolha às máquinas

“A vida é apenas uma sombra ambulante, um pobre cômico que se empavona e agita por uma hora no palco, sem que seja, após, ouvido; é uma história contada por idiotas, cheia de fúria e muita barulheira, que nada significa”.⁶²

O *Big Data*, ou esse conjunto massivo de dados pessoais, está atualmente responsável por uma série de tomadas de decisões ao redor dos mais diversos setores. Partindo de uma visão positiva destes reflexos, são proporcionadas decisões assertivas sobre problemas

61 Alibaba Group ou Grupo Alibaba é um grupo de empresas com sede em Hangzhou, China, de propriedade privada baseada em e-commerce na internet, incluindo sites online de business-to-business, serviços de varejo e pagamento online, um motor de busca para compras e serviços de computação na nuvem centrados em dados.

62 SHAKESPEARE, William. *Macbeth*. São Paulo: Paz e Terra, 1996. p. 126.

orgânicos e complexos. Todavia, resta-nos questionar sobre seus impactos na autonomia dos indivíduos para decidir e sobre os efeitos colaterais no uso indiscriminado deste meio.

Os usuários globais têm muitas vezes preterido sua própria autonomia em troca de decisões teoricamente mais inteligentes e convenientes operadas através do processamento de dados. Essa aparente contradição se justifica pois, ao utilizar uma interface que realiza parte de sua decisão, a eventual responsabilidade por decisões ruins passa a ser compartilhada com a máquina, ou até mesmo transferida integralmente a ela, de forma a se evadir da responsabilidade de uma decisão efetivamente autônoma.

Ao presumir desejos e ocultar o que supostamente não é de interesse do usuário, ocorre uma desmedida simplificação do processo decisório do indivíduo, do qual é retirada a oportunidade de se surpreender com alternativas nunca antes consideradas e de reavaliar suas próprias preferências. Nesse sentido, é suprimida característica intrínseca ao processo de conhecimento humano.⁶³

Um dos aspectos dessa tendência das máquinas efetuarem escolhas para os usuários, em razão de um suposto aprimoramento das mesmas, passa, inclusive, por nossas predileções afetivas nas redes sociais. Como exemplo, a plataforma do *Facebook*, através das bolhas de filtro, pode, dentre uma quantidade acentuada de amigos, determinar de quem vamos receber mais atualizações, ou como essa disposição se dará diante da *timeline* de cada usuário.

Essa escolha, que afeta relações pessoais e culturais do indivíduo, pode se dar com base na frequência da interação com os “amigos”, mas também pode levar em consideração uma série de outros fatores os quais ainda são desconhecidos para aqueles que fazem uso da plataforma.

63 RODRIGUEZ, Luís; SPITZ, Rejane. Big Data *versus* autonomia: O paradoxo do suporte à “decisão autônoma” usando Big Data. Congresso Brasileiro de Pesquisa e Desenvolvimento em Design – 12º P & D 2016. Rio de Janeiro, n. 2, vl. 9, 2016. Disponível em:<<http://pdf.blucher.com.br.s3.amazonaws.com/designproceedings/ped2016/0344.pdf>>. Acesso em: 23 nov. 2018.

Questiona-se David Lyon: “Haveria algo inelutável quanto aos efeitos malignos da mediação eletrônica, ou será que as mesmas tecnologias também facilitam as relações humanas e, ao que se espera, sociais?”⁶⁴. A partir desta indagação, não propõe o autor que se tenha uma visão neutra da rede e das escolhas que produz, muito pelo contrário, atenta para o fato do desenvolvimento tecnológico ser fruto do contexto social, político e cultural no qual está inserido.⁶⁵

Nesse sentido, apesar das escolhas produzidas apresentarem “tendências morais”, a tecnologia poderia vir a ser aplicada tanto em seu aspecto negativo de distanciamento entre pessoas e entre pessoas e suas escolhas, quanto num sentido positivo de romper barreiras geográficas.

Com o intuito de ilustrar o debate, convém apresentar um episódio da série original de Jornada nas Estrelas (*Star Trek*), no qual o tema central é a guerra computadorizada. O episódio *A Taste of Armagedon*⁶⁶, que foi ao ar no ano de 1967, tem início com a nave *Enterprise* adentrando em um sistema intergaláctico onde devem ser estabelecidas relações de paz com os cidadãos nativos do planeta.

Mesmo após receberem ordens para se afastar, o capitão Kirk é intimado pelo embaixador Robert Fox para ir até o planeta e tentar o diálogo com aqueles. Quando chegam ao planeta *Eminiar 7*, descobrem que este está inserido em um sistema computadorizado de guerra, onde os efeitos de eventuais conflitos com outros planetas são determinados por cálculos matemáticos feitos por um computador.

O computador era capaz de substituir a guerra em si, portanto, não existia mais o contato físico entre planetas inimigos. As mortes eram calculadas e registradas pelo computador que simulava os eventuais ataques e, neste diapasão, determinava também quem eram os cidadãos de cada planeta que haviam falecido neste fictício ataque. Em seguida,

64 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 91.

65 *Ibidem*, p. 92.

66 *A TASTE OF ARMAGEDON* (Temporada 1, ep. 23). *Star Trek* [Seriado]. Direção: Joseph Pevney. Produção: Gene L. Coon. Estados Unidos: Desilu Productions, 1967. 1 DVD (50 min.), son., color.

aqueles que fossem designados eram obrigados a entrar em uma câmara de desintegração onde de fato vinham a falecer. Desta maneira, não se perderia em construções, objetos e cultura, a *única* perda seriam vidas humanas.

O ápice da trama se dá no momento em que a nave *Enterprise* é considerada vítima do último ataque computadorizado, por estar inserida na órbita do planeta *Eminiar 7*. Destarte, Roddenberry⁶⁷ nos faz refletir sobre o desenvolvimento técnico da sociedade e em sua suposta evolução, mas que, por ventura, acabaria por corroborar para um falecimento de características essenciais da humanidade.

Uma das falas emblemáticas do episódio é externada pelo Capitão Kirk, após contornar a situação e salvar toda a tripulação da *Enterprise*, destruindo os referidos computadores logo em seguida:

Kirk: “Morte... destruição, doença, horror... isto é o que toda guerra é, Anan. É o que faz disto uma coisa a ser evitada. Você tem isto de maneira organizada e indolor. Tão organizada e indolor, que não tem razão para pará-la”.⁶⁸

Este episódio, portanto, apenas retrata a era de tecnicização que estamos vivendo até hoje e a cada vez maior delegação de nossas escolhas às máquinas. Com a inflexão da técnica neutralizando nossas decisões, podemos observar o caráter perigoso da pura e simples utilização de métodos objetivos em considerações que antes se davam de maneira prioritariamente subjetiva. Através dos recentes métodos de manipulações de dados por meio da Inteligência Artificial, constata-se uma crescente racionalização não humanista e que ignora propositalmente considerações de caráter moral e toda a discriminação que se possa decorrer disso.

Por fim, cabe-nos refletir sobre a existência ou não de padrões éticos na escolha da Inteligência Artificial, visto que os algoritmos também são projetados por seres humanos como nós, estes que não derivam de outros planetas. O intuito das indagações é de se atentar

⁶⁷ Eugene Wesley Roddenberry foi um roteirista e produtor de televisão norte-americano. É o criador da série de ficção científica Star Trek.

⁶⁸ PEREIRA, Yuan V. A fronteira final: Guerra fria e movimentos pacifistas refletidos em Jornada nas Estrelas. Unilasalle Editora – Diálogos. Canoas, n. 34, 2017. Disponível em:< <https://revistas.unilasalle.edu.br/index.php/Dialogo/article/view/3290>>. Acesso em: 23 nov. 2018.

para os desafios que se assomam aos avanços tecnológicos, não entendendo-os como meros instrumentos de neutralidade, e sim como uma parte integrante de uma reestruturação social e moral da modernidade.

Bauman aponta para uma forte tendência de “*adiaforização*”, em que se prega a separação entre sistemas e processos e quaisquer considerações de caráter moral. Caminha-se para formas de eufemização da culpa em vista da distância cada vez maior entre os sujeitos e os métodos decisórios. Inclusive a nomenclatura “dados pessoais” surge a partir do conceito de informações que originam de seu corpo e que afetam seus ensejos e escolhas existenciais.

69

Sistemas de decisões automatizadas têm cada vez mais sido utilizados para, através do recolhimento de informações, definirem uma postura a ser tomada. Os dados coletados, apesar de sempre parciais e incompletos, são utilizados para embasar decisões sobre os próprios usuários em questões “no mais das vezes, mais significativas que as judiciais ou administrativas, e que são aquelas que dizem respeito ao cidadão consumidor ou usuário de serviços (comerciais, bancários e assim por diante)”.⁷⁰

Diante da complexidade do tema, a legislação não pode se limitar a proibir que decisões sejam tomadas utilizando-se unicamente esses perfis automáticos, quando em verdade deviam apreciar o comportamento humano. Além dessa tutela negativa, deve-se ter em mente uma concepção positiva de direito à informação, visto que o interessado deve poder conhecer e julgar a forma como estão sendo tratadas suas informações.⁷¹

Segundo Rodotà, a automatização de perfis poderia conduzir a uma perda cognitiva por parte dos cidadãos, visto que:

“Por um lado, portanto, dá-se início a um mecanismo que pode bloquear o desenvolvimento daquela comunidade, solidificando-a no seu perfil traçado em uma situação determinada. Por outro lado, penalizam-se os poucos que não correspondem ao perfil geral, iniciando-se assim um perigoso processo de discriminação de

69 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 102.

70 RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 115.

71 *Ibidem*, p. 68-69.

minorias. A “categorização” dos indivíduos e grupos, além disso, ameaça anular a capacidade de perceber as nuances sutis, os gostos não habituais”.⁷²

Dessa forma, a criação de perfis gera a estigmatização daqueles que apresentam comportamentos desviantes dos demais, ao mesmo tempo em que ocasiona a penalização de minorias que também não se enquadram às expectativas dos provedores. Diante desse cenário, urgente se faz a necessidade de defender o direito em deixar rastros eletrônicos sem que, com isso, surja alguma forma de punição.

1.6. Internet das Coisas (IoT): O advento da *Web 4.0*

Segundo Olga Cavalli, pesquisadora da área, o que hoje é chamado de Internet das Coisas (*Internet of Things*) nada mais é que um aglomerado de tecnologias e protocolos associados que permitem que objetos se conectem a uma rede de comunicações. Através desta rede, portanto, os objetos seriam identificados e controlados.⁷³

Essas “coisas” seriam, de acordo com o cientista Silvio Meira, dispositivos que possuem, concomitantemente, capacidades de computação, comunicação e controle. Dessa forma, segundo o autor, se esse dispositivo não tem característica que lhe permita o controle das informações, seria apenas uma máquina em rede; por outro lado, se não possui capacidade de comunicação, é simplesmente um sistema de controle digital; por fim, se não apresenta capacidades de computação, é um sistema de telemetria, ou seja, um sistema tecnológico de monitoramento.⁷⁴

Portanto, as três características abordadas representam requisitos cumulativos e devem estar inseridas no meio digital para que se possa falar em Internet das Coisas. Nessa lógica, as “coisas” seriam objetos digitais completos. De forma genérica, poderíamos entender este ambiente como um ecossistema de computação onipresente, com o objetivo de facilitar a

72 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 83.

73 CAVALLI, Olga. Internet das coisas e inovação na América Latina. [S.l.: s.n.]: Mimeogr, 2016 apud MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. p. 20.

74 MEIRA, Silvio. Sinais do futuro imediato, #1: internet das coisas. Recife: Ikewai, dez. 2016 apud MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. p. 20.

integração e a solução de entraves do nosso dia a dia, em um contexto de *hiperconectividade*.

75

Assim sendo, faz-se necessário entender as Eras da *Internet* e suas respectivas características, salientando as diferenças entre a *Web 1.0*, *2.0*, *3.0* e possíveis futuros desdobramentos. Preliminarmente, em meados da década de 1980, a *Web 1.0* ficou popular por ser a “*web* do conhecimento” e por, justamente, representar uma facilidade de acesso a informações nunca antes vista na história, oferecendo aos seus usuários grandes volumes de conteúdo antes restritos aos objetos físicos, como os livros. Em seguida, surgiu a *Web 2.0*, conhecida como a “*web* da comunicação”, por conta de grande interatividade possibilitada por meio de suas plataformas.

Cumprido ressaltar que esse salto entre Eras não foi ocasionado por alguma inovação tecnológica relevante, e sim por conta das transformações nas formas de utilização de ferramentas que já estavam disponíveis na *Web 1.0*⁷⁶. Nesse contexto, as principais inovações da *Web 2.0* dizem respeito ao seu caráter colaborativo e de intensa interação entre os usuários. Essas novas formas de se relacionar na *internet* foram possibilitadas por conta da expansão das plataformas como as redes sociais e os blogs que, por seu lado, tornaram mais descomplicadas as produções de conteúdo na *internet*.

Por fim, o termo *Web 3.0*, que representa a 3ª e atual geração da *Internet*, foi empregado pela primeira vez pelo jornalista John Markoff em um artigo publicado no *The New York Times*⁷⁷, proporcionando um uso mais inteligente de todo o conteúdo já existente nas gerações pretéritas. Ao passo em que a *Web 2.0* possibilitou a interação entre os usuários, a *Web 3.0* foi a responsável por começar a proporcionar o cruzamento de dados, a fim de obter informações mais precisas. Uma das características mais inovadoras desta nova geração se daria justamente pelo conceito da Internet das Coisas, em que os objetos que a compõem interagem com pessoas e também com outros objetos.⁷⁸

⁷⁵ MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. p. 2.

⁷⁶ Ibidem, p. 65.

⁷⁷ MARKOFF, John. Entrepreneurs See a Web Guided by Common Sense. *The New York Times*, 12.11.2006. Disponível em: <https://www.nytimes.com/2006/11/12/business/12web.html>. Acesso em: 23 nov. 2018.

⁷⁸ MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. p. 68-69.

Segundo o pesquisador Eduardo Magrani, já estão sendo formuladas definições e predições sobre as gerações de *webs* que as seguirão, visto que os avanços tecnológicos avançam de forma cada vez mais intensa. Investigadores apontam que a *Web 4.0* ou *5.0* será uma “*web simbiótica*”, que integra cada vez mais o ser humano às tecnologias em si, esta geração de *web* poderá ser característica por incluir sentimentos e até emoções ao que antes eram só máquinas, ou, por outro lado, por transformar a *web* em um cérebro paralelo ao nosso.⁷⁹

Nessa linha, por meio da nova era, seria fabricado um sistema operacional dinâmico e inteligente capaz de coletar e processar dados disponíveis a fim de suportar uma série de tomadas de decisões. Dessa forma, um sistema complexo de inteligência artificial é, certamente, a característica mais esperada por estudiosos da *web*, esta que já se projeta em nossa realidade presente.

⁷⁹ MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Direito Rio, 2018. p. 73.

2. DIREITO À PRIVACIDADE E OS DADOS PESSOAIS COMO NOVO DIREITO DE PERSONALIDADE

“Quanto à “morte do anonimato” por cortesia da internet, a história é ligeiramente diferente: submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir”.⁸⁰

Segundo Stefano Rodotà, inicialmente, a privacidade não era vista como a realização de um direito natural de cada indivíduo, mas sim como fruto da aquisição de privilégios por parte de determinados grupos, representando a conotação elitista na qual se fundou.⁸¹ Em verdade, o “direito de ser deixado só” representava um real abandono dos mais fracos e menos privilegiados à violência social.⁸²

Todavia, apesar de não se abandonar inteiramente esse conceito, transforma-se com as novas tecnologias em um método de promover igualdade e paridade de tratamento entre os cidadãos, rompendo sua conexão direta com os privilégios da burguesia. Dessa forma, a proteção da privacidade tende a crescer ainda mais no futuro, visto que passa a ser de interesses de camadas cada vez mais amplas da sociedade.

É pacífica a posição de que a compreensão de privacidade como meramente o “direito de ser deixado só” já resta ultrapassada. Hoje em dia, o que se discute é a possibilidade de indivíduos e coletivos controlarem a disponibilização das informações e o modo como serão tratadas, a fim de estabelecer equilíbrios mais adequados nessa relação de poder que se forma através da crescente importância da informação, tanto para o setor público quanto para o privado.⁸³

80 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 28.

81 RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 27.

82 *Ibidem*, p. 28.

83 *Ibidem*, p. 24.

No atual contexto, tende a prevalecer uma visão funcional da privacidade, visto que, diante das novas tecnologias, esse termo faz referência à possibilidade do usuário conhecer, controlar e romper o fluxo de informações a ele relacionadas. Dessa forma, pode ser lida como um direito de manter o controle sobre as próprias informações, afastando formas de estigmatização social que poderiam ser produzidas.⁸⁴

As estratégias de defesa perseguidas visam “afastar os temores de uma iminente chegada do *1984* de Orwell ou do *Brave New World* imaginado por Aldouls Huxley”.⁸⁵ Entretanto, ainda estamos caminhando para uma transformação das definições jurídico institucionais que permeiam o debate. Dessa forma, faz-se mister a readaptação dos conceitos aos novos significados que a tecnologia produz, refletindo-se, também, na necessidade de ampliar sua dimensão coletiva, entendendo o indivíduo como pertencente a determinado grupo social.

2.1. Privacidade, intimidade e vida privada

Primeiramente, insta analisar os termos presentes na doutrina brasileira a fim de conceituar a noção de privacidade. Além do termo “privacidade” propriamente dito, foram utilizados outros termos como: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, entre outros. Dessa forma, Doneda atenta para o fato de que nos falta uma definição chave que abarcar estes conceitos.⁸⁶

Acontece que, no decorrer da história, foram diversos os caminhos trilhados para se chegar a uma ou mais definições, sendo que estas variavam conforme o ordenamento e as particularidades de cada sociedade. Nesse sentido, tornou-se cada vez mais difícil a definição de um sentido comum. Doneda alerta para o fato de que talvez essa indefinição não seja um

84 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 92.

85 Ibidem, p. 25.

86 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 63.

obstáculo a ser superado, podendo ser apreendida como “uma característica ontológica da própria construção da esfera privada”⁸⁷.

Especificamente no Brasil, a Constituição Federal de 1988⁸⁸ incluiu, entre as garantias e direitos fundamentais elencados no seu artigo 5º, a proteção da “intimidade” e da “vida privada” (além de “honra” e “imagem”), para fins de proteção da pessoa humana:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

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

Por conta disso, cabe ao intérprete a compreensão da amplitude destes termos. De toda forma, a terminologia utilizada pela CRFB/88 deve ser interpretada no contexto dos direitos fundamentais que busca proteger, não sendo o melhor caminho, de acordo com Doneda, “insistir em uma conceitualística que intensifique as conotações e diferenças semânticas dos dois termos”.⁸⁹

Dessa forma, com o intuito de fortalecer um ordenamento jurídico ordenado e unitário, faz-se miste integrar os dois termos, intimidade e vida privada, por meio de atividade interpretativa. Portanto, conclui o autor que os termos não devem ser valorados de forma diferente, principalmente por conta da ausência de clara distinção terminológica na doutrina e jurisprudência e porque essa discussão desviaria o foco da questão principal, que é a aplicação do direito fundamental.⁹⁰

Por fim, opta pela escolha terminológica em se utilizar unicamente o termo “privacidade”, visto que seria específico o suficiente para abarcar os valores expressos no

87 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 64-66.

88 BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

89 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 67.

90 Ibidem, p. 68.

termos intimidade e vida privada, ao mesmo tempo em que se distingue de outros termos como imagem, honra ou identidade pessoal.⁹¹

Dessa forma, importante compreender a evolução histórica do conceito de privacidade. No século XIX, para se alcançar a privacidade, era necessário o exercício do direito de propriedade, estando ambos conceitos estritamente vinculados um ao outro. Todavia, a partir do século XX, com o surgimento dos meios de comunicação de massa, houve intensa transformação no eixo de gravitação do ordenamento jurídico que culminou em mudanças no conceito de privacidade e nos meios de protegê-la.⁹²

Um ponto de partida corrente entre os estudiosos da privacidade se dá com a análise da definição presente nos artigos de Warren e Brandeis⁹³, que é muitas vezes ilustrada pelo “direito de ser deixado só” (*right to be let alone*). Todavia, cumpre ressaltar que os autores em nenhum momento chegaram a definir de forma limitante o *right to privacy* nesse sentido, deixando a definição em aberto.⁹⁴

Mesmo o artigo de Warren e Brandeis, publicado em 1890 na revista *Harvard Law Review*, sobre o *right to privacy*, parte de um conceito mais ampliado de privacidade, desvinculando sua proteção do direito de propriedade.⁹⁵ Nesse sentido, a sua defesa se daria em torno da proteção da pessoa humana em si, vindo a ocupar futuramente na jurisprudência americana o lugar de um verdadeiro direito geral de personalidade.⁹⁶

O contexto do supracitado artigo se deu a partir do surgimento de um novo fato social que correspondia às mudanças trazidas pelas tecnologias de informação da época, como jornais e fotografias, bem como ao fenômeno da comunicação em massa. Nesse sentido, o

91 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 69.

92 Ibidem, p. 80-82.

93 WARREN, Samuel; BRANDEIS, Louis D. The right to privacy. 4 Harvard Law Review 193, 1890. Disponível em: < <http://www.spywarewarrior.com/uiuc/w-b.htm>>. Acesso em: 26 nov. 2018.

94 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 65.

95 Ibidem, p. 83.

96 PINTO, Paulo Mota. O direito à reserva sobre a intimidade da vida privada. In: Boletim da Faculdade de Direito, n. 69, 1993. p. 494 apud DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 84.

artigo possibilitou que o direito à privacidade nos Estados Unidos fosse tido como uma garantia constitucional.⁹⁷

Dessa forma, a necessidade de definição de um conteúdo comum para o direito à privacidade é fruto dessa massificação no fluxo de informações, pois que amplia a necessidade de se fortificar as formas de proteção. Para exemplificar esse momento histórico, podemos analisar que a partir da década de 70 o direito interconectou cada vez mais a noção de privacidade com a problemática do armazenamento de dados. Segundo Robert Ellis Smith:

“(...) hoje, quando se fala sobre privacidade, geralmente refere-se não apenas ao direito de manter o caráter confidencial de fatos pessoais, porém ao direito de saber quais informações sobre si próprio são armazenadas e utilizadas por outros, e também o direito de manter estas informações atualizadas e verdadeiras.”⁹⁸

Diversas teorias surgiram com o intuito de fragmentar a noção de privacidade, como a teoria de Hubmann de 1953, ou teoria das esferas concêntricas, que afirmava existirem diferentes graus de externalização do sentimento de privacidade; a esfera mais interna seria representada pela intimidade ou pelo segredo, em torno dela ficaria a esfera privada e, circundando ambas, a esfera pessoal, que incluiria a vida pública.⁹⁹

Todavia, esta teoria também ficou conhecida, segundo Herbert Burkert, como a teoria da “pessoa como cebola passiva”, posto que não se mostrava adequada para a devida proteção da pessoa humana em razão da segregação de suas esferas de privacidade. Dessa forma, após ser alvo de diversas críticas, foi abandonada pelo Tribunal Constitucional Alemão, em notável sentença de 1983.¹⁰⁰ Esta emblemática sentença também foi responsável por anular parcialmente a lei de censo populacional alemã que permitia que os dados do censo fossem rastreados até os respectivos cidadãos e que os mesmos fossem empregados para outras finalidades.

97 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 85.

98 SMITH, Robert Ellis. Privacy. How to protect what's left of it. New York: Anchor Press, 1979, p. 11 apud DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 87.

99 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 66.

100 Ibidem, p. 67.

Nesse sentido, cunhou a noção de um direito constitucional de autodeterminação informativa, estruturando os fundamentos da proteção de dados alemã na época.¹⁰¹ Segundo extrato da decisão:

"Não se pode levar em consideração somente a natureza das informações; são determinantes, porém, a sua necessidade e utilização. Estas dependem em parte da finalidade para a qual a coleta de dados é destinada, e de outra parte, da possibilidade de elaboração e de conexão próprias da tecnologia da informação. Nesta situação, um dado que, em si, não aparenta possuir nenhuma importância, pode adquirir um novo valor; portanto, nas atuais condições do processamento automático de dados, não existe mais um dado 'sem importância'."¹⁰²

Nesse sentido, o desenvolvimento da própria personalidade, livre de ingerências externas, é responsável por evitar a submissão ao controle social imposto, este que poderia limitar a individualidade e restringir a autonomia privada do indivíduo.

Além disso, a proteção da privacidade não pode mais ser lida apenas a partir da lógica da exclusão, como escudo contra o exterior, mas também como elemento impulsionador da cidadania. Apresenta, portanto, dimensão coletiva, visto que a cidadania é pressuposto da sociedade democrática moderna e, também, função promocional, pois busca promover a proteção da pessoa humana.¹⁰³

Por fim, a proteção da privacidade não se daria através de administração de “bens” ou “espaços”, mas sim através da determinação de nossa esfera pessoal, nem seria a privacidade um valor em si mesma, mas uma “forma” de tutela da pessoa. Assume a privacidade, portanto, um caráter relacional, visto que está vinculada a relação com outras pessoas e com o mundo exterior.

Nesse sentido, diferiria da teoria dos círculos concêntricos, visto que busca a construção de uma individualidade e o livre desenvolvimento da personalidade a partir de um conceito universal, sendo esta tutela fundamental para proteção da dignidade da pessoa humana.¹⁰⁴

101 FRAU, Christian. A luta contra o terrorismo e a proteção de dados pessoais. Revista da AGU nº 28. p. 102-103. Disponível em: <<file:///C:/Users/Usu%C3%A1rio.DESKTOP-RINM3A4/Downloads/163-427-1-PB.pdf>>. Acesso em: 23 nov. 2018.

102 FROSINI, Vittorio. Contributi ad un diritto dell'informazione. Napoli: Liguori, 1991. p. 128-129.

103 DONEDA, Danilo. Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 87.

104 Ibidem, p. 89- 90.

2.2. Proteção da dignidade da pessoa humana e a autodeterminação informativa

Conforme já visto anteriormente, transformou-se, com o tempo, a concepção de privacidade. Do direito de ser deixado só emergiu o direito de determinar a forma de construção de nossa própria esfera privada, perpassando pela possibilidade de controle do que é feito com as nossas informações. Nesse sentido, um importante passo foi dado no sentido de promoção de práticas que evitem a discriminação decorrente do mal uso dos dados, a favor da liberdade e, principalmente, igualdade no ciberespaço e fora dele.

Em um contexto de sociedade de informação em que os indivíduos podem ser determinados pelo seu conjunto de dados pessoais, posto que estes nos definem, classificam e etiquetam; ter o controle sobre os mesmos se torna de suma importância. Hoje, ter meios para decidir quem detém nossas informações e o que delas é feito significa ter poder sobre si. Dessa forma, a privacidade passa a ser entendida como um direito à autodeterminação informativa.¹⁰⁵

Através de inovações e técnicas recentes, a vigilância é ampliada e as formas de controle se tornam cada vez menos perceptíveis e mais nocivas para a liberdade. Portanto, buscam-se atualmente estratégias institucionais aptas a conter esse avanço. Por ser um dos aspectos mais significativos, a proteção do indivíduo no tocante ao tratamento conferido aos seus dados pessoais se localiza no cerne da questão.

Nesse sentido, o tratamento de dados deve considerar a identidade social e individual do usuário, bem como seu corpo físico e eletrônico, a fim de obter meios de proteção adequados. No contexto da internet, necessário se faz equilibrar o princípio da liberdade de acesso com o princípio da dignidade da pessoa humana, princípio basilar do ordenamento jurídico brasileiro, como expresso no artigo 1º da CRFB/88:^{106 107}

105 BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 15.

106 BAIÃO, Kelly; GONÇALVES, Kalline. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*, a. 3. n. 2. 2014. p. 2. Disponível

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado democrático de direito e tem como fundamentos:

III – a dignidade da pessoa humana;

Princípio fundamental do ordenamento, a dignidade confere unidade ao mesmo. É responsável por conferir ao homem o direito de ser tratado como um fim em si mesmo, não como um meio que se submeteria a vontade dos demais. Portanto, como valor universal e incondicional, rege toda e qualquer ação. Nesse sentido, demonstra-se *anti-humana* condição que legitime discriminações ou reduções das pessoas inseridas na nova sociedade da informação.

Da mesma forma, atenta contra a dignidade tudo o que limita a pessoa à condição de objeto. Segundo Maria Celina Bodin de Moraes, “as coisas têm preço; as pessoas, dignidade”¹⁰⁸, posto que o homem em tempo algum poderá ser instrumentalizado para alcançar fins, quaisquer eles sejam.

A autonomia, antes entendida sob uma ótica individualista e patrimonialista, é reorientada para abranger aspectos existenciais de construção de identidades e de garantia da dignidade. Dessa forma, como a dignidade se encontra no centro do atual ordenamento constitucional brasileiro, as pessoas devem poder agir de maneira autônoma, abrangendo a pessoa em todas as suas emanações, como função promocional da Constituição Federal de 1988.

Assim sendo, a dignidade, enquanto parte essencial da pessoa humana, é também condição intrínseca da liberdade, posto que não existe dignidade sem autonomia.¹⁰⁹ Logo, a

em:< <http://civilistica.com/wp-content/uploads/2015/02/Bai%C3%A3o-e-Gon%C3%A7alves-civilistica.com-a.3.n.2.2014.pdf>>. Acesso em: 23 nov. 2018.

¹⁰⁷ BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em:< http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

¹⁰⁸ BODIN DE MORAES, Maria Celina. O princípio da dignidade da pessoa humana. In: Na medida da pessoa humana: estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010, p. 81.

¹⁰⁹ BAIÃO, Kelly; GONÇALVES, Kalline. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. Civilistica.com, a. 3. n. 2. 2014. p. 5-6. Disponível em:< <http://civilistica.com/wp-content/uploads/2015/02/Bai%C3%A3o-e-Gon%C3%A7alves-civilistica.com-a.3.n.2.2014.pdf>>. Acesso em: 23 nov. 2018.

autonomia é elemento ético da dignidade, devendo ser assegurada a possibilidade de autodeterminação do indivíduo, visto que este deve possuir o direito de desenvolver livremente sua personalidade, arbitrando os cursos de sua própria existência.¹¹⁰

2.3. Dados pessoais como direito de personalidade

Como já abordado anteriormente, a Sociedade da Informação, que se estrutura cada vez mais através da acumulação e circulação de informações, é também responsável por estabelecer novas situações de poder. Para tanto, torna-se cada vez mais difícil considerar o cidadão como um simples provedor de dados, visto que a ele deve caber minimamente um poder de controle sobre a conferência da exatidão das informações, sobre os sujeitos que as manipulam e sobre suas formas de utilização.¹¹¹

É de se notar uma ampliação progressiva, a partir das novas tecnologias, do conceito de esfera privada. Dessa forma, os dados pessoais hoje abrangem um núcleo muito maior de informações, em uma escalada de situações jurídicas relevantes, posto que incluem “o conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo”.¹¹² A privacidade, por fim, seria a forma de tutela dessas escolhas de vida contra eventuais abusos por parte das plataformas.

Os cidadãos, portanto, têm o direito de exercer um controle direto sobre seus próprios dados pessoais. Todavia, Rodotà atenta para a necessidade desse controle não se restringir a uma atuação individual, mas também coletiva, em razão de que “raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as

110 BAIÃO, Kelly; GONÇALVES, Kalline. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*, a. 3. n. 2. 2014. p. 6. Disponível em: < <http://civilistica.com/wp-content/uploads/2015/02/Bai%C3%A3o-e-Gon%C3%A7alves-civilistica.com-a.3.n.2.2014.pdf> >. Acesso em: 23 nov. 2018.

111 RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 36.

112 *Ibidem*, p. 92.

grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em controle”.¹¹³

Nesse contexto, faz-se necessária, além da articulação de diversas medidas de controle social, a definição de proteção de dados pessoais como novo direito da personalidade, no sentido de não subordinar este direito a nenhum outro, tendo em vista sua enorme relevância no atual contexto. Nesse sentido, não devemos nos ater a classificações que consideram o indivíduo como dono dos dados a seu respeito, visto que o direito à proteção de dados está estritamente vinculado à proteção da personalidade, e não a mero direito de propriedade.

Existem certos dados que, de forma alguma, poderiam vir a ser tratados com fins negociais, visto que acarretariam em imensa perda para a proteção da dignidade da pessoa humana. Como exemplo, temos os dados sensíveis, ou seja, aqueles que são especialmente propensos a ocasionar alguma espécie de discriminação ou estigmatização ao seu titular, tais como informações sobre convicções políticas e morais, bem como orientação e preferências sexuais.

Nesse sentido, a proteção de dados apresenta aplicação deveras relevante, visto que é expressão da própria liberdade e dignidade da pessoa. Os dados, portanto, não devem servir à objetificação do indivíduo, transformando-o em alvo de vigilância constante.¹¹⁴

Por fim, cumpre citar o “direito de não saber”, que pode também constituir fator essencial para a livre construção da personalidade. Rodotà, nesse sentido, ressalta o caráter negativo do direito de controle sobre nossas informações. Poderíamos, dessa forma, excluir de nossa esfera privada determinadas categorias de informações, que não seja de nosso interesse obter conhecimento sobre, como informações sobre nossas propensões genéticas a doenças específicas.¹¹⁵

113 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p 37.

114 Ibidem, p. 19.

115 Ibidem, p. 108-109.

O direito de controlar o fluxo de informações, portanto, existe tanto no tocante às informações que produzimos quanto às que recebemos como, por exemplo, a fim de evitar o recebimento de mensagens de e-mails e ligações indesejadas. Através deste empoderamento, então, poderíamos moldar de maneira ativa a construção de nossa própria esfera privada.

2.3.1. Princípios norteadores

Atualmente, a relevância da proteção conferida aos direitos da personalidade decorre do aumento exponencial dos meios de comunicação de massa, esses que produzem uma verdadeira publicização da vida privada. Nesse sentido, incrementou-se também a regulamentação jurídica dos fatores e conflitos decorrentes desta nova Sociedade da Informação.¹¹⁶

No que se refere aos direitos da personalidade em si, esses representam categoria aberta, posto que sempre surgem novas instâncias relativas à personalidade dos indivíduos ainda não contempladas pelo legislador e que merecem a devida tutela. Dessa forma, os direitos da personalidade não estão e nem poderiam estar inseridos em um rol taxativo, pois a personalidade da pessoa humana é um todo unitário reconhecido pelo ordenamento jurídico e que deve ser integralmente protegido.

É certo, portanto, que o conceito desse direito é elástico, apresentando um ilimitado número de hipóteses de aplicação. Sua tutela somente encontra limites quando entram em conflito com outros direitos de personalidade, em razão da proteção dos direitos da personalidade dever ser sempre a mais eficaz e ampla possível. De acordo com a Carta Magna¹¹⁷ brasileira, em seu inciso III, artigo 1º, a dignidade da pessoa humana é valor sobre o qual se funda a República, significando uma cláusula geral de tutela dos direitos da personalidade.

116 BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 2.

117 BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

Nesse sentido, o princípio da dignidade da pessoa humana promove a tutela dos direitos da personalidade em suas mais diversas ramificações e manifestações, não podendo ser restringido pelo legislador ordinário. A eventual colisão ou conflito de direito envolvendo a personalidade deve ser resolvida com base na técnica da ponderação, nenhum deles podendo sobrelevar-se ao outro. Segundo Maria Celina Bodin de Moraes, a solução para o caso concreto deve observar onde mais se realiza a dignidade da pessoa humana.¹¹⁸

De acordo com a autora, com a Constituição de 1988, pode-se observar marco histórico de suma importância no sentido de uma perspectiva constitucional voltada definitivamente a pessoa humana. Nesse sentido, as relações não patrimoniais passaram a conter relevância fática e interpretativa sobre as relações patrimoniais, como as derivadas de contratos e da propriedade.

Também o Código Civil de 2002¹¹⁹ representou a concretização desses princípios visto que englobou noções como as de abuso do direito, boa-fé, confiança e de função social do contrato e da propriedade.¹²⁰ No tocante aos direitos da personalidade, estes só estavam indiretamente previstos no Código Civil de 1916¹²¹. Os debates acerca desse tema se afluam apenas na década de 60, vindo a serem estipulados na Constituição Federal de 1988 alguns direitos da personalidade como cláusulas pétreas. Um capítulo próprio tratando dos direitos da personalidade só surge com o Código Civil de 2002 (vide Capítulo II – Dos direitos da personalidade).

Dessa forma, portanto, atualmente apresentamos proteção constitucional e civil dos direitos da personalidade, aplicando-se, no que couber, também às pessoas jurídicas. São previstas, também, duas formas de tutela, a tutela reparatória, que se dá através de

118 BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 5-6.

119 BRASIL. Código Civil, Lei 10.406, de 10 de janeiro de 2002. 1ª edição. São Paulo: Revista dos Tribunais, 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm >. Acesso em: 28 nov. 2018.

120 BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 3.

121 BRASIL. Código Civil dos Estados Unidos do Brasil, Lei 3.071, de 1º de janeiro de 1916. Diário Oficial da União, Rio de Janeiro, RJ, 5 de janeiro de 1916. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L3071.htm >. Acesso em: 29 nov. 2018.

indenização; e a tutela inibitória como, por exemplo, a imposição da remoção de determinado conteúdo.

Tratando especificamente dos dados pessoais e da atual problemática decorrente, principalmente, de seu tratamento automatizado, podemos perceber o risco de sua utilização indevida ou abusiva por parte de agentes ou plataformas. Por essa razão, a necessidade de se debater a proteção de dados pessoais hoje como direito fundamental é fruto deste se tratar de instrumento de proteção da própria dignidade da pessoa humana, princípio fundador de nosso ordenamento.

A instituição de mecanismos aptos a fornecer conhecimento e controle sobre os dados pessoais é expressão direta da proteção dos próprios direitos de personalidade dos indivíduos.¹²² De acordo com Pierre Catala, “quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade.”¹²³

Neste diapasão, o reconhecimento, pelo ordenamento brasileiro, da proteção de dados pessoais como direito autônomo e fundamental deriva justamente dos riscos que o tratamento automatizado traz para os direitos de personalidade. De acordo com Danilo Doneda, as garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, bem como a proteção da privacidade, representam o fundamento dessa acepção.¹²⁴

Já podemos encontrar referência ao caráter de direito fundamental dos dados pessoais na Declaração de Santa Cruz de La Sierra¹²⁵, produzido na XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, subscrita pelo Governo Brasileiro em 15 de novembro de 2003. No item 45 da Declaração supracitada, enfatiza-se o caráter de direito fundamental

122 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Joaçaba*, v. 12, n. 2, p. 91-108, 2011. p. 92-93.

123 CATALA, Pierre. “Ebauche d’une théorie juridique de l’information”, in: *Informatica e Diritto*, ano IX, jan-apr. 1983, p. 20.

124 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Joaçaba*, v. 12, n. 2, p. 91-108, 2011. p. 103.

125 SEGIB. XIII Cimeira Ibero-americana de chefes de estado e de governo. Declaração de Santa Cruz de la Sierra. 14-15 nov. 2003. Disponível em: <<https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>>. Acesso em: 26 nov. 2018.

conferido aos dados pessoais e destaca-se a importância de proteção da privacidade dos cidadãos.

Partindo para uma análise do tratamento da matéria em nossa legislação constitucional¹²⁶, encontram-se dois dispositivos; um presente no artigo 5º, X, que considera invioláveis a intimidade e a vida privada, e outro, no artigo 5º, XII, que coíbi a interceptação de comunicações telefônicas, telegráficas ou de dados. Para alguns autores, a distinção de tratamento conferido aos dados e a privacidade, por esses constarem em dispositivos distintos, significa que a privacidade deva ser entendida como direito fundamental e que, por outro lado, as informações pessoais só seriam protegidas no tocante à sua “comunicação”.

Acontece que a privacidade e as informações pessoais atualmente se encontram cada vez mais relacionadas, ao ponto de em alguns casos tornarem-se indissociáveis. Nesse sentido, leis que tratam da proteção de dados pessoais atualmente tendem a associar o caráter de direito fundamental à proteção de dados pessoais, em razão do risco da interpretação das legislações anteriores ocasionar uma certa complacência em relação ao tratamento das informações.¹²⁷ Dessa forma, o intérprete hoje deve reconhecer a íntima relação entre a privacidade e a proteção de dados e atentar para a necessidade de “integração da personalidade em sua acepção mais completa nas vicissitudes da Sociedade da Informação”.

128

Além disso, consta instrumento, verdadeiro remédio constitucional, no artigo 5º, LXXII da Constituição Federal de 1988¹²⁹; o *habeas data*. Este instrumento foi introduzido pela Constituição de 1988, representando verdadeiro de direito de acesso e de retificação dos dados pessoais. Inicialmente, tratava apenas da requisição de informações pessoais em poder

¹²⁶ BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

¹²⁷ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, v. 12, n. 2, p. 91-108, 2011. p. 105.

¹²⁸ Ibidem, p. 106.

¹²⁹ BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

de órgãos públicos, todavia, após a edição da Lei 9.507/97¹³⁰, ampliou-se para o setor privado e englobou a possibilidade de requisição de acesso e de retificação.

Entretanto, até hoje não encontra instrumentos hábeis a tornar essa tutela ágil e eficaz na proteção da personalidade. Segundo Doneda, “ela é, substancialmente, um instrumento que proporciona uma tutela completamente anacrônica e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação”.¹³¹ Também segundo Luís Roberto Barroso, “um remédio de valia, no fundo, essencialmente simbólica”¹³²

Por outro lado, a legislação infraconstitucional, mesmo antes da nova Lei Geral de Proteção de Dados¹³³, também apresentou dispositivos de tutela, com destaque para o Código de Defesa do Consumidor (Lei nº 8.078/90)¹³⁴, em seu artigo 43, que estabelece uma gama de direitos e garantias para o consumidor em relação às informações pessoais inseridas em bancos de dados ou cadastros:¹³⁵

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

¹³⁰ BRASIL. Lei 9.507, de 12 de novembro de 1997. Diário Oficial da União, Brasília, DF, de 13 de novembro de 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm >. Acesso em: 29 nov. 2018.

¹³¹ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Joaçaba, v. 12, n. 2, p. 91-108, 2011. p. 104.

¹³² BARROSO, Luís Roberto. Constituição da República Federativa do Brasil Anotada. 3a edição, amplamente revista e atualizada até a EC no 32/2001. São Paulo: Saraiva, 2001. p. 212.

¹³³ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 29 nov. 2018.

¹³⁴ BRASIL. Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990. Diário Oficial da União, Brasília, DF, 12 de setembro de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm >. Acesso em: 28 nov. 2018.

¹³⁵ DONEDA, op. cit., p. 103.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

2.4. Abuso por parte das plataformas

Como ilustra perfeitamente o romance *O Círculo*¹³⁶ de Dave Eggers, o caráter imaterial e abstrato da informação pode gerar formas menos perceptíveis de controle social, uma vez que acaba por estruturar práticas totalitárias de forma muito sutil. Rodotà atenta para o fato de que regimes totais podem se instalar sem que para isso seja necessária a realização de prisões ou de práticas de torturas, como apresentado, por outro lado, no romance *1984*¹³⁷ de Orwell.

Eis porque se torna fundamental compreender o poder das plataformas no sentido de formular meios de tutela que não se desvinculem de nossas sensibilidades sociais e de nossa capacidade de reação. Nesse sentido, as armas institucionais devem ser enriquecidas e constantemente repensadas, de forma a abarcar as transformações que se assomam.¹³⁸

Segundo Rodotà, uma primeira geração de leis sobre proteção de dados visava unicamente reprimir violações da intimidade individual que poderiam ser ocasionadas pela tecnologia. Apesar de ampliada, essa visão continua a exercer influente relevância na fase atual.¹³⁹

Todavia, para proteger de maneira mais completa a própria privacidade, requer-se um verdadeiro alargamento da lógica individualista e institucional desta primeira geração. Deve ser incetiva a integração entre controles individuais e coletivos, deixando por superada a lógica meramente proprietária. Dessa forma, exige-se esforço coletivo no sentido de integrar

¹³⁶ EGGERS, Dave. *O Círculo*. São Paulo. Companhia das Letras, 2014.

¹³⁷ ORWELL, George. 1984. São Paulo: Companhia das Letras, 2009.

¹³⁸ RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 58.

¹³⁹ *Ibidem*, p. 49.

estratégias capazes de regular a circulação de dados em seu conjunto, passando de uma expressão passiva da proteção de dados para uma positiva e dinâmica.¹⁴⁰

O autor italiano frisa constantemente a necessidade de forjar um caráter ativo e não meramente passivo nos grupos e indivíduos sujeitos ao controle de dados. Para além de defesas individuais passivas, o caminho seria o de armar institucionalmente os grupos e indivíduos através de meios dinâmicos de controle para, dessa forma, também ver surgir novas identidades coletivas.

2.4.1. Consentimento como ficção jurídica

“Em vez de perguntarmos por que a pessoa atrás do balcão nos pede número de telefone, identidade e código postal, ou questionarmos a exigência, pela máquina, de novos dados para que a transação se complete, presumimos que deve haver alguma razão que nos beneficiará”.¹⁴¹

Gary T. Marx, acadêmico de prestígio, especialmente no campo da ética na tecnologia, aponta-nos aspectos que deveriam ser observados ao se tratar de vigilância nas redes e, principalmente, indica caminhos a serem seguidos por parte de legislações que pretendem tratar do tema da privacidade hoje. Seu trabalho¹⁴², dessa forma, fornece verdadeiro manual para a criação de intervenções jurídicas e regulatórias no meio digital, estabelecendo princípios e dando absoluta prioridade a dignidade da pessoa humana e a prevenção de eventuais infortúnios.

Essas intervenções se tornam cada vez mais necessárias posto que é clara a situação de profunda disparidade entre os usuários de serviços informáticos e telemáticos em relação aos fornecedores de tais serviços. Como a discrepância é tamanha, não se pode falar atualmente em livre consentimento no que se refere às disposições de informações pessoais. O contratante é “vulnerável”, pois que não apresenta liberdade substancial ao dar seu consentimento.

140 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 50.

141 BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. p. 119.

142 MARX, Gary T. An ethics for the new surveillance. Information Society, v.14, n.3, 1998.

Na realidade, propagadas formas de controle individual sobre a disponibilização de nossos dados acabam por gerar unicamente a ampliação da legitimidade de atuação das plataformas. Ficam, dessa forma, claros os limites de um controle que se limita às nossas “escolhas” individuais, visto que, muitas das vezes, o único meio de ter acesso a determinado serviço se dá através do consentimento. Nesse sentido, faz-se necessário um fortalecimento de um poder geral de vigilância que seria de incumbência de órgãos criados especificamente para fins de proteção de dados pessoais.¹⁴³

Devido às facilidades fornecidas pelas novas tecnologias, a questão do consentimento foi alvo de diversas conjecturas. Podemos observar uma evolução do conceito, passando do *implied consent*, modelo de consentimento implícito que ignorava e simplificava diversos aspectos do consentimento, para o moderno *informed consent*. O *informed consent*, ou consentimento informado, pode ser encontrado em uma série de disposições, pois prescreve o modo como as informações devem ser fornecidas ao interessado “para que seu consentimento seja validamente expresso”.¹⁴⁴

Assim, o consentimento surge e se reforça como meio alternativo, tendo em vista as dificuldades em se estabelecer um completo sistema de autorizações e proibições pela lei, bem como pelo perigo de se deixar a matéria sem regulação alguma (*deregulation*).

Todavia, a falta de real liberdade de escolha ainda deve ser trazida ao debate, posto que não superada. Quando se condiciona a utilização de determinados serviços ao consentimento, é claramente perceptível a pressão e o poder que exercem os gestores das plataformas. Dessa forma, resta intacto seu poder ante a necessidade de acesso a determinada ferramenta.¹⁴⁵

Esse meio alternativo, entretanto, não pode ser renegado por conta da existência de limites intrínsecos ao livre consentimento. Devem ser rediscutidos e exigidos *standards*

143 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 60.

144 Ibidem, p. 75.

145 Ibidem, p. 76.

mínimos por parte dos provedores, objetivando-se a aproximação de uma real proteção dos direitos fundamentais em questão e a um efetivo controle sobre essas relações mercadológicas.

Além disso, têm-se também a proteção especial aos dados sensíveis, ou “núcleo duro da privacidade”¹⁴⁶, que seriam os dados sobre opiniões políticas, religião, raça, saúde, hábitos sexuais, etc. Ao se estipular uma caracterização específica para eles, busca-se protegê-los e evitar práticas discriminatórias através dos mesmos. Dessa forma, existiriam dados que não poderiam ser livremente negociados, mesmo que em caso de consentimento. A tendência, portanto, segundo Rodotà, seria a de atribuir maior importância aos contextos em que a utilização estaria inserida.¹⁴⁷

Nesse sentido, como o mercado da informação é marcado pelo desnível de poder entre os “contratantes”, faz-se necessária a criação de legislação ativa como estratégia institucional integrada. Esta constitui chave fundamental para que sejam estipuladas regras de mercado no âmbito tecnológico, representando também um avanço positivo na democratização da internet e no reforço do direito à autodeterminação informativa.

Utilizar o argumento de que seria extremamente custoso para as empresas e para a Administração Pública o respeito às normas de proteção de dados é de veras superficial, visto que são custos diretamente ligados às garantias constitucionalmente previstas. Dessa forma, é sim papel da legislação de dados o de estabelecer obrigações a cargo dos coletores de informações, passíveis inclusive de sanções pecuniárias.¹⁴⁸

Apesar de também haver um fluxo no sentido de autorregulamentação por parte das empresas, podemos observar, em diversos países, o fenômeno de surgimento de normas sobre

146 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 78.

147 Ibidem, p. 77.

148 Ibidem, p. 52-53.

proteção de dados que, segundo Rodotà, “tem ampliado extraordinariamente nos últimos anos o panorama dos instrumentos jurídicos disponíveis”¹⁴⁹.

Dessa forma, a proteção de dados tem se expandido em quantidade e qualidade ao redor do globo, como, por exemplo, com a inclusão do novo direito à autodeterminação informativa em nível constitucional, ao mesmo tempo em que se expandiu também em normas inferiores.

2.4.2. Comercialização de dados

Inicialmente, cumpri ressaltar que na Constituição de 1988¹⁵⁰, em seu artigo 199, parágrafo 4º, encontra-se disposição que veda todo tipo de comercialização relativa a órgãos, tecidos e substâncias humanas. Por outro lado, no tocante à privacidade ou às informações pessoais, a única proteção constitucional disponível é o *habeas data*, visando tanto os dados sensíveis quanto os dados pessoais em sua acepção mais ampla. Todavia, este instrumento se demonstra insuficiente pois se limita a permitir a retificação e não a disposição sobre os dados pessoais.¹⁵¹

Bauman compreende que as prateleiras do mercado, hoje, são preenchidas pelos próprios usuários, ao produzirem informações sobre si mesmos de forma incessante, comercializando-as. O autor conclui que, neste contexto, as pessoas são “(...) forçadas a se vender no mercado e procurando, para isso, a melhor oferta, são incitadas, instigadas ou obrigadas a promover uma *mercadoria* atraente e desejável; assim, fazem todo o possível, usando os melhores recursos à disposição, para aumentar o valor de mercado dos artigos que estão vendendo. Os produtos que elas são estimuladas a colocar no mercado, assim como promover e vender, são *elas próprias*”.¹⁵²

149 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 55.

¹⁵⁰ BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, Outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

151 BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010. p. 3.

152 BAUMAN, Zygmunt. Vigilância Líquida. Rio de Janeiro: Zahar, 2014. p. 37.

Prossegue explicando que “elas são, simultaneamente, *promotoras de produtos e os produtos que promovem*. São, ao mesmo tempo, a mercadoria e seus agentes de *marketing*, os artigos e seus vendedores itinerantes (...)”¹⁵³. Seguem, portanto, uma lógica perversa de comodificação¹⁵⁴ humana. Para que se possa acender socialmente ou ter acesso a determinadas ferramentas e aplicativos na internet, aceita-se a venda de parte de nosso *eu*, ou seja, nossos dados.¹⁵⁵

Em uma complexa interação de recebimento e processamento de dados, surgem novos e significativos contextos de utilização dos mesmos. Informações obtidas através do fornecimento de determinados serviços podem gerar novas informações, como, por exemplo, perfis de consumo, análises de preferência e dados estatísticos.¹⁵⁶

Essas “novas” informações podem vir a interessar novos sujeitos e, dessa forma, serem vendidas para estes. São, portanto, novas mercadorias. De acordo com Stefano Rodotà:

“Assim se torna possível não só um controle mais direto do comportamento dos usuários, como também a identificação precisa e atualizada de certos hábitos, inclinações, interesses, preferências. Daí decorre a possibilidade de uma série de usos secundários dos dados, na forma de “perfis” relacionados aos indivíduos, famílias, grupos. Trata-se de uma nova “mercadoria” cujo comércio pode determinar os tradicionais riscos para a privacidade: mas pode, sobretudo, modificar as relações entre fornecedores e consumidores de bens e serviços, reduzindo a autonomia destes últimos de tal forma que pode chegar a incidir sobre o modelo global de organização social e econômica.”¹⁵⁷

2.4.3. Uso de dados para reprodução de padrões discriminatórios

Em estudo sobre a ferramenta do *Big Data* e discriminação ocasionada pelos algoritmos, Cathy O’Neil na obra *Weapons of Math Destruction*¹⁵⁸, demonstra a possibilidade

153 BAUMAN, Zygmunt. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2014. p. 37.

154 Processo através do qual as instituições passam a ser definidas e organizadas em termos de produção, distribuição e consumo de mercadorias.

155 BAUMAN, op. cit., loc. cit.

156 RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 46.

157 Ibidem, p. 62.

158 O’NEIL, C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Denver: Crown, 2016.

destas novas tecnologias proporcionarem discriminações raciais e sociais em níveis alarmantes na sociedade de hoje. Os algoritmos seriam utilizados, além de outras formas, para captarem tendências dos usuários, de forma a criar perfis sobre os mesmos. Estes perfis determinariam a possibilidade do indivíduo ter ou não acesso a determinado serviço, como uma concessão de crédito.

A questão é que, no processo de formação de perfis por parte da máquina, são levados em consideração também outras informações como a região em que a pessoa mora, sua classe social ou sua raça. Nesse sentido, busca a autora atentar para os perigos de permitir que as máquinas tomem decisões com base nesses critérios pessoais, visto que apresentam claras pretensões discriminatórias se utilizados para determinar quem tem ou não direito a determinada coisa.

Ficaria muito mais fácil, portanto, permitir uma discriminação sistemática, com aparente neutralidade, por conta do uso da técnica. Nesse sentido, a autora demonstra que o efeito seria o oposto, proporcionando, com o tempo e com a crescente presença do *Big Data*, a ampliação da desigualdade e restrição da universalização do acesso que a internet teoricamente proporcionaria.

Stefano Rodotà entende que existem diversos riscos políticos ao registro desenfreado de dados pessoais da população. Um deles, e talvez o mais relevante, pode ser definido como a possibilidade de discriminação de determinados grupos ou indivíduos a partir da manipulação desses dados. Essa consequência atinge, sobretudo, as diferentes minorias e aqueles que pertencem às classes menos favorecidas economicamente.¹⁵⁹

Conclui Rodotà que, no tocante à revisão do processo de classificação das informações pessoais, “deveria ser garantido o máximo de opacidade às informações suscetíveis de

159 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 30.

originar práticas discriminatórias e o máximo de transparência àquelas que, referindo-se à esfera econômica dos sujeitos, concorrem para embasar decisões de relevância coletiva.”¹⁶⁰

O “núcleo duro” da privacidade, que antes se restringia à saúde ou aos hábitos sexuais, hoje abarca também outras categorias de informações, visto que se ampliou o leque de possibilidade de causar dano ao usuário através de práticas discriminatórias por meio dessas. Portanto, informações como opiniões políticas, raça e credo religioso merecem também especial atenção na categorização dos dados “sensíveis”.

Nesse sentido, busca-se restringir sua coleta por parte de determinados sujeitos, como os empregadores, e tornar ilegítimas certas formas de recolhimento de dados. Neste diapasão, reforça-se o reconhecimento do direito à autodeterminação informativa como direito fundamental do indivíduo. Este movimento representa verdadeira constitucionalização dos novos direitos no âmbito da Sociedade de Informação, que tendem a ganhar maior amplitude com o decorrer do tempo.¹⁶¹

Eis o motivo de se atentar para a dimensão coletiva de proteção de dados pessoais, visto que já podemos ver hoje uma série de ataques a determinados grupos sociais. Como exemplo, dados anônimos que não se vinculem diretamente aos indivíduos, mas ao grupo que pertencem, como minorias raciais ou linguísticas, também podem ser manipulados de maneira gravosa, ocasionando danos para esses grupos ou por conta de decisões políticas ou econômicas tomadas com base nesses dados.¹⁶²

Importante, pois, incentivar a cultura de um controle do processamento de dados por parte da coletividade, e não unicamente por parte de órgãos públicos especializados. É fundamental o empoderamento dos sujeitos face às intensas transformações que vivenciamos e que ameaçam violarem direitos fundamentais, caso não sejam devidamente combatidas.

160 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 35.

161 Ibidem, p. 96.

162 Ibidem, p. 32.

Para ilustrar o debate, podemos usar como exemplo os dados sensíveis vinculados à saúde do usuário. A proteção especial que recai sobre eles não se justifica unicamente pelo fato de serem fatos íntimos, mas, sobretudo, pelo alto risco que apresenta a sua manipulação com fins econômicos e discriminatórios.

Nossas informações genéticas, assim como dados acerca de doenças que possuímos, constituem nossa própria estrutura como pessoas, posto que não são modificáveis pela vontade própria do interessado. Dessa forma, Rodotà considera esses dados como “a parte mais dura do núcleo duro da privacidade”¹⁶³, em razão de sua propensão catastrófica em proporcionar modelos de “normalidade” genética que discriminariam indivíduos e grupos inteiros.

163 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 107.

3. MODELO BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS E O CONTEXTO DA LEI 13.709/18

Diante da necessidade de regulação que hoje está posta, faz-se mister refletir sobre as técnicas que podem vir a ser empregadas pela legislação e pela jurisdição brasileira, bem como sobre a influência de legislações estrangeiras nestas.

Stefano Rodotà, em sua obra *A Vida na Sociedade da Vigilância*¹⁶⁴, publicada no ano de 2001, já atentava para a necessidade de estruturação de um órgão de controle que completasse o sistema de proteção de dados. Esse seria responsável por exercer um controle geral e continuado, através de uma vigilância necessária sobre as plataformas.¹⁶⁵

Os órgãos de controle seriam verdadeiros: “cães de guarda da legalidade da ação de quem coleta, trata e faz circular informações (seja através do exercício de um poder de autorização, geral ou especial, seja através de uma ação de vigilância nesta área); organismos consultivos do setor público (e, eventualmente, do setor privado), também com a finalidade de facilitar práticas consensuais para a fixação das regras de circulação das informações; instituições de resolução e/ ou de atenuação de conflitos; organismos dotados de um poder normativo autônomo ou de um poder regulamentar de adaptação dos princípios fixados em lei”¹⁶⁶.

Além do mais, reforçou a necessidade de se estruturar paralelamente a vigilância eventual e fragmentada a ser exercida por indivíduos ou coletivos de forma difusa. Especificamente no tocante ao requerimento de dados não pessoais, como informações sobre o tratamento automático de dados, a legitimação também pode ser dada a sujeitos diferentes daqueles que foram diretamente atingidos.

A atuação dos sujeitos coletivos como sindicatos, associações para a tutela dos consumidores ou para a defesa de direitos civis, não deve necessariamente estar subordinada

¹⁶⁴ RODOTÀ, Stefano. *A vida na sociedade de vigilância. Privacidade hoje*. Rio de Janeiro: Renovar, 2008.

¹⁶⁵ *Ibidem*, p. 86.

¹⁶⁶ *Ibidem*, p. 87.

ao consentimento do ofendido, por tratar-se de interesse da coletividade. Dessa forma, através dos sujeitos coletivos, seriam proporcionadas condições reais de garantir um efetivo controle social, redistribuindo o poder entre os sujeitos da *internet*.¹⁶⁷

3.1. O Marco Civil da Internet: Lei 12.965/2014

O Marco Civil da Internet¹⁶⁸ surgiu da necessidade de regulação das relações e responsabilidades envolvendo a *internet*, sendo marco relevante e inovador no mundo jurídico. Segundo seu Artigo 1º, a Lei estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e determina diretrizes de atuação de entes federados na regulação da matéria. A definição de *internet* se encontra no Art. 5º, I, qual seja, “o sistema constituído de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes”.

Dentre os princípios que fundamentam a legislação ora em análise está a neutralidade da rede, a liberdade de expressão, o direito ao sigilo de informações, bem como a responsabilidade civil de provedores de internet. Nesse sentido, os princípios fundamentais da legislação podem ser elencados em três pilares, quais sejam, a liberdade de expressão, a privacidade e a neutralidade da rede.¹⁶⁹

Cumprido ressaltar que no Artigo 2º e no Artigo 3º, I, do Marco Civil¹⁷⁰, encontra-se expresso o princípio da liberdade de expressão, este que se apresenta em posição preferencial aos demais. Dessa forma, de acordo com jurisprudência majoritária do Supremo Tribunal

167 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 72-73.

168 BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

169 SANTOS, Thiago; DUARTE, Bruno. A responsabilidade civil dos provedores de aplicação de internet no tratamento de dados à luz da Lei nº 12.965/14 denominada o marco civil da internet. Revista de Direito da Faculdade Estácio do Pará. Belém, v. 5, n. 7. p. 82.

170 BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

Federal e do Superior Tribunal de Justiça, a liberdade de expressão tende a ser princípio preferencial na ponderação, todavia, cumpre salientar que esse posicionamento não é pacífico. É o que se extrai do Acórdão do STF na Reclamação 22328/ RJ:

“(…) 11. A Carta de 88 incorporou um sistema de proteção reforçado às liberdades de expressão, informação e imprensa, reconhecendo uma prioridade *prima facie* destas liberdades públicas na colisão com outros interesses juridicamente tutelados, inclusive com os direitos da personalidade. Assim, embora não haja hierarquia entre direitos fundamentais, tais liberdades possuem uma posição preferencial (*preferred position*), o que significa dizer que seu afastamento é excepcional, e o ônus argumentativo é de quem sustenta o direito oposto. Conseqüentemente, deve haver forte suspeição e necessidade de escrutínio rigoroso de todas as medidas restritivas de liberdade de expressão.”¹⁷¹

Dessa forma, com o Marco Civil da Internet¹⁷², foi dada ênfase às liberdades comunicativas e à segurança jurídica no âmbito da liberdade de expressão, estas que representam a base e fundamento da Lei. Todavia, também se deve garantir a proteção dos demais princípios elencados no Art. 3º. A proteção da privacidade, presente no inciso II do Artigo, engloba também o direito de controlar o tratamento dado aos dados pessoais.

Já no inciso III do Art. 3º, há previsão expressa de proteção aos dados pessoais, na forma da lei. Contudo, antes de 2018 ainda não existia uma lei de proteção de dados no Brasil que regulasse a matéria. Acontece que, apesar do Marco Civil tentar fornecer essa proteção às informações pessoais, ainda existiam diversos obstáculos a uma efetiva aplicabilidade dessa proteção. Com a publicação da Lei 13.709/18¹⁷³, portanto, foi dado passo importante para sua real efetividade, visto que passou a tratar especificamente da questão do tratamento de dados pessoais, tanto de forma manual quanto de maneira automatizada.

No Marco Civil, também, a questão do consentimento não foi devidamente estipulada, posto que os termos de uso das plataformas são irrelevantes para que se considere um efetivo

¹⁷¹ BRASIL. Supremo Tribunal Federal. Reclamação nº 22328-RJ. Primeira Turma. Relator: Ministro Roberto Barroso. Rio de Janeiro, julgado em 06.03.2018. Reclamante: Abril Comunicações S/A. Disponível em: <<http://portal.stf.jus.br/processos/downloadPeca.asp?id=314302526&ext=.pdf>>. Acesso em: 28 nov. 2018.

¹⁷² BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

¹⁷³ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

consentimento por parte dos usuários. Existia lacuna quanto aos requisitos necessários para que aquele fosse aferido no caso concreto, lacuna essa que recebeu maior profundidade e complementação com a publicação da nova Lei Geral de Proteção de Dados Pessoais (LGPD). Contudo, ainda não encontramos grandes especificidades em relação ao tema do consentimento mesmo na LGPD.

A maior problemática sempre se deu no tocante aos acessos, por parte das plataformas, a dados desnecessários ao seu funcionamento rotineiro. Da mesma forma, outra prática comum é a retenção dos mesmos por longos períodos de tempo e o compartilhamento das informações a outros aplicativos sem o nosso conhecimento ou consentimento. Mesmos nos casos em que haveria tal consentimento este era visto como mera ficção jurídica, posto que não era dada real opção de escolha ao usuário, que era impelido a aceitar as condições impostas pelas plataformas.

Por fim, no inciso VI do Art. 3º está presente a possibilidade de responsabilização dos agentes de acordo com as suas respectivas atividades. Especificamente quanto à responsabilização referente aos dados pessoais, esta poderá ser aferida nos casos de tratamento inapropriado dos mesmos. É certo que os direitos do titular devem ser resguardados, não podendo os provedores dispor dos dados à terceiros sem a devida autorização ou ordem judicial. Nesse sentido, podemos apreender que a não observância deste requisito ou dos demais especificados na legislação acarretaria na responsabilização do agente.¹⁷⁴

3.1.1. Dados pessoais no Marco Civil

No Artigo 7º, VII, do Marco Civil¹⁷⁵, temos que é assegurado ao usuário da internet o direito de não ter seus dados pessoais fornecidos a terceiros, inclusive registros de conexão e

174 SANTOS, Thiago; DUARTE, Bruno. A responsabilidade civil dos provedores de aplicação de internet no tratamento de dados à luz da Lei nº 12.965/14 denominada o marco civil da internet. Belém: Revista de Direito da Faculdade Estácio do Pará, v. 5. n. 7. p. 94.

175 BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

de acesso a aplicações de internet, salvo no caso de consentimento expresso, livre e informado, bem como nas hipóteses previstas em lei.

No mesmo artigo, em seu inciso VIII, é garantido o direito a obter informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, devendo também respeitar o princípio da finalidade, visto que se exige que o tratamento de dados seja legítimo e que esteja expresso nos contratos e termos de uso.

Em seguida, no inciso IX, é dada ênfase à necessidade das cláusulas contratuais de consentimento estarem destacadas das demais, a fim de que esse se dê de maneira expressa. Por fim, no inciso X, alterado recentemente pela Lei 13.709/18¹⁷⁶, o artigo traz o direito do usuário de obter a exclusão definitiva de seus dados pessoais caso assim o requeira, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória.

Já a Seção II da Lei 12.965/14¹⁷⁷ trata da proteção aos dados pessoais, registros e comunicações privadas. No Artigo 10 encontramos a previsão de que a guarda e disponibilização de dados pessoais devem atender à preservação da intimidade, vida privada, honra e imagem das pessoas que puderem ser afetadas pelo tratamento dos dados pessoais em questão. É ressalvada a obrigação do provedor de contribuir com o compartilhamento de dados pessoais de usuários mediante ordem judicial (Artigo 10, § 1º).

Também existe exceção no § 3º, posto que é permitida a requisição por parte de autoridades administrativas, quando estas tiverem competência, dos dados referentes a qualificação pessoal, filiação e endereço de usuários. Já no Artigo 11, frisa-se que quando houver coleta, armazenamento ou tratamento de dados pessoais, em território nacional, por provedores da *internet*, essas devem respeitar obrigatoriamente a legislação brasileira e os direitos à privacidade e à proteção de dados.

¹⁷⁶ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

¹⁷⁷ BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

Nesse sentido, os provedores de conexão e de aplicações da *internet* deverão prestar informações no sentido de corroborar o fato de que estejam respeitando a legislação brasileira especificada. No Artigo 12 encontramos elencadas as sanções cabíveis no caso de desrespeito ao estipulado nos Artigos 10 e 11 do Marco Civil da Internet¹⁷⁸. Essas sanções variam conforme a gravidade do fato, podendo ser mera advertência, multa pecuniária, suspensão ou proibição do exercício das atividades de armazenamento e tratamento de dados.

Por fim, no Artigo 16, também alterado recentemente pela Lei 13.709/18, encontra-se vedação a guarda de registros de acesso a outras aplicações da internet, por parte dos provedores de aplicações, sem o devido consentimento prévio do usuário. Da mesma forma, é vedada a guarda de dados pessoais que sejam excessivos no tocante à finalidade para a qual foi dado consentimento.

O Decreto 8.771/2016¹⁷⁹ veio para regulamentar o Marco Civil da Internet no que diz respeito, entre outras questões, à indicação de procedimentos para guarda e proteção de dados por parte dos provedores e ao estabelecimento de parâmetros para fiscalização e apuração de infrações. O Capítulo III do referido Decreto trata da proteção aos registros, dados pessoais e das comunicações privadas, sendo que, na Seção I, é abordado especificamente o caso de requisição de dados cadastrais (qualificação pessoal, endereço e filiação) por parte de autoridades administrativas.

Por outro lado, na Seção II, Artigos 13 ao 16 do Decreto 8.771, é abordada a questão dos padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas. No tocante ao armazenamento e tratamento de dados pessoais, os provedores devem observar diversas diretrizes sobre os parâmetros de segurança, entre eles, o estabelecimento de controle

¹⁷⁸ BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

¹⁷⁹ BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União, Brasília, DF, 11 de maio de 2016. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 28 nov. 2018.

preciso sobre quem tem acesso aos dados e o uso de técnicas que garantam a inviolabilidade das informações pessoais, como a técnica da encriptação.

Da mesma forma, os provedores devem reter o mínimo de dados possível, devendo ser excluídos tão logo se atinga a finalidade ou o prazo determinado por obrigação legal. Há, ainda, no Decreto, a definição de dado pessoal como sendo o dado relacionado a pessoa natural identificada ou identificável, bem como a definição de seu tratamento, como toda operação realizada com esses dados pessoais (Artigo 14).

3.2. A inspiração da Lei 13.709/18 na Regulação Europeia (RGPD)

Com a Diretiva Europeia nº 95/46/CE¹⁸⁰ de 24 de outubro de 1995, que trata da proteção às pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses, foi imposto que diversos países elaborassem princípios e regras para a proteção dos dados pessoais, limitando a atuação dos órgãos e entidades na coleta de dados.

O objetivo da Diretiva supracitada era o de oferecer aos cidadãos europeus um elevado nível de tutela dos seus dados pessoais. Em 1995, portanto, já havia a obrigatoriedade aos países-membros de que instituíssem uma autoridade central responsável pela fiscalização dessas proteções, dando real efetividade aos princípios estipulados.

Rodotà ressalta que “o resultado pode parecer paradoxal: na região que a importou, a Europa, a privacidade tem hoje um estatuto jurídico mais forte do que naquele de sua pátria de origem, os Estados Unidos”.¹⁸¹ Todavia, este resultado se deu por conta da junção entre a tradição americana de defesa da privacidade com a tradição europeia de tutela dos direitos do homem.¹⁸²

¹⁸⁰ EUROPA. Diretiva 95/46/CE, de 24 de outubro de 1995. Jornal Oficial da União Europeia, L281, de 23 de novembro de 1995. p. 31-50. Disponível em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>>. Acesso em: 29 nov. 2018.

¹⁸¹ RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 145.

¹⁸² Ibidem, p. 149.

Nesse contexto, consta na Carta dos Direitos Fundamentais da União Europeia¹⁸³, proclamada em 7 de dezembro de 2000, bem como no Tratado Constitucional para a União Europeia de 2004¹⁸⁴, que estabeleceu uma Constituição para a Europa, o reconhecimento de dois importantes direitos autônomos. Em seu artigo 7º e 8º, a Carta afirma que:

“Artigo 7º

Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8º

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

Dessa forma, por um lado temos o direito ao respeito à vida privada e familiar, que representa conteúdo individualista e a lógica de exclusão abordada anteriormente e, por outro lado, a proteção de dados pessoais, que fixa uma lógica dinâmica de intervenção positiva. De toda forma, o direito à autodeterminação informativa é ponto de partida para essas diretrizes que possibilitaram o poder de controle sobre nossas informações, frisando-se pelo consentimento e pelo direito de acesso.

Cumprе ressaltar que a Carta de Direitos Fundamentais¹⁸⁵ apresenta como princípio norteador a proteção da dignidade da pessoa humana, pois já em seu artigo 1º apresenta a dignidade da pessoa humana como inviolável, devendo ser respeitada e protegida. A partir disso, a proteção do corpo eletrônico abordada no Artigo 8º da Carta contribui para uma “constitucionalização da pessoa”, colaborando para a formação dos aspectos da cidadania do novo milênio.

¹⁸³ EUROPA. Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000. Jornal Oficial das Comunidades Europeias, C 364/1, de 18 de dezembro de 2000. Disponível em:< http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 29 nov. 2018.

¹⁸⁴ EUROPA. Tratado que estabelece uma Constituição para a Europa, de 29 de outubro de 2004. Jornal Oficial da União Europeia, C 310, 47º ano, de 16 de dezembro de 2004. Disponível em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:C:2004:310:TOC>>. Acesso em: 29 nov. 2018.

¹⁸⁵ EUROPA. Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000. Jornal Oficial das Comunidades Europeias, C 364/1, de 18 de dezembro de 2000. Disponível em:< http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 29 nov. 2018.

Em seu artigo 51, frisa-se que qualquer limitação ao exercício dos direitos e liberdades estabelecidos na Carta deve necessariamente ser revista por lei, ao mesmo tempo em que também deve ser respeitada a essência desses direitos e liberdades estipulados em seus artigos.

A legislação europeia também foi cirúrgica ao apontar que não bastava o controle difuso por parte dos usuários, em razão de claros desníveis de poder existentes, dessa forma, abriu-se caminho também para o princípio da finalidade, que será abordado mais adiante, e para os casos de indisponibilidade de dados, casos em que nem mesmo o interessado pode ceder suas informações através do consentimento. Todavia, cumpre ressaltar que a criação de autoridades protetoras não se restringiu a uma visão paternalista, mas sim como forma de tornar efetiva a tutela dos direitos.¹⁸⁶

Dessa forma, anos antes da elaboração da GDPR (Regulamento Geral sobre a Proteção de Dados 2016/679), que veio a revogar a Diretiva 95/46/CE, a proteção de dados pessoais já estava se consolidando no ambiente europeu, tendo como base, além do princípio da dignidade humana, os princípios da finalidade, pertinência, proporcionalidade, simplificação, harmonização e necessidade.

De acordo com a atual legislação europeia sobre a proteção de dados (GDPR)¹⁸⁷, em seu Artigo 4º, os dados pessoais seriam o conjunto de informações relativas a uma pessoa viva, identificada ou identificável, também se inserindo no conceito as informações que podem levar a identificação de determinadas pessoas. Dessa forma, mesmo os dados colhidos de maneira descaracterizada, ou seja, de maneira teoricamente anônima, podem vir a ser abrangidos pela GDPR se for constatado que estes podem ser utilizados para reidentificar uma pessoa.

186 RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 149.

187 EUROPA. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L119, 59º ano, de 4 de maio de 2016. Disponível em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>. Acesso em: 29 nov. 2018.

Por outro lado, os dados definitivamente anônimos, em que a pessoa não seja ou deixe de ser identificável, não são considerados dados pessoais pela lei. Todavia, cumpre ressaltar que esse processo de anonimização deve ser irreversível. Para exemplificar o que seriam os dados pessoais, podemos elencar o nome e apelido, o endereço de uma residência, um endereço de correio eletrônico pessoal, um endereço IP, testemunhos de conexão (*cookies*) ou até mesmo dados de determinado paciente retido por um hospital. De outro modo, o número de registro de empresa ou dados anonimizados não são considerados pessoais.

Insta salientar que, em se tratando de dados pessoais, estes serão protegidos independentemente da forma como foram tratados ou armazenados, se de maneira tecnológica ou manual, desde que sejam organizados de acordo com critérios pré-definidos. Em ambos os modos de tratamento e armazenamento, esses dados pessoais estarão sujeitos às normas de proteção estipuladas na legislação europeia.¹⁸⁸

Importante destacar que os dados são recursos praticamente infinitos, podendo vir a ser utilizados a qualquer tempo por diferentes agentes. O direito da proteção de dados pessoais representa área extensa e completamente nova do direito, em que o Direito Digital é apenas um de seus componentes. A proteção de dados se aplica a qualquer relação em que haja coleta de dados, não só representando restrições às empresas e provedores da internet.

Nesse sentido, a criação do GDPR se deu a partir de uma perspectiva de abrangência horizontal da legislação, ou seja, aplicando-se a empresas de diversas áreas que tenham contato com dados pessoais por qualquer que seja o meio, como formulários preenchidos em salões de beleza ou academias de musculação. Também apresenta abrangência extraterritorial, inserindo-se mesmo fora da União Europeia, sendo ainda aplicáveis penalidades e multas.

Dessa forma, a proteção de dados se encontra cada vez mais próxima de direito fundamental e de um viés de proteção de direitos humanos. Este direito engloba saber como seus dados são tratados e quem tem acesso aos mesmos. Insta salientar que os princípios que

188 EUROPA. Comissão Europeia. O que são dados pessoais. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 26 nov. 2018.

regem a proteção de dados pessoais estão elencados no Artigo 5 da legislação europeia¹⁸⁹ e são, dentre eles, a licitude, lealdade, transparência e a limitação das finalidades a que o tratamento se destina, bem como a garantia de exatidão e de confidencialidade das informações.

Em se tratando da licitude do tratamento, o Artigo 6 do GDPR afirma que o tratamento só será lícito quando for dado consentimento para aquela finalidade específica, quando for necessário para execução de um contrato ou de diligências pré-contratuais, para cumprimento de obrigação jurídica, para defesa de interesses vitais, quando necessário ao interesse público ou quando se tratar de interesses legítimos que o justifique, ressalvados os casos em que prevalece o interesse do titular, especialmente quando se tratar de criança.¹⁹⁰

De acordo com o GDPR, para termos o consentimento, precisa-se de uma clara afirmativa nesse sentido, também que os dados sejam oferecidos de maneira gratuita e livre, constituindo um consentimento específico, informado e não ambíguo. Outro requisito presente na legislação seria de que esse seja documentado e que a outorga seja explícita, não podendo ser fruto de cláusulas *escondidas* (ou “*easily withdrawn*”). Portanto, trata-se de um *informed consent*, já abordado anteriormente.

Segundo os princípios do GDPR, existem algumas regras que devem ser seguidas pela empresa no tocante à coleta de dados pessoais. Os deveres se resumem na notificação do consumidor e no fato de dever ser devidamente explicado o propósito da coleta de dados e o modo como serão processados, bem como a necessidade das informações serem guardadas e coletadas de modo seguro e a garantia do usuário poder ter acesso constante à sua base de dados pessoal.

¹⁸⁹ EUROPA. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L119, 59º ano, de 4 de maio de 2016. Disponível em: < <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>. Acesso em: 29 nov. 2018.

¹⁹⁰ GALVÃO E SILVA ADVOCACIA. Lei GDPR em português. Galvão & Silva Advocacia, 19.07.2018. Disponível em: <https://www.galvaoesilva.com/lei-gdpr-em-portugues/>. Acesso em: 26 nov. 2018.

Por outro lado, os direitos do sujeito de dados presentes no Capítulo III do GDPR são os de ser informado adequadamente sobre o tratamento de dados; de obter transparência nas informações e comunicações; de poder solicitar que seus dados sejam retificados em caso de erro, bem como que sejam definitivamente apagados; o direito de portabilidade de dados, ou seja, de transmitir os mesmos a outro responsável e o direito de se opor ao tratamento automatizado de dados quando implique em formação de perfis ou tomada de decisões.

Nessa lógica, pelo fato de existir previsão quanto ao apagamento de dados, resta clara e expressa a possibilidade do direito ao esquecimento na legislação europeia, o que não se encontra na legislação brasileira atual. No Artigo 17 do GDPR está expresso o direito a ser esquecido, visto que o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, quando se aplique um dos motivos elencados pela Lei, como no caso do fim da finalidade ou do consentimento aferido.

191

Dentre as obrigações das organizações públicas e privadas está a necessidade de indicação do *Data Protection Officer* (DPO), ou seja, de contratação de pessoas por parte das empresas que seriam as responsáveis diretas por presar pelo cumprimento das obrigações e garantias previstas no GDPR. Portanto, o DPO é a pessoa que servirá como canal de comunicação entre os titulares dos dados pessoais e os órgãos reguladores, supervisionando todas as práticas de tratamento de dados dentro da empresa.¹⁹² Na LGPD¹⁹³ brasileira essa pessoa é denominada de encarregado, figura que será aprofundada posteriormente.

Além dessa figura, há previsão de que cada país fomente a estruturação de uma autoridade supervisora competente, ou seja, as Autoridades de Proteção de Dados (DPA). Tais

¹⁹¹ GALVÃO E SILVA ADVOCACIA. Lei GDPR em português. Galvão & Silva Advocacia, 19.07.2018. Disponível em: <https://www.galvaosilva.com/lei-gdpr-em-portugues/>. Acesso em: 26 nov. 2018.

¹⁹² BIONI, Bruno R.; MONTEIRO, Renato L. O papel do Data Protection Officer. Jota, 04.12.2017. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Acesso em: 26 nov. 2018.

¹⁹³ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

autoridades seriam responsáveis por homogeneizar os procedimentos de proteção de dados e de controle do tratamento dado aos mesmos, bem como por fiscalizar e aplicar sanções quando cabíveis.¹⁹⁴ Todavia, no Brasil, essa previsão foi objeto de veto pelo Presidente Michel Temer, o qual será tratado mais adiante.

Assim, a Lei de Proteção de Dados da União Europeia (GDPR), que entrou em vigor no dia 25 de maio de 2018, foi o balizador para que tenhamos, hoje, no Brasil, uma lei de proteção de dados pessoais. A publicação da Lei Geral de Proteção de Dados no Brasil (Lei 13.709/2018) é componente essencial na elaboração de estratégias de tutela de privacidade no país, visto que as legislações até então em vigor não foram suficientes para gerar uma proteção adequada aos dados pessoais.

Nesse sentido, Rodotà nos aponta direcionamentos possíveis para as legislações de proteção de dados no mundo, como um reforço do “direito de oposição” a determinadas formas de coleta e de circulação de dados; a possibilidade de atuações individuais tanto quanto coletivas neste sentido; a defesa do “direito de não saber” já tratado anteriormente; a observância da concretização do princípio da finalidade, este que condiciona a legitimidade do recolhimento de dados à prévia comunicação do interessado sobre como serão processadas essas informações; bem como especial interesse aos dados sensíveis, em que a única finalidade admissível seria o interesse da pessoa em questão.¹⁹⁵

Essa legislação, afinal, deve ser acompanhada de severas sanções civis e penais em caso de descumprimento de seus pressupostos. No entanto, apesar do modelo europeu apresentar severas penas; a LGPD brasileira ainda não cumpriu tal requisito elencado por Rodotà. No tocante às infrações, pode-se destacar que as multas e penalidades impostas pelo GDPR são muito mais severas que as constantes na lei brasileira.

¹⁹⁴ LEMOS, Ronaldo. et. al. GDPR: A nova legislação de proteção de dados pessoais da Europa. Jota, 25.05.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Acesso em: 26 nov. 2018.

¹⁹⁵ RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 134.

Como exemplo, de acordo com a legislação europeia, uma infração grave pode custar vinte milhões de euros ou 4% do volume de negócio global da empresa. Já a LGPD brasileira a infração somente pode alcançar a cifra de cinquenta milhões de reais ou até o limite de 2% do faturamento total do ano anterior.

3.3. Principais pontos da Lei 13.709/18 no tocante à privacidade

A Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/18)¹⁹⁶, foi publicada no dia 15 de agosto de 2018 e entrará em vigor no dia 16 de fevereiro de 2020. Este período de quase dois anos foi estipulado com o fim de proporcionar o tempo adequado de adaptação, principalmente das empresas e plataformas, ao novo cenário de controle posto.

Cumprе salientar que a necessidade de proteger a privacidade não nasceu com a *internet*. No próprio Código Civil de 1916¹⁹⁷ já era apresentada como questão relevante principalmente no âmbito do direito de vizinhança, entre outros temas. Todavia, o que temos hoje é um aumento da preocupação com a privacidade com o advento da *internet*.

Dessa forma, aumentou-se a vulnerabilidade e hipossuficiência técnica do usuário no contexto do ciberespaço. Os provedores e plataformas se apresentam em posição de superioridade na *internet*, bem como em posição de verdadeiros agentes de controle e de vigilância dos usuários. Por conta disso, fala-se em uma proteção voltada ao usuário, este mais suscetível à atuação de diversos fatores capazes de violarem seus direitos fundamentais, como o direito à privacidade.

¹⁹⁶ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

¹⁹⁷ BRASIL. Código Civil dos Estados Unidos do Brasil, Lei 3.071, de 1º de janeiro de 1916. Diário Oficial da União, Rio de Janeiro, RJ, 5 de janeiro de 1916. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/L3071.htm>. Acesso em: 29 nov. 2018.

Como exemplo, casos de vazamentos de dados por parte de plataformas, como ocorrido recentemente com a *Netflix*, *LinkedIn* e *YouPorn*¹⁹⁸, tornam-se cada vez mais comuns na mídia, podendo apresentar consequências nefastas para um usuário ou grupo específico que delas se utiliza e confia suas informações.

Nesse sentido, torna-se cada vez mais relevante o debate acerca da proteção de dados pessoais em um cenário de crescentes violações da privacidade no espaço virtual e fora dele. Logo em seu artigo 1º, a Lei 13.709 ressalta essa característica do tratamento dos dados pessoais, visto que protege tanto o espaço *online* como o mundo *offline*. Também de acordo com o artigo citado, o objetivo da Lei é de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Nessa lógica, alguns dos principais fundamentos da LGDP são o direito à autodeterminação informativa (Art. 2º, II), entendido nesse contexto como a possibilidade de controle sobre o conteúdo dos dados pessoais e sobre o que deles é feito; e a proteção da privacidade (Art. 2º, I).

A proteção conferida pela Lei tem como destinatário o titular de dados pessoais, ou seja, aquele a quem se referem os dados pessoais objeto de tratamento, passando a apresentar, com a vigência da Lei, maiores garantias no tocante às suas informações (Art. 5º, V). Também fica estendida a tutela a todas as operações realizadas com os respectivos dados.

No que se refere ao âmbito de aplicação da Lei, o Artigo 3º da Lei nº 13.709 e o artigo 11º do Marco Civil da Internet (Lei 12.965)¹⁹⁹, definem que a legislação será aplicável quando o tratamento de dados se der no território nacional, se a atividade de tratamento tiver por objetivo oferta ou fornecimento de bens ou serviços para brasileiros, se tiver relação com dados de indivíduos localizados no Brasil ou se os dados forem coletados no Brasil.

¹⁹⁸ ZOGBI, Paula. Netflix, LinkedIn e YouPorn têm vazamento de 1,4 bilhão de dados sigilosos. InfoMoney, 12.12.2017. Disponível em: <<https://www.infomoney.com.br/minhas-financas/gadgets/noticia/7136758/netflix-linkedin-youporn-tem-vazamento-bilhao-dados-sigilosos>>. Acesso em: 26 nov. 2018.

¹⁹⁹ BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

Já o Artigo 4º da LGPD²⁰⁰ trata do âmbito de exclusão da legislação, isto é, situações em que a Lei não se aplica ao tratamento de dados pessoais. Como exemplo, a lei não se aplica quando não há fins econômicos no tratamento de dados realizado por pessoa natural ou quando se trate de fins exclusivamente jornalísticos, artísticos ou acadêmicos.

Também não se aplica quando realizado com fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou repressão de infrações, bem como nos casos de dados pessoais provenientes de fora do território nacional, desde que não compartilhados com agentes brasileiros ou objeto de transferência internacional, e desde que o país de proveniência proporcione grau de proteção adequado.

De acordo com o Artigo 5º da LGPD, os dados pessoais são definidos como informações relacionadas a pessoa natural identificada ou identificável como, por exemplo, através de seu IP²⁰¹ (*internet protocol*). Já os dados pessoais sensíveis seriam os dados relacionados a questões de saúde, vida sexual, raça, etnia, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados genéticos ou biométricos.

Os dados sensíveis apresentam essa denominação pois estão mais suscetíveis a serem utilizados para reprodução de padrões discriminatórios. Como exemplo de utilização histórica e catastrófica dos mesmos, há provas de utilização da tecnologia da empresa norte-americana IBM nos campos de concentração nazistas. Essa empresa facilitou a manipulação de dados dos censos populacionais e, por conseguinte, a identificação e a seleção daqueles perseguidos pelo Terceiro Reich, permitindo o controle massivo do processo de extermínio.²⁰²

²⁰⁰ BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

²⁰¹ Um número que identifica um dispositivo em uma rede (um computador, impressora, roteador, etc.).

²⁰² BLACK, Edwin. IBM e o Holocausto. 3. ed. São Paulo: Campus, 2006.

Já os dados anonimizados, aqueles que não são rastreáveis ou identificáveis, considerando os meios técnicos disponíveis no momento, não estariam inseridos no conceito de dado pessoal trazido pela legislação. Dessa forma, as empresas teriam maior liberdade para seu tratamento.

Todavia, de acordo com a Teoria do Mosaico, o fato de se tratarem de dados anonimizados não é garantia de proteção, visto que posso chegar a pessoa específica se reunir esses dados em um grupo. Essa teoria trata dos dados que, a priori, não seriam abrangidos pela proteção da privacidade, porém que em contato com outros dados anonimizados poderiam tornar plenamente transparente aquele indivíduo.²⁰³

Outro ponto importante da Lei nº 13.709 é o fato de poder ser dividida em partes que ora dizem respeito ao titular, ora ao controlador ou ao operador de dados pessoais; estes últimos representando os agentes de tratamento. O controlador é a pessoa a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI), já o operador é a pessoa que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII). Ambos os agentes são juridicamente responsáveis pela segurança e privacidade dos dados.²⁰⁴

Para além destes agentes, aponta-se a necessidade de indicação do encarregado, todavia, este representa a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional, acerca de qualquer informação relevante sobre o tratamento de dados (Art. 5º, VIII).

O consentimento, de acordo com a LGPD, é requisito obrigatório para que haja a coleta de dados pessoais (Art. 7º, I). Neste diapasão, segundo o Art. 5º, XII, o consentimento é a manifestação livre, inequívoca e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. De acordo com o Art. 8º, caput, o

203 MAIA, Luciano Soares. A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. In: CONSELHO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM DIREITO. Anais do XVI Congresso Nacional do Conpedi. Florianópolis: Fundação Boiteux, 2008. p. 458.

204 PINHEIRO, Patricia Peck. Tabela comparativa. Consultor Jurídico, 10.07.2018. Disponível em: <<https://www.conjur.com.br/dl/tabela-comparativa-pl-protacao-dados.pdf>>. Acesso em: 26 nov. 2018.

consentimento deverá se dar por escrito ou por outro meio que explicita a manifestação de vontade do titular.

Portanto, o consentimento deve se dar de forma específica e detalhada, devendo os agentes apresentarem cláusulas destacadas no caso do consentimento escrito. Essas cláusulas reforçam o consentimento do titular sobre determinado tratamento, visto que se encontram separadas das demais cláusulas contratuais. Cumpre frisar que o consentimento pode ser revogado a qualquer momento ou declarado nulo caso haja algum vício. Todavia, esses termos ainda se encontram de maneira muito abstrata na legislação brasileira, necessitando de futuras regulações da matéria para melhor aplicação ao caso concreto.

Da mesma forma, a lei limita o tratamento da informação, devendo respeitar a boa-fé e uma série de outros princípios elencados no Artigo 6º. Dentre eles, o da finalidade, que significa a exigência do tratamento se dar de modo legítimo e desde que informado de maneira adequada ao titular. Nesse sentido, os agentes devem apresentar uma finalidade certa e justificável para o tratamento, de modo que o dado seja utilizado somente para tal finalidade²⁰⁵.

Os demais princípios atentam para a necessidade do tratamento ser adequado de acordo com o contexto em que está inserido, não promover nenhum tipo de discriminação ilícita ou abusiva, se dar de forma transparente para o titular, bem como a adoção de medidas que visem a proteger os dados pessoais de acessos não autorizados ou de situações acidentais ou ilícitas.

Já no Artigo 11º da LGPD estão presentes as hipóteses de tratamento dos dados pessoais sensíveis. Nesses casos, o tratamento só se dará se consentido pelo titular. Todavia, a lei elenca sete hipóteses em que não é necessário tal consentimento. Dentre eles, nos casos de cumprimento de obrigação legal ou regulatória; quando necessário para execução de políticas públicas por parte da Administração; quando necessário a órgão de pesquisa; para o exercício regular de direitos; para proteção da vida ou de incolumidade física; para a tutela da vida em

205 PINHEIRO, Patricia Peck. Tabela comparativa. Consultor Jurídico, 10.07.2018. Disponível em: <<https://www.conjur.com.br/dl/tabela-comparativa-pl-protacao-dados.pdf>>. Acesso em: 26 nov. 2018.

procedimentos realizados por profissionais ou quando necessário para garantir a segurança do titular nos procedimentos de cadastro em sistemas eletrônicos (Art. 11, II).

Em seguida, na Seção III da LGPD, são abordados os dados de crianças e adolescentes. Deve-se buscar sempre o melhor interesse da criança e do adolescente, sendo necessário que o consentimento se dê de maneira específica e que conste o consentimento de um dos pais ou do responsável legal. Para averiguar esse consentimento, faz-se mister um procedimento de verificação por parte do controlador, visto que pode ter sido a própria criança a fornecer o consentimento (Art. 14, § 5º).

Importante frisar também os direitos do titular, estes que se encontram nos Artigos 17 ao 22 da LGPD. Inicialmente, é dada ênfase aos direitos fundamentais de liberdade, intimidade e de privacidade. Mediante requisição, o titular tem direito de obter acesso aos seus dados pessoais; de corrigi-los quando incompletos, desatualizados ou inexatos; de eliminar dados desnecessários; de obter a portabilidade de dados a outro fornecedor do produto ou serviço; de ter conhecimento de todas as entidades públicas e privadas que têm acesso compartilhado aos seus dados; bem como o direito à revogação do consentimento.

Dessa forma, podemos apreender o direito de informação, o direito de retificação e de revisão dos dados pessoais, assim como a necessidade de se manterem atualizados. Importante previsão se encontra expressa no artigo 20 da LGPD, em que é garantido ao titular o direito de solicitar revisão nos casos de discriminação prejudicial ocasionada unicamente pelo tratamento automatizado de dados. Dessa forma, decisões pautadas por algoritmos, com base em dados pessoais, formadoras de perfis dos usuários, podem ser revistas.

Os critérios e procedimentos a serem utilizados pelos algoritmos devem sempre ser claros para o titular, quando solicitado esclarecimento. Nesse sentido, o tratamento de dados pessoais referentes a exercício regular de direito não pode ser utilizado em prejuízo ao titular. Por fim, no Art. 22 há previsão de que a defesa em juízo desses direitos possa ser realizada individual ou coletivamente mediante instrumento adequado, podendo o *habeas data* se enquadrar como um desses instrumentos.

Quanto ao direito de exclusão, é garantida ao usuário a possibilidade de alterar ou excluir dado pessoal a qualquer tempo, com exceção das hipóteses previstas em lei. Por outro lado, as informações devem ser eliminadas caso termine o tratamento de dados, seja porque foi revogado seu consentimento ou porque o tratamento já cumpriu sua finalidade, conforme estipulado nos Artigos 15, 16 e 18, II, III, IV e VI da LGPD.

No tocante à responsabilidade civil do controlador ou operador que causar dado patrimonial, moral, individual ou coletivo no decorrer do tratamento de dados, o Artigo 42 da LGPD determina que aqueles são obrigados a reparar o ofendido. Em determinados casos, cumpre frisar que essa responsabilidade pode ser solidária entre ambos. A responsabilidade civil, a priori, seria objetiva, visto que não se fala explicitamente da necessidade de culpa na lei.

Já em relação a segurança e ao sigilo de dados, encontramos disposições nos Artigos 46 ao Artigo 49. As organizações têm o dever de aplicar medidas técnicas ou administrativas de prevenção e de proteção à segurança dos dados que possui em seus sistemas. Nos eventos comuns de vazamentos de dados ainda resta dúvida sobre em que casos seria possível a responsabilização civil das plataformas, todavia, é obrigatória a notificação imediata das autoridades para que sejam tomadas as providências cabíveis.

De todo modo, essa questão ainda será objeto de discussão por parte do Judiciário, visto que ainda não sabemos se essa obrigação de segurança prevista na legislação seria meramente uma obrigação de meio ou se seria uma obrigação de resultado. Uma eventual obrigação de resultado poderia vir a ser deveras onerosa para as plataformas, em razão de que não seja cabível que a segurança seja ilimitadamente protegida. Existiriam investidas externas que não poderiam ser previstas ou remediadas por parte das plataformas.

No Artigo 50 da LGPD, bem como no Artigo 25 do GDPR²⁰⁶, existe previsão de criação de procedimentos de boa prática e de governança por parte dos controladores e operadores.

²⁰⁶ EUROPA. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L119, 59º ano, de

Estes poderão formular regras que estabeleçam, entre outros aspectos do tratamento de dados pessoais, as condições de organização, normas de segurança e padrões técnicos a serem seguidos. Nesse sentido, a autoridade nacional deverá estimular esses agentes a adotarem regras que facilitem o controle dos titulares sobre seus dados.

No tocante à fiscalização, há ainda muitas questões que deverão ser aprofundadas pela legislação brasileira, como o caso das sanções administrativas. Na LGPD, as sanções variam entre advertências, multas, bloqueio de dados pessoais, inclusive a suspensão ou proibição de atividades de tratamento de dados para quem violar de alguma forma a lei. Essas sanções serão aplicadas após procedimento administrativo que assegure contraditório e ampla defesa e irão variar de acordo com o caso concreto, ao analisar quesitos como a gravidade da infração e a sua reincidência.

No Artigo 52 da LGPD há previsão de que as multas possam ser diárias ou simples. As multas simples podem apresentar valor de até 2% (dois por cento) do faturamento do último exercício da pessoa jurídica de direito privado ou do grupo responsável, limitada a cinquenta milhões de reais por infração. Cumpre ressaltar que ainda devem ser melhor estruturadas as medidas coercitivas e punitivas, a fim de que se dê real efetividade a norma. Comparada à legislação europeia, as multas administrativas impostas pela lei brasileira ainda são muito pequenas. No GDPR, as sanções administrativas podem chegar até vinte milhões de euros ou até 4% (quatro por cento) do faturamento anual da empresa (Artigo 83).

Cumpre frisar que, apesar do importante passo que foi dado com a publicação da Lei 13.709/18 no sentido de proteção dos direitos fundamentais dos cidadãos, alguns de seus principais instrumentos de efetividade foram objeto de veto (Art. 55 ao 59 LGPD), quais sejam, a Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, verdadeiro auxiliar da Autoridade Nacional. O motivo do veto do Presidente Michel Temer foi alegado vício de iniciativa, pois a criação do órgão

deveria partir do Executivo Federal. Todavia, concordou com o mérito de criação do órgão.
207

A criação de uma Autoridade Nacional de Proteção de Dados é de fundamental importância pois seria a responsável por fiscalizar o cumprimento, aplicar sanções e sanar dúvidas sobre a aplicação da lei, tendo em vista a elevada especificidade da matéria. A ANPD seria uma instituição autárquica vinculada ao Ministério da Justiça e que gozaria de autonomia e independência frente ao Poder Público, visto que este por vezes é também violador da privacidade dos cidadãos.

Por fim, cabe análise do atual contencioso no Brasil relativo a matéria. Cabe acentuar que já existe prática contenciosa com vistas a obter a proteção dos dados pessoais no país, mesmo antes da publicação da LGPD. Essa atuação apresenta fundamento na própria Constituição Federal de 1988, no Código de Defesa do Consumidor e no Marco Civil da Internet pois, como já abordado anteriormente, são normas que já oferecem proteção aos dados pessoais sob diferentes perspectivas.

Portanto, com a entrada em vigor da LGPD, a tendência é de aumento exponencial do número de ações coletivas, como as ações civis públicas impetradas pelo Ministério Público, e de inquéritos civis para apurar eventuais infrações. Como exemplos atuais temos o Inquérito Civil nº 347/5ª PJDC/2016, em que o Ministério Público do Rio de Janeiro impetrou ação civil pública em face da DECOLAR.COM, pessoa jurídica de direito privado, com fundamento na defesa do consumidor no comércio eletrônico. A empresa foi acusada de discriminar consumidores com base em algoritmos que levavam em consideração sua origem geográfica e/ou nacionalidade, tendo em vista que manipulava os preços (*geo pricing* ou precificação diferenciada) e a disponibilidade de ofertas de hospedagem (*geo blocking* ou bloqueio da oferta) de acordo com a sua localização ou origem.²⁰⁸

207 BRASIL. Agência Senado. Sancionada com vetos lei geral de proteção de dados pessoais. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 26 nov. 2018.

208 CONSUMIDOR VENCEDOR. Ação civil pública Decolar.com. Disponível em: <http://rs.consumidorvencedor.mp.br/documents/13137/332720/acp.pdf>. Acesso em: 26 nov. 2018.

Outro exemplo é a Ação Civil Pública nº 0000188-96.2015.8.07.0001 impetrada pelo Instituto Brasileiro de Política e Direito de Informática (IBDI) em face da *Google*, pessoa jurídica de direito privado, com o fim de obter indenização por danos morais coletivos, em razão de coletas de dados pessoais indiscriminadas. Essa coleta teria sido realizada pela plataforma do *Google Street View* e do *Google Buzz*, que processaram e analisaram indevidamente as informações pessoais de terceiros. Em sede liminar, foi pedido que a empresa fornecesse informações detalhadas sobre a atuação desses projetos em território brasileiro.^{209 210}

Por último, temos o caso da Ação Civil Pública nº 1090663-42.2018.8.26.0100 movida pelo Instituto Brasileiro de Defesa do Consumidor em face da Concessionária da Linha 4 do Metrô de São Paulo, também conhecida pelo nome fantasia ViaQuatro, em razão de coleta de dados biométricos sem consentimento dos usuários do transporte público. A empresa implementou tecnologias no interior do metrô que eram capazes de captar a emoção (como alegria, raiva ou neutralidade), o gênero e a faixa etária das pessoas posicionadas em frente aos sensores, estes que se encontravam acima de propagandas publicitárias.²¹¹

Nesse sentido, foi alegado que a coleta de dados pessoais é ilegal e que violaria uma série de direitos, como o direito do consumidor à informação, visto que esses não foram informados sobre a coleta. Da mesma forma, não era oferecida opção para consentir ou não com o processamento e tratamento dos dados.²¹²

209 MIGALHAS. Ação coletiva indenizatória Google. Disponível em: <<https://www.migalhas.com.br/arquivos/2015/7/art20150721-03.pdf>>. Acesso em: 26 nov. 2018.

210 MIGALHAS. Instituto ajuíza ações coletivas contra o Google por invasão de privacidade dos brasileiros. Migalhas, 21.07.2015. Disponível em: <https://www.migalhas.com.br/Quentes/17,MI223791,91041-Instituto+ajuiza+acoes+coletivas+contra+o+Google+por+invasao+de>. Acesso em: 26 nov. 2018.

211 IDEC. Ação civil pública ViaQuatro. Disponível em: <https://idec.org.br/sites/default/files/acp_viaquatro.pdf>. Acesso em: 26 nov. 2018.

212 Disponível em: <<https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp>>. Disponível em: 26 nov. 2018.

CONCLUSÃO

Em meio a um desenvolvimento tecnológico desenfreado que tende a reduzir os direitos fundamentais dos indivíduos, resta a indagação: deve a democracia deixar crescer em seu interior aquilo que pode se tornar uma famigerada proliferação de Pequenos Irmãos (*Small Brothers*) de controle social?

A resposta para essa indagação pode ser formulada através da recente emergência de técnicas e legislações em todo o mundo com o intuito de frear o poder de controle das plataformas e provedores sobre os usuários e cidadãos. Intensifica-se, dessa forma, a preocupação atual quanto aos rumos traçados pela disrupção de novas tecnologias, como o aprimoramento da Inteligência Artificial e de métodos de manipulação de escolhas e de informações.

Por conseguinte, necessário se torna abordar a ética das escolhas feitas pelas máquinas, bem como as práticas discriminatórias decorrentes da manipulação de informações pessoais. Em razão desse cenário, não se pode afastar considerações de caráter social e moral ao se regularem as relações no ciberespaço. Segundo Rodotà:

“Para as tecnologias da informação e da comunicação também é preciso questionar se tudo o que é tecnicamente possível é socialmente e politicamente aceitável, eticamente admissível, juridicamente lícito”.

²¹³

Destarte, tendo em vista a imensa massa de informações pessoais hoje disponíveis e a forte tendência de commodificação de dados pessoais, Rodotà aponta que é preciso agir de forma tal que a sociedade em rede não seja progressivamente identificada como um espaço comercial, no qual os direitos reconhecidos são somente aqueles ligados à troca de bens e serviços. Conclui, nesse sentido, que é preciso impedir essa tendência totalitária do consumismo, reduzindo o cidadão a mero consumidor e seus dados pessoais a meros objetos de consumo. ²¹⁴

²¹³ RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 142.

²¹⁴ Ibidem, p. 157-158.

Apesar disso, Rodotà nos atenta para a possibilidade de uma visão democrática da publicização dos dados, em que os dados possam ser utilizados como meios para a “socialização” do acesso à informação. Dessa forma, poderia ocasionar uma maior paridade entre os cidadãos visto que poderiam ter acesso a informações antes indisponíveis para todos. Reduzindo-se a desproporção entre os dados coletados e os dados tornados públicos, poderíamos vislumbrar uma visão utópica do futuro da tecnologia, esta que, entretanto, parece se afastar cada vez mais de nossa realidade.²¹⁵

²¹⁵ RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 33.

REFERÊNCIAS BIBLIOGRÁFICAS

3% [Seriado]. Direção: César Charlone et al. Produção: César Charlone et al. Brasil: Boutique Filmes, 2016.

A TASTE OF ARMAGEDON (Temporada 1, ep. 23). **Star Trek** [Seriado]. Direção: Joseph Pevney. Produção: Gene L. Coon. Estados Unidos: Desilu Productions, 1967. 1 DVD (50 min.), son., color.

BAIÃO, Kelly; GONÇALVES, Kalline. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**, a. 3. n. 2. 2014. p. 2. Disponível em: < <http://civilistica.com/wp-content/uploads/2015/02/Bai%C3%A3o-e-Gon%C3%A7alves-civilistica.com-a.3.n.2.2014.pdf> >. Acesso em: 23 nov. 2018.

BARROSO, Luís Roberto. **Constituição da República Federativa do Brasil Anotada**. 3ª edição, amplamente revista e atualizada até a EC no 32/2001. São Paulo: Saraiva, 2001.

BAUMAN, Zygmunt. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2014.

BENTHAM, J. **O panóptico**. Belo Horizonte: Autêntica Editora, 2008.

BIONI, Bruno R.; MONTEIRO, Renato L. O papel do Data Protection Officer. **Jota**, 04.12.2017. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-papel-do-data-protection-officer-04122017>. Acesso em: 26 nov. 2018.

BLACK MIRROR [Seriado]. Direção: Joe Wright et al. Produção: Barney Reisz. Reino Unido: Zeppotron, 2011.

BLACK, Edwin. **IBM e o Holocausto**. 3. ed. São Paulo: Campus, 2006.

BODIN DE MORAES, Maria Celina. **Ampliando os direitos da personalidade**. In: Na medida da pessoa humana. Estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

BRASIL. Agência Senado. **Sancionada com vetos lei geral de proteção de dados pessoais**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protacao-de-dados-pessoais>. Acesso em: 26 nov. 2018.

BRASIL. Código Civil dos Estados Unidos do Brasil, Lei 3.071, de 1º de janeiro de 1916. **Diário Oficial da União**, Rio de Janeiro, RJ, 5 de janeiro de 1916. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L3071.htm>. Acesso em: 29 nov. 2018.

BRASIL. Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990. **Diário Oficial da União**, Brasília, DF, 12 de setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm>. Acesso em: 28 nov. 2018.

BRASIL. Constituição da República Federativa de Brasil, de 5 de outubro de 1988. **Diário Oficial da União**, Brasília, DF, Outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 nov. 2018.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial da União**, Brasília, DF, 11 de maio de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 28 nov. 2018.

BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 29 nov. 2018.

BRASIL. Lei 13.709, 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, DF, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29 nov. 2018.

BRASIL. Lei 9.507, de 12 de novembro de 1997. **Diário Oficial da União**, Brasília, DF, de 13 de novembro de 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 29 nov. 2018.

BRASIL. Supremo Tribunal Federal. Reclamação nº 22328-RJ. Reclamante: Abril Comunicações S/A. Relator: Ministro Roberto Barroso. Rio de Janeiro, julgado em

06.03.2018. Disponível em:<
<http://portal.stf.jus.br/processos/downloadPeca.asp?id=314302526&ext=.pdf>>. Acesso em: 28 nov. 2018.

BRASIL. Código Civil, Lei 10.406, de 10 de janeiro de 2002. 1ª edição. São Paulo: **Revista dos Tribunais**, 2002. Disponível em:<
http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 28 nov. 2018.

BROOKER, Charlie. The dark side of our gadget addiction. **The Guardian**, 01.12.2011. Disponível em:< <https://www.theguardian.com/technology/2011/dec/01/charlie-brooker-dark-side-gadget-addiction-black-mirror>> . Acesso em: 23 nov. 2018.

CASTELLS, M. **A sociedade em rede: Vol.1**. A era da informação: Economia, sociedade e cultura. 2. ed. São Paulo: Paz e Terra, 1999.

CATALA, Pierre. **Ebauche d'une théorie juridique de l'information**. In: Informatica e Diritto, ano IX, jan-apr. 1983.

CAVALLI, Olga. **Internet das coisas e inovação na América Latina**. [S.l.: s.n.]: Mimeogr, 2016.

CONSUMIDOR VENCEDOR. Ação civil pública Decolar.com. Disponível em:
<http://rs.consumidorvencedor.mp.br/documents/13137/332720/acp.pdf>. Acesso em: 26 nov. 2018.

DELEUZE, Gilles. **Foucault**. São Paulo: Brasiliense, 2013.

DELEUZE, Gilles. **Postscript on the societies of control**. October, n. 59, 1992.

DICK, Philip K. **Minority Report – A nova lei**. Brasil: RECORD, 2002.

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

DONEDA, Danilo. **Pessoa e privacidade na sociedade da informação, Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DOS SANTOS, Marcos Moura Baptista. **Sociedade em rede e modo de desenvolvimento informacional: descrições sociológicas da sociedade contemporânea**. Texto de trabalho, escrito como roteiro para aulas da disciplina de sociologia no curso de ciências sociais da Unisc. Disponível em: < <https://docplayer.com.br/20768790-Sociedade-em-rede-e-modo-de-desenvolvimento-informacional-descricoes-sociologicas-da-sociedade-contemporanea-sob-o-capitalismo-avancado.html>>. Acesso em: 23 nov. 2018.

DOS SANTOS, Sara Gomes. **Era do espelho: A captura do olhar nas redes sociais**. UEPB, Campina Grande, 2016. Disponível em: < <http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/11696/1/PDF%20-%20Sara%20Gomes%20dos%20Santos.pdf>>. Acesso em: 25 nov. 2018.

EGGERS, Dave. **O Círculo**. São Paulo. Companhia das Letras, 2014.

EUROPA. Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000. **Jornal Oficial das Comunidades Europeias**, C 364/1, de 18 de dezembro de 2000. Disponível em: < http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 29 nov. 2018.

EUROPA. Comissão Europeia. **O que são dados pessoais**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 26 nov. 2018.

EUROPA. Diretiva 95/46/CE, de 24 de outubro de 1995. **Jornal Oficial da União Europeia**, L281, de 23 de novembro de 1995. p. 31-50. Disponível em: < <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>>. Acesso em: 29 nov. 2018.

EUROPA. Ratificação do Regulamento (EU) 2016/679, de 27 de abril de 2016. **Jornal Oficial da União Europeia**, L127, 61º ano, de 23 de maio de 2018. Disponível em: < <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2018:127:FULL&from=PT#%FE%FF%00O%00J%00X%00%00%000%002%000%001%00P%00T>>. Acesso em: 29 nov. 2018.

EUROPA. Regulamento (EU) 2016/679, de 27 de abril de 2016. Relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L119, 59º ano, de 4 de maio de 2016. Disponível

em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>>. Acesso em: 29 nov. 2018.

EUROPA. Tratado que estabelece uma Constituição para a Europa, de 29 de outubro de 2004. **Jornal Oficial da União Europeia**, C 310, 47º ano, de 16 de dezembro de 2004. Disponível em:< <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:C:2004:310:TOC>>. Acesso em: 29 nov. 2018.

FOUCAULT, M. **Vigiar e punir**. Petrópolis: Vozes, 2000.

FOUCAULT, Michel. **A Arqueologia do Saber**. Rio de Janeiro: Forense Universitária, 2009.

FRAU, Christian. **A luta contra o terrorismo e a proteção de dados pessoais**. Revista da AGU nº 28. p. 102-103. Disponível em:<<file:///C:/Users/Usu%C3%A1rio.DESKTOP-RINM3A4/Downloads/163-427-1-PB.pdf>>. Acesso em: 23 nov. 2018.

FROSINI, Vittorio. **Contributi ad un diritto dell'informazione**. Napoli: Liguori, 1991.
GALVÃO E SILVA ADVOCACIA. Lei GDPR em português. **Galvão & Silva Advocacia**, 19.07.2018. Disponível em: <https://www.galvaoesilva.com/lei-gdpr-em-portugues/>. Acesso em: 26 nov. 2018.

GHISLENI, Eduardo Steffenello. **Vigilância na sociedade em rede: A coleta de dados pessoais na internet e suas implicações ao direito à privacidade**. 2015. 60 f. Trabalho de Conclusão de Curso (Graduação em Direito)-UFSM, Santa Maria, 2015. Disponível em:< <https://repositorio.ufsm.br/bitstream/handle/1/11518/MONOGRAFIA%20EDUARDO%20%20GHISLENI.pdf?sequence=1&isAllowed=y>>. Acesso em: 25 nov. 2018.

HER. Direção: Spike Jonze. Estados Unidos da América: Warner Bros. Pictures, 2013. 1 DVD (125 minutos).

HUXLEY, A. **Admirável mundo Novo**. Rio de Janeiro: Editora Globo, 1932.
IDEC. Ação civil pública ViaQuatro. Disponível em: < https://idec.org.br/sites/default/files/acp_viaquatro.pdf>. Acesso em: 26 nov. 2018.

LEMOS, Ronaldo. et. al. GDPR: A nova legislação de proteção de dados pessoais da Europa. **Jota**, 25.05.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018>. Acesso em: 26 nov. 2018.

LEOPOLDO, Rafael. **Vigilância Líquida: Variações sobre o Panoptismo**. Sapere Aude – Revista de Filosofia. Belo Horizonte, v. 6, n. 12, jan. 2016. p. 894-902. Disponível em: <<http://periodicos.pucminas.br/index.php/SapereAude/article/view/11261/9115>>. Acesso em: 23 nov. 2018.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Direito Rio, 2018.

MAIA, Luciano Soares. **A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais**. In: CONSELHO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM DIREITO. Anais do XVI Congresso Nacional do Conpedi. Florianópolis: Fundação Boiteux, 2008.

MARKOFF, John. Entrepreneurs See a Web Guided by Common Sense. **The New York Times**, 12.11.2006. Disponível em: <https://www.nytimes.com/2006/11/12/business/12web.html>. Acesso em: 23 nov. 2018.

MARX, Gary T. **An ethics for the new surveillance**. Information Society, v.14, n.3, 1998.

MARX, Karl; ENGELS, Friedrich. **O Manifesto comunista**. 14 ed. São Paulo: Paz e Terra, 2004.

MEIRA, Silvio. **Sinais do futuro imediato, #1: internet das coisas**. Recife: Ikewai, dez. 2016.

MIGALHAS. Ação coletiva indenizatória Google. Disponível em: <<https://www.migalhas.com.br/arquivos/2015/7/art20150721-03.pdf>>. Acesso em: 26 nov. 2018.

MIGALHAS. Instituto ajuíza ações coletivas contra o Google por invasão de privacidade dos brasileiros. **Migalhas**, 21.07.2015. Disponível em: <https://www.migalhas.com.br/Quentes/17,MI223791,91041-Instituto+ajuiza+acoes+coletivas+contra+o+Google+por+invasao+de>. Acesso em: 26 nov. 2018.

MINORITY REPORT. Direção: Steven Spielberg. Estados Unidos da América: Cruise/Wagner Productions et al, 2002. 1 DVD (2h 26 minutos).

MORE, Sir. Thomas. **Utopia**. Tradução (da versão em inglês) de Jefferson Luiz Camargo e Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 1999.

NOSEVIDE (Temporada 3, ep. 1). **Black Mirror** [Seriado]. Direção: Joe Wright et al. Produção: Barney Reisz. Reino Unido: Zeppotron, 2016. 1 DVD (63 min.), son., color.

O'NEIL, C. **Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. Denver: Crown, 2016.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PEREIRA, Yuan V. **A fronteira final: Guerra fria e movimentos pacifistas refletidos em Jornada nas Estrelas**. Unilasalle Editora – Diálogos. Canoas, n. 34, 2017. Disponível em: <<https://revistas.unilasalle.edu.br/index.php/Dialogo/article/view/3290>>. Acesso em: 23 nov. 2018.

PINHEIRO, Patricia Peck. Tabela comparativa. Consultor Jurídico, 10.07.2018. Disponível em: <<https://www.conjur.com.br/dl/tabela-comparativa-pl-protecao-dados.pdf>>. Acesso em: 26 nov. 2018.

PINTO, Paulo Mota. **O direito à reserva sobre a intimidade da vida privada**. In: Boletim da Faculdade de Direito, n. 69, 1993.

RAMONET, Ignacio. A atualidade chocante de ‘Admirável Mundo Novo’. **Revista Fórum**, 26.07.2015. Disponível em: <<https://www.revistaforum.com.br/a-atualidade-chocante-de-admiravel-mundo-novo/>>. Acesso em: 23 nov. 2018.

ROCHA, Camila. Por que é fácil confundir realidade e distopia nos dias atuais. **Nexo Jornal**, 03.08.2017. Disponível em: <<https://www.nexojornal.com.br/expresso/2017/08/03/Por-que-%C3%A9-f%C3%A1cil-confundir-realidade-e-distopia-nos-dias-atuais>>. Acesso em: 23 nov. 2018.

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

RODRIGUEZ, Luís; SPITZ, Rejane. **Big Data versus autonomia: O paradoxo do suporte à “decisão autônoma” usando Big Data.** Congresso Brasileiro de Pesquisa e Desenvolvimento em Design – 12º P & D 2016. Rio de Janeiro, n. 2, vl. 9, 2016. Disponível em:< <http://pdf.blucher.com.br.s3.amazonaws.com/designproceedings/ped2016/0344.pdf>>. Acesso em: 23 nov. 2018.

RR. “Black Mirror” ou vida real? China começa a “avaliar” pessoas em aplicação. **Renascença**, 20.03.2018. Disponível em: <https://rr.sapo.pt/noticia/108659/black-mirror-ou-vida-real-china-comeca-a-avaliar-pessoas-em-aplicacao>. Acesso em: 23 nov. 2018.

SANTOS, Thiago; DUARTE, Bruno. **A responsabilidade civil dos provedores de aplicação de internet no tratamento de dados à luz da Lei nº 12.965/14 denominada o marco civil da internet.** Revista de Direito da Faculdade Estácio do Pará. Belém, v. 5, n. 7.

SEGIB. XIII Cimeira Ibero-americana de chefes de estado e de governo. **Declaração de Santa Cruz de la Sierra.** 14-15 nov. 2003. Disponível em: <<https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>>. Acesso em: 26 nov. 2018.

SHAKESPEARE, William. **Macbeth.** São Paulo: Paz e Terra, 1996.

SMITH, Robert Ellis. Privacy. **How to protect what's left of it.** New York: Anchor Press, 1979.

SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age.** NYU Press, 2004.

WARREN, Samuel; BRANDEIS, Louis D. **The right to privacy.** 4 Harvard Law Review 193, 1890. Disponível em:< <http://www.spywarewarrior.com/uiuc/w-b.htm>>. Acesso em: 26 nov. 2018.

ZOGBI, Paula. Netflix, LinkedIn e YouPorn têm vazamento de 1,4 bilhão de dados sigilosos. **InfoMoney**, 12.12.2017. Disponível em:<<https://www.infomoney.com.br/minhas-financas/gadgets/noticia/7136758/netflix-linkedin-youporn-tem-vazamento-bilhao-dados-sigilosos>>. Acesso em: 26 nov. 2018.

ZUBOFF, Shoshana. **Big other: surveillance capitalism and the prospects of na information civilization.** Journal of Information Technology, 2015.