UNIVERSIDADE DE BRASÍLIA – UnB
FACULDADE DE DIREITO – FD
CURSO DE GRADUAÇÃO EM DIREITO

PRISCILA MARIA MENEZES DE ARAÚJO

A UTILIZAÇÃO DE DADOS PESSOAIS SENSÍVEIS NA FORMAÇÃO DO PERFIL COMPORTAMENTAL DE PESSOAS NATURAIS E O POTENCIAL DANO AOS SEUS TITULARES

BRASÍLIA – DF
2019

PRISCILA MARIA MENEZES DE ARAÚJO

A UTILIZAÇÃO DE DADOS PESSOAIS SENSÍVEIS NA FORMAÇÃO DO PERFIL COMPORTAMENTAL DE PESSOAS NATURAIS E O POTENCIAL DANO AOS SEUS TITULARES

Monografia apresentada como requisito parcial à obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.
Orientadora: Professora Dra. Ana de Oliveira Frazão.

BRASÍLIA – DF
2019

PRISCILA MARIA MENEZES DE ARAÚJO

A UTILIZAÇÃO DE DADOS PESSOAIS SENSÍVEIS NA FORMAÇÃO DO PERFIL COMPORTAMENTAL DE PESSOAS NATURAIS E O POTENCIAL DANO AOS SEUS TITULARES

Monografia apresentada como requisito parcial à obtenção do grau de Bacharela em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.
Brasília, 05 de dezembro de 2019.

_____
Professora Doutora Ana de Oliveira Frazão (Orientadora)
Universidade de Brasília

_____
Professora Doutora Laura Schertel Ferreira Mendes (Avaliadora)
Universidade de Brasília

_____
Professor Doutor Thiago Luís Sombra (Avaliador)
Universidade de Brasília

_____
Wenderson Siqueira Borges (Avaliador suplente)
Torreão Braz Advogados

How do we have so much information but we know so little?

(Noam Chomsky)

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por me permitir chegar até aqui. Sem Ele, teria sido impossível superar todos os obstáculos e vencer mais uma luta em prol da realização de um sonho.

Aos meus pais, Fátima e Maurício, exemplos de vida e superação, que tanto me incentivaram.

À minha amada avó Francisca, que tem toda a minha saudade e que mesmo ausente deste mundo, proporciona-me todo o acalento.

Agradeço às minhas irmãs, Mariana e Juliane, ao meu padrinho Robson e ao meu cunhado Bruno, que me ensinaram o valor da persistência. Ao meu querido sobrinho Matheus, que com o seu olhar de criança, conquistou todo o meu coração.

À Claudia Pedreira, exemplo ímpar de luta e força.

Também agradeço à Amanda Carrilho e à Heloísa Gonçalves. Sem vocês, a experiência universitária não teria sido tão enriquecedora e completa. Todos os momentos em que passamos juntas na Faculdade de Direito da UnB ficarão guardados para sempre com muito carinho.

À querida amiga Thais Soares, que mesmo tão longe, tanto me apoia em todos os projetos de vida. Aos demais amigos, toda a minha gratidão, especialmente à Andressa Rayane, ao Paulo Roberto, Caetano Almeida, Bruno Sales, Guilherme Teles, à Gabriela Reis e à Anna Clara Fennol.

Às advogadas responsáveis pelo desenvolvimento da paixão gigantesca e ininterrupta pela advocacia: Maira Ramos e Sofia Pelegio, que primeiro me apresentaram essa profissão tão incrível.

Ao Núcleo de Execuções contra a Fazenda Pública do Torreão Braz Advogados, que me instiga a ser melhor todos os dias. Em especial, à Gabriela Teixeira, que me inspira e me auxilia em todos os projetos profissionais, à Camila Fischgold e ao Denny Peixoto, que oferecem os subsídios necessários ao meu crescimento.

À advogada Priscilla Brazil, que me fornece tanta confiança e me ensina o caminho certo a ser percorrido. Sem você, certamente minha trajetória não teria sido tão proveitosa.

À minha querida orientadora Ana Frazão, que desde as lições de Teoria Geral do Direito Privado, despertou-me o interesse para tantas discussões. Por toda a dedicação e orientação que proporcionaram a concretização desse projeto. A você, devo toda a minha paixão pela pesquisa. Que sigamos juntas em outros desafios.

À professora Laura Schertel, ao professor Thiago Sombra e ao advogado Wenderson Siqueira, que abrilhantaram a composição da banca examinadora.

Por fim, à Universidade de Brasília, lugar que me apresentou uma gama infinita de possibilidades, experiências e sonhos. Minha amada casa.

RESUMO

A Nova Lei Geral de Proteção de Dados, LGPD, configura-se como importante instrumento normativo que servirá como principal vetor na regulação do tratamento de dados pessoais no Brasil, especialmente os dados pessoais sensíveis. Desse modo, o presente trabalho tem como objetivo analisar a utilização desses dados pessoais sensíveis na formação de perfis de comportamento e de modelos classificatórios e preditivos, que geram danos aos titulares dessas informações pessoais e criam ou fomentam cenários discriminatórios, seja no âmbito laboral, em discussões políticas ou até mesmo no que diz respeito aos dados de saúde coletados. Também serão abordadas ferramentas, como o estímulo das boas práticas de governança, capazes de mitigar tais cenários desfavoráveis aos usuários. A fim de subsidiar tal análise, foram utilizadas as revisões bibliográfica e legislativa do tema, que tem como ponto central a Lei n. 13.709/2018 e, subsidiariamente, o *General Data Protection Regulation*. Por fim, a análise do objeto de estudo foi feita com o intuito de despertar e desenvolver alguns pontos importantes que fomentam inúmeras discussões as quais a LGPD deverá enfrentar, principalmente, a partir de agosto de 2020.

Palavras-chave: Dados pessoais sensíveis. Perfil comportamental. Monitoramento comportamental. Discriminação. Dano.

ABSTRACT

The New General Data Protection Act, LGPD, is an important normative instrument that serves as the main control vector for the processing of personal data in Brazil, especially the identified personal data. Thus, the present work aims to analyze the use of this sensitive personal data in the formation of behavioral profiles and classifying and predictive models, which cause damage to the holders of this personal information and create or foster discriminatory scenarios, either at work, in political discussions or even regarding the health data collected. Tools should also be addressed, such as encouraging good governance practices that can mitigate them for users. In order to support this analysis, the bibliographic and legislative reviews of the theme were used, which has as its central point Law 13,709/2018 and, in the alternative, the General Data Protection Regulation. Finally, the analysis of the object of study was made in order to awaken and develop some important points that foment countless discussions that LGPD will face, mainly, from August 2020.

Keywords: Sensitive personal data. Behavioral profile. Behavioral monitoring. Discrimination. Damage.

LISTA DE SIGLAS E ABREVIATURAS

ANPD – Autoridade Nacional de Proteção de Dados

CCPA – California Consumer Privacy Act

CDC – Código de Defesa do Consumidor

CNBB – Confederação Nacional dos Bispos do Brasil

EDPS – European Data Protection Supervisor

GDPR – General Data Protection Regulation

IBGE – Instituto Brasileiro de Geografia e Estatística

IDEC – Instituto de Defesa do Consumidor

LGPD – Lei Geral de Proteção de Dados Pessoais

PEC – Proposta de Emenda à Constituição

PLC – Projeto de Lei da Câmara

PROCON - Proteção e Defesa do Consumidor

TJUE – Tribunal de Justiça da União Europeia

SENACON - Secretaria Nacional do Consumidor

SUS – Sistema Único de Saúde

SUMÁRIO

INTRODUÇÃO

A economia movida a dados tem estimulado um debate intenso a respeito da proteção de dados pessoais, de sorte que se viu a necessidade de se editar uma lei transversal que alcançasse não só a coleta, o tratamento e a eliminação de dados pessoais por parte de agentes privados, mas também de agentes públicos, que deverão promover uma verdadeira adequação à Lei Geral de Proteção de Dados (LGPD).

Assim, a tutela conferida pela LGPD (Lei n. 13.709/2018), que terá o início da sua vigência em agosto de 2020, configura-se como um importante avanço na regulação tecnológica brasileira, de modo que, a partir de então, o Brasil passou a compor o grupo de países que possui uma norma geral que visa à proteção dos dados pessoais dos seus cidadãos.

Nessa linha, o presente trabalho pretende, ao acompanhar os avanços da tecnologia, desenvolver o tema alvo de inúmeras discussões, como é o caso da formação de perfis de comportamento a partir da utilização de dados pessoais sensíveis.

Tal investigação será feita com o aprofundamento de conceitos caros à relação entre direito e tecnologia e ao estudo de fenômenos sociais, de modo a suscitar algumas soluções que terão o condão de contribuir para o entendimento de um fenômeno cada vez mais latejante na realidade brasileira e mundial, como é o caso do tratamento de dados pessoais.

Inicialmente, parte-se da nova realidade em que o Brasil adentra mediante a instituição de uma norma geral protetiva de dados pessoais. Isso porque, anteriormente, as legislações que tratavam o tema de forma setorial não abrangiam boa parte das questões e das problemáticas que envolvem o tratamento de dados pessoais no país, inclusive no que diz respeito aos dados pessoais sensíveis.

Desse modo, a hipótese primária que a presente pesquisa busca explanar é a de que de fato a perfilização e a tomada de decisões algorítmicas com base em dados pessoais, especialmente os dados sensíveis, podem gerar e/ou reproduzir situações discriminatórias e preconceituosas que causam danos aos titulares dos dados.

A hipótese seguinte é uma consequência da anterior: indicar alguns caminhos quanto à responsabilização civil desses agentes e oferecer algumas ferramentas que auxiliarão, à luz da Lei n. 13.709/18 e do arcabouço principiológico do *General Data Protection Regulation*, GDPR – o regulamento europeu sobre o tema – os agentes privados e públicos a criarem cenários em que o tratamento de dados pessoais não causem discriminação e danos aos titulares.

Busca-se averiguar os reflexos da perfilização e das decisões automatizadas que possuem o potencial de promover resultados irreversíveis para incontáveis pessoas, como, por

exemplo, a seleção de pessoas para o preenchimento de uma vaga de emprego feita com base nas informações sobre o *credit scoring*, o que leva a crer que pessoas com baixa pontuação de crédito possuem certo grau de risco e que, por isso, estão em desvantagem em relação aos demais candidatos ou até mesmo serão eliminados apenas com base nessa informação. Tal hipótese caracteriza evidente discriminação entre os indivíduos e os grupos sociais a que pertencem os candidatos à vaga.

No primeiro capítulo, a era informacional e a economia movida a dados serão abordadas a fim de expor o cenário em que se fez necessária a adoção de uma norma geral de proteção de dados. Após, será abordada a influência do GDPR no contexto brasileiro e, por fim, serão expostos alguns dos inúmeros conceitos importantes elencados pela LGPD.

No segundo capítulo, o paradoxo da constante vigilância dos usuários e da opacidade do tratamento das suas informações pessoais será retratado. Posteriormente, o tema da proteção de dados será apresentado como um direito fundamental e o restante do capítulo se dedicará a estudar a influência dos algoritmos e das suas decisões no processo de formação dos perfis de comportamento, além da ocorrência de dado e da criação e/ou do fomento de práticas discriminatórias que decorrem da manipulação dos dados pessoais sensíveis.

No que diz respeito ao terceiro capítulo, será feita uma análise da responsabilidade civil relacionada ao tema, momento em que será abordado o panorama com o qual a Lei Geral de Proteção de Dados deverá lidar. Também será tratada a coexistência das responsabilidades subjetiva e objetiva, com a análise dos pontos em comum entre elas e, no que diz respeito à responsabilidade objetiva, a abordagem será feita também sob o prisma da teoria do risco.

Após, serão pincelados alguns dispositivos trazidos pela Lei n. 13.709/2018 no que diz respeito à responsabilização dos agentes de tratamento de dados pessoais, como a responsabilidade solidária, a reparação por dano coletivo e a própria ausência da responsabilidade.

O terceiro capítulo se encerra com uma abordagem acerca da inversão do ônus probatório que, assim como na esfera do direito consumerista, far-se-á de suma relevância para a seara da proteção de dados pessoais.

O último capítulo abordará algumas questões que, na prática, são decisivas para a gestão de dados pessoais, e serão ainda mais com o advento efetivo da Lei n. 13.709/2018, como, a adoção do *Compliance* e das boas práticas de governança pelos agentes de tratamento de dados, que se constituirá como um meio essencial dotado de ferramentas que viabilizarão o tratamento de dados pessoais sem que haja a geração de dano aos titulares ou a formação e/ou o fomento de contextos discriminatórios.

A respeito dessas ferramentas, inclusive, destacam-se modelos prezam pela privacidade em sua arquitetura, como o *privacy by design*, bem como a importância do papel do *Data Protection Officer*, o DPO para o GDPR, ou encarregado para a LGPD.

Também serão abordados alguns dos mecanismos de *enforcement* que atuam e deverão atuar de forma mais incisiva, a partir do início da vigência da Lei Geral de Proteção de Dados e por meio da análise e do controle das atividades atreladas ao tratamento de dados pessoais, a fim de que haja um alinhamento satisfatório ao que dispõe a referida lei.

Por fim, a questão do consentimento também será abordada como hipótese autorizadora do tratamento de dados pessoais, de modo a suscitar questionamentos acerca da medida em que essa hipótese pode ser aplicada ao tratamento de dados pessoais sensíveis sem que haja o perigo da manifestação do dano.

Ao analisar a era informacional e o capitalismo de vigilância, busca-se entender a formação de perfis de comportamento com base em dados pessoais sensíveis e a própria ocorrência do dano decorrente dessas práticas, além da criação ou do agravamento de contextos discriminatórios.

O presente trabalho, portanto, será desenvolvido por meio da análise bibliográfica e legislativa, que permitirão desenvolver e apresentar um dos temas mais instigantes para a proteção de dados pessoais, que deverá ser enfrentado pela Lei n. 13.709/2018.

CAPÍTULO 1 - A UTILIZAÇÃO DE INFORMAÇÕES PESSOAIS

1.1. A sociedade informacional e a economia movida a dados: delineando o contexto da manipulação de dados pessoais

A sociedade da informação, que nasce na década de 1980, é marcada pelo desenvolvimento de um novo modelo que tem como protagonista a tecnologia geradora de conhecimento, processamento de informação e de comunicação. Nesse sentido, Manuel Castells[1] explana que a revolução tecnológica, a reestruturação econômica e a crítica à cultura vigente à época, juntas, redefinem as relações de produção, de poder e de experiência e, assim, constituem a era da informação.

Essa revolução e reestruturação ditam a esfera do comportamento social e da própria comunicação entre indivíduos e agentes econômicos, de modo que, estes últimos, dotados do controle das novas tecnologias, fixam novos parâmetros do sistema econômico nascente, como: (i) a maximização ainda maior do lucro nas relações entre capital e o trabalho; (ii) o aumento da produtividade do trabalho viabilizado pelas novas tecnologias; (iii) o direcionamento de recursos a fim de obter maiores ganhos; e (iv) a globalização da produção e da própria circulação de produtos e serviços[2].

Quanto ao último parâmetro, a rede de conexões entre agentes econômicos, governo e indivíduos foi viabilizada pela formação de novas estruturas e modelos de negócio que abriram caminhos para a atuação da economia que, agora global, lida com uma nova capacidade produtiva, segundo Manuel Castells:

> Por outro lado, o novo sistema de comunicação transforma radicalmente o espaço e o tempo, as dimensões fundamentais da vida humana. Localidades ficam despojadas de seu sentido cultural, histórico e geográfico e reintegram-se em redes funcionais ou em colagens de imagens, ocasionando um espaço de fluxos que substitui o espaço de lugares. O tempo é apagado no novo sistema de comunicação já que passado, presente e futuro podem ser programados para interagir entre si na mesma mensagem. O espaço de fluxos e o tempo intemporal são as bases principais de uma nova cultura, que transcende e inclui a diversidade dos sistemas de representação historicamente transmitidos: a cultura da virtualidade real, onde o faz-de-conta vai se tornando realidade. (CASTELLS, 2005, p. 462)

É nesse contexto de controle que os dados pessoais se apresentam cada vez mais como uma poderosa matéria-prima para os agentes que a manipulam, mas que, em contrapartida, é

[1] CASTELLS, Manuel. *A sociedade em rede*. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.
[2] Op.cit., pp. 459-462.

desconhecida em seu tratamento e manipulação para os seus titulares e traz consequências desconhecidas não só para juristas, psicólogos, economistas e cientistas políticos, mas também para os próprios profissionais de tecnologia da informação, que lidam com redes cada vez mais complexas.

Para Manuel Castells[3], a era da informação se retroalimenta, de forma que as fontes de conhecimento, que também decorrem do grande volume de dados existentes e constituídos a cada dia, renovam-se e se robustecem, o que permite a otimização e a geração de mais conhecimento e informação. Esse ciclo, marcado por um novo modo de desenvolvimento, é um dos cernes da economia movida a dados.

Essa economia baseada em conhecimento, informação e tecnologia está pautada também em hábitos de uso da internet pelos usuários. Desde os aplicativos utilizados, as informações inseridas para fins de registro em alguns sites, o tempo em que os usuários permanecem conectados, quais as páginas visitadas, quantas e quais as fotos e vídeos foram curtidos e até mesmo a velocidade e a força aplicada ao digitar e interagir com os mais diversos dispositivos eletrônicos.

Victor Carvalho[4] elucida que esses hábitos formam verdadeiros rastros digitais que, com o tratamento, o cruzamento e a análise dos dados, permite a construção de modelos de negócios que geram retornos financeiros gigantescos.

A utilização desses dados pessoais como insumos e matéria-prima, renováveis e em grande quantidade, foi abarcada, inclusive, pelo Fórum Econômico Mundial, no relatório *Our Shared Digital Future: Building an Inclusive, Trustworthy and Sustainable Digital Society*[5], o qual ressaltou que os dados pessoais seriam "a moeda do mundo digital" e que, portanto, constituem "uma nova classe de ativos econômicos".

Diante desse cenário, em que a tecnologia se faz cada vez mais presente, Shoshana Zuboff[6] entende que a chamada *information technology* possui uma dualidade. Isso porque pode ser aplicada tanto para automatizar operações, como substituir o ser humano por máquinas, quanto para a geração de um profundo nível de informação sobre questões que, antes da

---

[3] CASTELLS, Manuel. *A sociedade em rede*. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

[4] CARVALHO, Victor M. Barros de. *O direito à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória.* Dissertação (mestrado em direito). Centro de Ciências Sociais aplicadas, Universidade Federal do Rio Grande do Norte. Natal, 2018, pp. 73-74.

[5] Committed to Improving the State of the World. World Economic Forum. Insight Report. *Our Shared Digital Future: Building an Inclusive, Trustworthy and Sustainable Digital Society*. Decem. 2018. Disponível em: http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf. Acesso em 05/09/2019.

[6] ZUBOFF, Shoshana. *Big other: surveillance capitalismo and the prospects of na information civilization.* Journal of Information Technology, 30, 2015, p. 76.

sociedade informacional, eram desconhecidas e que, a partir de então, tornaram-se visíveis, passíveis de serem conhecidas a fundo e que também se tornaram compartilháveis.

"Informate" foi a expressão utilizada pela autora para definir essa capacidade dual (automatizar e informar). Shoshana Zuboff aponta que, na década de 1980, a coleta de informação já refletia os fluxos de produção, as interfaces dos clientes e os procedimentos administrativos, mas também revelava o comportamento humano por meio de ligações feitas pelo telefone, a pressão que os usuários aplicavam nas teclas ao digitarem algo, os locais, as ações, as conversas e até mesmo os compromissos firmados com outras pessoas[7].

Para além, a autora fundamenta que a utilização dessas informações na dialética mercadológica é feita por meio da acumulação e da organização dessas informações, que se transforam em dados, e que são utilizados a fim de conferirem vantagens a certos modelos de negócio[8].

Dessa forma, a utilização desses dados outorga poder a esses modelos, que moldam o campo de possibilidades de forma invisível, isto é, determina as informações que serão medidas ou repassadas, como os recursos e as pessoas serão alocadas e organizadas, define papeis e fixa quais as atividades que serão realizadas e com quais finalidades. Assim, a lógica adotada é aquela que preza pela acumulação e pela utilização dessas informações, que definem as relações, as concepções e o uso da autoridade e do poder na sociedade[9].

Portanto, Shoshana Zuboff[10] esclarece que os dados e o poder da informação na sociedade são universais em escala e em escopo, uma vez que as suas características são direcionadas a uma nova dimensão simbólica propiciada pelo monitoramento gerado a partir da coleta dos dados pessoais, que informam sobre uma ampla gama de atividades diárias dos indivíduos.

Desse modo, a autora aponta que questionamentos acerca de temas relevantes e estruturais, como as relações de poder presentes em uma sociedade, devem ser abordados de modo que seja levado em consideração o cenário atual, qual seja, o da *information society*[11].

É diante dessa nova conjuntura caracterizada pelo poder da informação e da atribuição de um papel central aos dados pessoais coletados e tratados, bem como dos reflexos, das

[7] Op.cit., p. 76.
[8] Op.cit., p. 77.
[9] Op.cit., p. 77.
[10] Op.cit., p. 77.
[11] Op.cit., p. 77.

consequências e dos seus novos desafios que, países[12] como a Austrália, a Coreia do Sul, o Japão, o Uruguai[13] e a União Europeia[14] instituíram normas que visam à tutela dos dados pessoais de seus habitantes, bem como de previsões acerca dos desdobramentos a respeito do tema no âmbito internacional.

No Brasil, o tema era abordado por normas esparsas, conforme será exposto mais adiante. Contudo, no segundo semestre de 2018, foi aprovada a Lei Geral de Proteção de Dados (LGPD), originada do Projeto de Lei da Câmara n. 53/2018[15], que promete, a partir de agosto/2020, regulamentar de forma mais estrutural o tema da proteção de dados pessoais e suas nuances, com o foco no equilíbrio entre o desenvolvimento econômico e a proteção dos titulares de dados diante do contexto da sociedade informacional e da economia movida a dados estudada por Manuel Castells.

1.2. A legislação anterior à Lei n. 13.709/2018 (LGPD)

O Brasil editou alguns diplomas normativos que se dedicam, há alguns anos, a regular e a direcionar o tratamento de dados pessoais ou, pelo menos, apresentam diretrizes e princípios que norteiam a proteção de dados pessoais.

O Código de Defesa do Consumidor (1990), o Código Civil (2002), A Lei do Cadastro Positivo (2011), a Lei do Acesso à Informação (2011) e o Marco Civil da Internet (2014) se dedicaram, cada um à sua maneira e de acordo com os seus propósitos e demandas iniciais, a abordar temas como a proteção da privacidade e da intimidade, além da utilização de dados de consumidores e alguns fenômenos da internet.

Inicialmente, com a sanção da Lei n. 8.078/90, o conhecido Código de Defesa do Consumidor, o país inaugurou sua primeira fase de regulação dos dados pessoais coletados e armazenados pelos mais diversos agentes econômicos que prestam serviços e oferecem produtos.

---

[12] Para se ter uma visão acerca da presença de normas protetivas de dados no mundo, vide o mapa intitulado como "Proteção de Dados Pessoais ao redor do mundo", localizado no Anexo A do presente trabalho.

[13] Trata-se do "estudo sobre o compartilhamento de dados em outros países" feito pela Secretaria de Governo Digital do Ministério da Economia, órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação do Governo Federal (SISP), em que foram levantadas informações a respeito da proteção de dados nos países mencionados. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/Relatorio%20Estudo%20Troca%20Informacoes%20Outros%20Paises.pdf. Acesso em 04/09/2019.

[14] EU 2016/679. *General Data Protection Regulation.* 25 de março de 2018. Disponível em: https://gdpr-info.eu. Acesso em 22/06/2019.

[15] Projeto de Lei da Câmara n. 53/2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em 01/07/2019.

Apesar de o referido código trazer de maneira tímida e setorial o início da regulação direcionada à proteção de dados pessoais no Brasil, essa primeira fase é importantíssima, pois se predispõe a estabelecer limites aos eventuais abusos decorrentes das relações de consumo.

Desse modo, parte dos conceitos basilares da Lei Geral de Proteção de Dados Pessoais já foi elencada pelo art. 43 do Código de Defesa do Consumidor, isto é, os princípios do livre acesso, da transparência, da qualidade dos dados e da adequação.

Assim, a título comparativo, podem-se relacionar alguns dispositivos do Código de Defesa do Consumidor e da LGPD a fim de demonstrar as primeiras previsões acerca do tema de proteção de dados, com as últimas previsões, que foram elencadas pela Lei n. 13.709/2018.

O art. 43, *caput*, do mesmo diploma dispõe que "o consumidor, (...) 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".

Nessa mesma linha, a LGPD, em seu art. 6º, inciso IV, prevê o princípio do livre acesso e da consulta facilitada sobre a "forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".

Já os §§§ 1º, 2º e 3º do art. 43 do referido código[16] estão previstos no art. 6º, incisos VI, V e II, da Lei n. 13.709/2018, isto é, a garantia da transparência, da relevância e do atendimento às adequações necessárias ao tratamento de dados.

Outro aspecto essencial é o trazido pelo § 2º do art. 43, também do Código de Defesa do Consumidor, o qual dispõe que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele". Assim, a proteção direcionada ao consumidor já previu, de certa forma, uma realidade com a qual a LGPD terá de lidar prontamente, qual seja, o dever de comunicação aliado à transparência e a política de registro dos dados pessoais.

Como será analisado em capítulo específico, o dever de comunicação daquele que é responsável por manipular os dados pessoais é um grande desafio regulatório para a Lei n. 13.709/18.

[16] Os §§§ 1º, 2º e 3º do art. 43 do Código de Defesa do Consumidor dispõem que "os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão", "o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção" e "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". Isto é, o Código de Defesa do Consumidor, enquanto primeiro instrumento normativo que previu a regulação do tratamento de dados, já tratou de conceitos caros à LGPD, quais sejam a transparência, a exatidão dos dados e a previsão de que não deve haver a sua utilização para finalidades daquelas que lhe foram imputadas inicialmente.

Isso porque o mencionado código foi previsto para tratar de responsáveis pontuais relacionados ao registro de novos dados pessoais de indivíduos na condição de consumidores e, na década de 1990, apenas iniciava-se o acesso à internet no Brasil. A LGPD, portanto, deverá regular o tratamento de um número infinitamente superior de dados, com possibilidades das mais variadas possíveis no que diz respeito à utilização dessas informações por agentes econômicos em um cenário em que a internet está a um clique de distância não apenas dos consumidores em potencial, mas também de crianças e até mesmo de indivíduos e grupos que nem sempre se enquadram nas relações de consumo e que ainda assim têm os seus dados pessoais tratados, especialmente aqueles ligados a temas delicados, como política, religião, saúde e vida sexual.

Ademais, registros de dados pessoais são feitos todos os dias por meio de várias plataformas, aplicativos e softwares diferentes que, muitas vezes, não observam, por exemplo, três, dos dez princípios previstos na Lei de Proteção de Dados.

Tais princípios, que possuem papel fundamental na busca pela especificação da coleta e do tratamento de dados para determinados fins e na eliminação de excessos, são assim delineados pela LGPD:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - **finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

A finalidade, entendida como a limitação da utilização dos dados coletados com objetivos específicos, mostra-se como uma forte ferramenta para se evitar o tratamento de dados pessoais com um propósito diferente daquele que originou a necessidade da sua utilização.

A adequação complementa o princípio supramencionado e reforça que o tratamento de dados pessoais deverá ser feito de acordo com os moldes informados ao titular. Nesse caso, é fácil perceber o desvio de finalidade e a ausência de adequação em muitos aplicativos oferecidos como, por exemplo, aplicativos indicadores de caminhos e trajetos que não apenas requerem a localização do usuário, mas também o acesso à sua rede de contatos, ou até mesmo aplicativos de bancos digitais que requerem o acesso ao microfone, à câmera e à localização do usuário.

Já o princípio da necessidade está ligado de maneira íntima ao princípio da finalidade, de modo que deverão ser coletados apenas aqueles dados necessários à realização de uma ou mais atividades pré-informadas aos titulares.

O Código Civil (Lei n. 10.406/02), em seu Capítulo II intitulado como "Dos Direitos da Personalidade", no art. 20, *caput*, preocupou-se em proibir a divulgação de escritos, a transmissão da palavra ou sua publicação, além da exposição ou a utilização da imagem de uma pessoa, caso lhe atinjam a honra, a boa fama ou a respeitabilidade, ou, ainda, se se destinarem a fins comerciais[17].

Nessa linha, Danilo Doneda[18] aponta que o Código Civil adota uma postura de proteção já considerando a hipótese de violação à privacidade e lida com a ocorrência do dano propriamente dito também por meio do art. 21.

De fato, tanto o art. 21[19], do referido código, quanto o art. 5º, inciso X[20] da Constituição da República, trazem à baila a possibilidade do ajuizamento de ações reparatórias no caso de haver violação à privacidade, de modo que a intimidade, a vida privada, a honra e a imagem do indivíduo são alvos de tutela do ordenamento.

Entretanto, analisando os artigos supramencionados no contexto da economia movida a dados (ou economia digital), a divulgação e a publicação de escritos, palavras e imagens das pessoas naturais se tornaram mais fáceis e rápidas para os responsáveis pelo tratamento de dados pessoais, e mais complexas e obscuras para os titulares desses dados, uma vez que, o *Big Data*[21], assim entendido como um volume colossal e veloz de dados, dificulta o controle de eventuais abusos tratados pelo art. 20, caput, do Código Civil.

Já a segunda fase relacionada ao tratamento de dados pessoais no Brasil é representada pela Lei do Cadastro Positivo (Lei n. 12.414/11), pela Lei de Acesso à Informação (Lei n.

---

17 Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais.

18 DONEDA, Danilo. *A tutela da privacidade no código civil de 2002.* Revista eletrônica do curso de direito. Centro Universitário UniOpet.

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

20 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;

21 (...) "We call this the problem of big data. When data sets do not fit in main memory (in core), or when they do not fit even on local disk, the most common solution is to acquire more resources." PRESS, Gil. *12 Big Data Definitions: what's yours?* FORBES, 2014. Disponível em https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#75a4dde313ae. Acesso em 01/05/2019.

12.527/11) e pelo Marco Civil da Internet (Lei n. 12.965/14) que, embora sejam normas setoriais, ampliam ainda mais conceitos como o consentimento e a finalidade, além de reforçarem a necessidade de uma política de transparência.

A Lei do Cadastro Positivo (Lei n. 12.414/11), por sua vez, também tratou de pontos de extrema relevância para a proteção de dados pessoais como a transparência, o livre acesso e a possibilidade de oposição do titular dos dados em relação à alguma informação que esteja errada (essa discussão é de extrema relevância quando se trata de decisões automatizadas e será abordada mais a frente).

Merece destaque o art. 3º, § 3º, inciso II, da Lei n. 12.414/11, que traz pela primeira vez a disposição mais clara a respeito das chamadas "informações sensíveis", que seriam aquelas relacionadas à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas dos indivíduos.

Nota-se, portanto, a preocupação do legislador que, intrinsecamente, aplicou os três princípios expostos anteriormente (finalidade, adequação e necessidade) para evitar danos e cenários discriminatórios, limitando-se à coleta de dados pessoais apenas para os fins da lei, o que não abarca, por óbvio, essas informações mais sensíveis.

Quanto à Lei de Acesso à Informação (Lei n. 12.527/11), ressalta-se o remédio constitucional *habeas data* previsto no art. 5º, inciso LXXII, da Constituição da República e na Lei n. 9.507/97, que regula o direito de acesso a informações e disciplina o *habeas data.*

Esse remédio constitucional se propõe a "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidade governamentais ou de caráter público", conforme art. 7º, inciso I, da Lei n. 9.507/97.

Danilo Doneda[22] elucida que o *habeas data* por si só não garante os direitos necessários na sociedade informacional, uma vez que sua atuação se restringe apenas ao direito de acesso, sem tutelar aspectos como o controle do armazenamento de informações, a utilização destas, a finalidade e até mesmo a reparação pelos danos eventualmente causados em decorrência da manipulação dessas informações que dizem respeito à pessoa natural.

Por fim, o Marco Civil da Internet, em seu art. 3º, inciso II previu a proteção da privacidade do indivíduo, agora usuário da internet. De forma mais específica, a Lei n. 12.965/14, em sua Seção II assim intitulada "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas" tratou de alguns aspectos caros à LGPD, especialmente no § 4º e

[22] DONEDA, Danilo. *A proteção de dados pessoais no ordenamento brasileiro e a ação de Habeas Data*. Rev. Democracia Digital e Governo Eletrônico. Universidade Federal de Santa Catarina, 2009, p. 128-142.

caput art. 10[23] e no § 3º e caput do art. 11[24], que abarcam a proteção à intimidade, à vida privada, à honra e à imagem do usuário de internet, e também repisam a importância da clareza das informações a serem prestadas pelo provedor da internet[25].

Ainda que as legislações mencionadas, até a edição da LGPD, sejam extremamente relevantes para assegurar aos titulares de dados uma mínima proteção, seja na condição de consumidor, de cidadão ou de usuário de internet, o Brasil carecia de uma normativa mais abrangente e incisiva para tutelar os dados das pessoas naturais, que fornecem suas informações diariamente às mais diversas plataformas, tanto na internet quanto fora dela.

Esse cenário regulatório novo e desafiador está abarcado não só pelo setor privado, mas também pelo público que, conforme a LGPD, também deverá se ajustar de acordo com os moldes normativos propostos.

Também a pressão internacional, mormente pela aprovação, em maio de 2018, da *California Consumer Privacy Act* (CCPA)[26] e do próprio *General Data Protection Regulation*, vigente na União Europeia desde maio de 2018, são grandes influenciadores que impulsionaram ainda mais o debate e a efetiva criação de uma lei mais abrangente e axiológica como a Lei Geral de Proteção de Dados.

1.3. O *General Data Protection Regulation* e a sua influência no cenário brasileiro

[23] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (...)
§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

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

[25] No caso do § 4º do art. 10, há a menção à "confidencialidade quanto a segredos empresariais". Na LGPD, tal previsão está no art. 6º, inciso VI, que, ao também tratar da transparência, dispõe sobre a observação dos segredos comercial e industrial. Inclusive, a Lei do Cadastro Positivo também prevê o segredo em seu art. 5º, inciso IV. Nesse ponto, os questionamentos que se levantam são: quais seriam os limites impostos por tais segredos? No caso de estes estarem conectados aos dados pessoais, o segredo comercial e industrial devem sempre ser respeitados mesmo à custa de uma eventual ausência de proteção efetiva dos titulares que forneceram os dados?

[26] SOMERS, Geert. BOGHAERT, Liesa. *The California Consumer privacy Act and The GDPR: two of a kind?* Expert briefin, Data privacy. Financier worldwide. Disponível em: https://www.financierworldwide.com/the-california-consumer-privacy-act-and-the-gdpr-two-of-a-kind#.XW2CuJNKh-U Acesso em: 02/09/2019.

No cenário europeu, o *General Data Protection Regulation* (GDPR) apresentou-se como uma forma de unificar e aplicar efetivamente os princípios e dispositivos que visam à tutela dos dados pessoais. Assim, um regulamento próprio como instrumento fixo que reduz as margens de manobra configurou-se como um verdadeiro salto europeu no que diz respeito à proteção de dados pessoais, conforme entende Yves Poullet[28].

O GDPR, como é chamado, buscou substituir a Diretiva 95/46/CE, criada pelo Parlamento Europeu e pelo Conselho da União Europeia, que tinha a incumbência de orientar as autoridades em assuntos relacionados à proteção de dados pessoais de indivíduos europeus pertencentes aos Estados-Membro da UE.

Desse modo, com a promessa de sanar a aplicação fragmentada e diminuir as interpretações divergentes proporcionadas pela Diretiva 95/46/CE, o GDPR fornece critérios que determinam o papel das autoridades de supervisão relacionado ao fluxo de dados entre as fronteiras e busca sanar divergências de interpretação entre as *Data Protection Authorities*.

A edição de um regulamento para substituir uma diretiva muda o foco principal da proteção de dados na Europa, pois, de acordo com Bruno Bioni e Laura Schertel[29], o GDPR possui como objetivo principal a criação de um regime jurídico mais uniforme e homogêneo, consoante dispõem os artigos 8 e 9, do GDPR.

Segundo Yves Poullet[30], o regulamento europeu amplia o alcance da proteção de dados pessoais e firma compromissos internacionais que buscam a garantia do direito dos europeus titulares desses dados.

Tudo isso porque a evolução da era digital exigiu que fosse adotada uma forma mais incisiva de regulamentação para a proteção de dados pessoais. O fluxo exacerbado de dados conferido pelo chamado *Big Data*, a rede de informações, as interações e conexões de dados, a chamada *cloud computing*, o desenvolvimento da inteligência artificial, da nano e da biotecnologia traduzem um cenário cada vez maior do que Yves Poullet chama de *transhumanism*[31], isto é, a fusão cada vez maior do cérebro humano, suas percepções, sensações e a sua própria cognição com os softwares.

---

[28] POULLET, Yves. *Is the general data protection regulation the solution?* Computer law & security review. Namur Digital Institute, University of Namur, Belgium, 2018, pp. 774-778.
[29] BIONI, Bruno R. SCHERTEL, Laura. *Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência.* In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, Revista dos Tribunais, 2019, p. 804.
[30] Op.cit., pp. 774-778.
[31] Op.cit., p. 774.

Nesse caso, conforme constatado pelo autor, a implementação do GDPR passa por dois cenários básicos. O primeiro seria a reciprocidade das vantagens, ou seja, os responsáveis pelo tratamento e pela utilização dos dados pessoais devem ter uma margem minimamente satisfatória à luz de uma perspectiva econômica e os titulares dos dados pessoais fornecidos devem não só exercer a figura de sujeito passivo, mas devem utilizar a própria tecnologia como forma de exercerem seus direitos previstos pelo GDPR, como o direito à clareza e à gestão do consentimento, o exercício da transparência, da finalidade e da adequação no tratamento dos seus dados, além de outros aspectos previstos pelo regulamento europeu[32].

O segundo cenário seria o que Yves Poullet chama de *privacy by design* ou até mesmo o *privacy by default*, que seria alinhar a proteção de dados pessoais ao centro da tecnologia, além de acompanhá-la desde o início do desenvolvimento dos softwares que irão compor aplicativos, chips, celulares e demais aparelhos, isto é, no "momento zero", desde a sua concepção. Isso evitaria que o GDPR fosse aplicado somente após a conclusão do projeto tecnológico, ou seja, no momento em que já estivesse à disposição do usuário.

Portanto, o *privacy by design* viabilizaria uma maior proteção das informações coletadas, pois estaria presente no âmago da produção de uma determinada tecnologia, ou seja, em sua fase de pré-constituição[33].

Para alcançar tais objetivos, Yves Poullet[34] destaca quatro ferramentas de eficácia propostas pelo GDPR: i) maior robustez em relação aos direitos dos titulares; ii) o *Compliance* como forma de autorregulação e promoção das normas a serem aplicadas nos ambientes internos das empresas que tratam dados pessoais; iii) a implementação de instrumentos regulatórios alternativos; e iv) a capacitação das chamadas *Data Protection Authorities* com novos métodos de coerção para que a perspectiva do *command and control* seja utilizada.

Parte-se, aqui, da afirmativa de que o GDPR e o contexto em que foi criado exerceram forte influência para a adoção de uma lei geral multisetorial de proteção a dados pessoais no Brasil, e, além disso, o GDPR cumpriu o papel de catalisador para a promulgação da lei brasileira.

Bruno Bioni e Laura Schertel destacam três aspectos importantes de convergência entre o GDPR e a Lei Geral de Proteção de Dados, Lei n. 13.709/2018, quais sejam, (i) os princípios

[32] Op.cit., p. 774-775.
[33] Op.cit., p. 774-775.
[34] Op.cit., p. 775.

em comum presentes nas duas normas; (ii) o modelo *ex-ante* de proteção; e (iii) o papel central da *accountability*.

Inicialmente, segundo os autores supramencionados, surgiu, na Alemanha, na Inglaterra e nos Estados Unidos da América, na década de 1970, uma espécie de quadro de princípios comuns, o chamado "*Fair Information Practice Principles*"[35].

Tais princípios, em suma, versavam sobre a transparência na coleta, no tratamento e no armazenamento de dados pessoais; o livre acesso do titular aos seus dados pessoais; a restrição da utilização daqueles dados à finalidade específica, de modo que, caso houvesse uma mudança de finalidade, o titular deveria fornecer novamente o seu consentimento; a possibilidade de correção das informações de um indivíduo[36]; a previsão da existência de uma limitação na coleta dos dados pessoais, de modo que não fossem colhidas informações em demasia; a facilidade que deve ter o indivíduo para acessar e tomar conhecimento de quais informações pessoais foram coletadas; e a previsão de um sistema de segurança capaz de detectar violações ao sistema que armazena os dados pessoais[37].

Ressalta-se que a base principiológica acima citada foi incorporada, à sua maneira, tanto no GDPR, quanto na LGPD que, ainda, incorporou os princípios da segurança, da prevenção e da não discriminação, de modo que este último é central para que não haja dano ao titular, tampouco a construção ou agravamento de preconceitos, consoante expõem Bruno Bioni e Laura Schertel[38]:

> Esses novos princípios previstos na LGPD evidenciam a preocupação da Lei com aspectos contemporâneos da proteção de dados e com novas demandas sociais, como o princípio da não discriminação pelo tratamento de dados, abordando o potencial discriminatório do uso de dados gerado por mecanismos de decisão automatizada, ou mesmo o princípio da prevenção – que pode ser utilizado para o desenvolvimento de medidas relacionadas à privacidade na concepção, como os conceitos de *Privacy by Design* e o *Security by Design*.

Inclusive, no que diz respeito às decisões automatizadas, tanto o GDPR quanto a LGPD resguardam a possibilidade de haver o direito à explicação, que deve ser fornecida pelo agente

---

[35] Op.cit., p. 806.
[36] U. S. Departiment of Health, Education and Wefare. *Report of the Secretary's Advisory Committe on Automated Personal Data Systems*, 1973. Disponível em: www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em 10/09/2019.
[37] BENNETT, Colin. *Regulating Privacy: data Protection and public policy in Europe and the United State.* Cornell University Press, Ithaca and London, 1992, pp. 98-99.
[38] Op.cit., p. 808.

manipulador dos dados ao titular, e a possibilidade de auditoria, se houver um potencial discriminatório no tratamento desses dados[39].

Nessa linha, destaca-se a Lei n. 13.853/2019, a qual tem origem na Medida Provisória n. 869/2018, que vetou a possibilidade anteriormente prevista no art. 20, da LGPD, de que o titular teria direito de solicitar a revisão, especialmente por pessoa natural, das decisões tomadas unicamente com base no tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões que definam o perfil pessoal, profissional, de consumo, de crédito ou, ainda, de características da personalidade do titular.

Com o veto, a revisão das decisões automatizadas poderá ser feita por um novo sistema algorítmico que, novamente, pode repetir eventuais danos e contextos discriminatórios gerados pela primeira decisão. Assim, foi retirada uma previsão de suma relevância, que atuaria como um dos instrumentos aptos a evitar a formação de cenários discriminatórios por meio do tratamento dos dados pessoais, especialmente os dados pessoais sensíveis.

Isso porque, ao retirar a exigência da revisão por uma pessoa natural, caso o algoritmo responsável pela decisão esteja eivado, em sua cadeia, de informações delicadas como aquelas que dizem respeito à origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, há a possibilidade de tal decisão causar graves prejuízos aos titulares desses dados pessoais, o que afronta o princípio da não discriminação cunhado pela LGPD em seu art. 6º, inciso IX.

O veto, inclusive, diverge da tutela conferida pelo GDPR nesse caso, que prevê em seu art. 22/1, "o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar".

Para além, outro ponto de convergência entre o GDPR e a LGPD, conforme esclarecem Bruno Bioni e Laura Schertel, configura-se pela racionalidade *ex-ante* de proteção, isto é, um modelo consolidado pelo GDPR que prevê, no art. 6º, os requisitos que tornam o tratamento de dados pessoais lícito, quais sejam, (i) o consentimento; (ii) a execução de um contrato; (iii) a obrigação jurídica; (iv) a defesa de interesses vitais; (v) o exercício de funções de interesse público; e (v) o legítimo interesse[40].

[39] BIONI, Bruno; SCHERTEL, Laura. Op.cit., p. 809.
[40] Op.cit., p. 810.

De acordo com os autores, "qualquer tratamento de dados acaba por influenciar a representação da pessoa na sociedade, podendo afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais"[41]. Assim, o referido modelo, que está amparado no tratamento de dados pessoais com base legal, tem como objetivo viabilizar o tratamento das informações pessoais dos titulares de forma lícita, amparada na boa-fé e em princípios que visam a resguardar e proteger os indivíduos.

Por fim, a terceira semelhança entre o GDPR e a LGPD, está na *accountability* como forma de "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas", consoante disposto no art. 6º/10, do GDPR.

O princípio da *accountability* será melhor esclarecido no capítulo quatro, subtópico 4.2.1.

1.4. Conceitos importantes elencados pela Lei Geral de Proteção de Dados Pessoais

Além dos princípios elencados no subtópico acima, que foram absorvidos pela Lei Geral de Proteção de Dados Pessoais, cabe mencionar alguns conceitos centrais introduzidos pela referida lei, que servirão para o entendimento das explanações que serão delineadas.

Primeiramente, segundo a Lei n. 13.709/2018, os titulares dos dados pessoais objeto de tutela são as pessoas naturais "a quem se referem os dados pessoais que são objetos de tratamento", ou seja, não são objetos de tutela as pessoas jurídicas, de direito público ou privado, que tenham os seus dados coletados, tratados e armazenados, assim como os dados que não são considerados pessoais, ainda que se refiram a uma pessoa natural.

A LGPD define o dado pessoal como toda "informação relacionada à pessoa natural identificada ou identificável", isto é, para que haja o alcance da norma, o titular dos dados pessoais deve ser conhecido ou potencialmente conhecido.

Por outro lado, o referido instrumento legislativo também dispõe sobre aquilo que não é considerado um dado pessoal e que, portanto, não sofre a incidência da lei, isto é, o dado anonimizado, que se caracteriza pela informação relativa a um "titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento".

[41] BIONI, Bruno; SCHERTEL, Laura. Op.cit., p. 811.

Ressalta-se que, para o GDPR, ainda há uma terceira classificação de dados, os chamados pseudonimizados, isto é, dados que foram descaracterizados, mas que podem ser utilizados para identificar novamente uma pessoa por meio de uma tecnologia empregada.

Outro conceito de suma relevância assentado pela LGPD foi a definição dos dados pessoais sensíveis, que possuem informações do titular a respeito da sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Contudo, ainda que a Lei n. 13.709/2018 tenha feito a distinção entre os dados pessoais sensíveis e os demais dados pessoais, para Ana Frazão, a depender da conjuntura fática, os demais dados pessoais podem se tornar dados pessoais sensíveis, pois "a linha distintiva entre dados pessoais e dados pessoais sensíveis pode não ser tão nítida, até porque a perspectiva de análise deve ser dinâmica e não estática" [42].

Dessa forma, os dados pessoais *lato sensu,* quais sejam, os dados pessoais *stricto sensu* mais os dados pessoais sensíveis, muitas vezes não estão isolados dos demais dados, o que dificulta a tutela a respeito dessas informações sensíveis.

O tratamento dessas informações pessoais, segundo o art. 5º, inciso X, da Lei Geral de Proteção de Dados, consiste em "toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração", isto é, para fins explicativos, a expressão "tratamento" abarca toda a cadeia supra que pode envolver inúmeras subetapas, a depender do tipo de dado, da sua utilização e do seu armazenamento.

Esses dados, que são coletados tanto no meio *on-line* quanto no meio *off-line*, têm como agentes responsáveis pelo seu tratamento, segundo a LGPD, duas figuras: (i) o controlador e (ii) o operador.

O controlador caracteriza-se por ser a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", enquanto o operador é a "pessoal natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", conforme dispõe o art. 5º, incisos VI e VII.

---

[42] FRAZÃO, Ana. *Nova LGPD: o tratamento de dados pessoais sensíveis.* JOTA, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 03/06/2019.

Nos artigos 37 a 40, a referida lei elenca algumas obrigações desses agentes, tais como, o dever de sigilo das informações pessoais tratadas, a possibilidade de elaboração de um relatório de impacto e a necessária atenção que deverá possuir o operador quanto ao tratamento dos dados pessoais segundo as instruções fornecidas pelo controlador, a fim de evitar eventuais desvios e excessos.

Outra figura relevante é a do encarregado, ou *Data Protection Officer*, que será melhor explanada no capítulo quatro. Essa figura, segundo o art. 5º, inciso VIII, da LGPD, constitui-se como uma "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD)".

A Lei Geral de Proteção de Dados ainda define outros conceitos caros à futura aplicação da lei, tais como o bloqueio e a eliminação dos dados pessoais, a transferência internacional de dados pessoais, a utilização destes de forma compartilhada, o órgão de pesquisa que atuará no desenvolvimento tecnológico relacionado ao tema e a definição do consentimento, do legítimo interesse e da própria autoridade nacional.

Definidos alguns dos conceitos principais elencados pela LGPD, mormente a definição de dados pessoais sensíveis, das figuras dos agentes responsáveis pelo tratamento de dados pessoais, isto é o controlador e o operador, bem como da definição da figura do encarregado, que deverá ser o vetor do tratamento de dados à adequação e conformidade traduzida pelas boas práticas de governança e pela atuação perante o agente regulatório, que foi instituído pela Lei n. 13.853/2019, passa-se a entrelaçar tais conceitos e a conectá-los à possibilidade de configuração de dano ou da construção de um cenário discriminatório por meio do tratamento de dados pessoais sensíveis.

Ademais, buscar-se-á indicar algumas ferramentas que viabilizarão a tutela dos dados pessoais e dos seus pressupostos, como a tutela da privacidade e a utilização de boas práticas como forma de obter resultados práticos e lícitos a respeito do tratamento de dados pessoais.

CAPÍTULO 2 – DA PRIVACIDADE À MANIPULAÇÃO DE PERFIS COMPORTAMENTAIS

2.1. O capitalismo de vigilância e a proteção da privacidade

Em um cenário transformador caracterizado pela era informacional, faz-se importante analisar o papel da privacidade e da proteção de dados para que haja um maior entendimento

sobre em que medida há uma apropriação da privacidade pelo indivíduo em uma sociedade que tem o tratamento de dados pessoais inseridos em sua espinha dorsal e de que modo agentes públicos e privados manipulam a realidade social e econômica de acordo com os seus interesses, sem que haja a devida transparência em relação aos usuários.

Essa manipulação, antes feita pela mídia televisiva e jornalística, ganha uma nova função, ainda mais forte, com o advento da internet. Assim, a capacidade de transmissão de informações, o que inclui os dados pessoais, tornou-se cada vez mais incisiva, potencialmente manipulável e que se alinhou aos interesses específicos de agentes que detinham e/ou detém as informações proporcionadas por esses dados.

Laura Schertel[43] elucida que, no cenário de *common law*, desde o surgimento de tecnologias tais como a fotografia e a imprensa, o reconhecimento da privacidade segundo o juiz McIntyre Cooley seria o "direito a ser deixado a só". Contudo, em uma sociedade movida a dados pessoais, esse conceito de privacidade se tornou insuficiente para abarcar a realidade.

Nesse contexto, Simson Garfinkel[44] entende que, em vez de se realizar um verdadeiro *trade-off* entre a privacidade e a tecnologia, deve-se analisar a perspectiva social com base no equilíbrio entre o desenvolvimento tecnológico, o que inclui o tratamento de dados pessoais e a preservação da privacidade.

De acordo com o matemático Clive Humby[45], o dado pessoal é o "novo petróleo", uma vez que possuem um potencial de comércio vasto ao influenciarem os hábitos dos consumidores, tendências de mercado e até mesmo seleções e juízos de valor com base em dados que dizem respeito à saúde, à religião, à origem étnica ou racial, à opinião política, à filiação sindical, à vida sexual à biometria, dentre outros.

Entretanto, há quem diga que o dado pessoal é, na realidade, o "novo poder nuclear", como é o caso do escritor James Bridle[46]. Isso porque os dados pessoais constituem uma valiosa mercadoria que, em contrapartida ao petróleo citado por Clive Humby, são ilimitados tanto sob o ponto de vista da quantidade quanto sob o ponto de vista da potencialidade para causar danos.

---

[43] SCHERTEL, Laura. *Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo*. Dissertação (Mestrado em direito), Faculdade de Direito, Universidade de Brasília. Brasília, 2008, p. 15.

[44] GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. O'Reilly Media: California, 2000, p. 5.

[45] ARTHUR, Charles. *Tech giants may be huge, but nothing matches big data: When Nasdaq stopped trading this week, it again showed how global firms are at the mercy os a power that created them.* The Guardian, 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em 12/07/2019.

[46] BRIDLE, James. Opinion: *Data isn't the new oil – it's the new nuclear power*. Ideas.Ted.Com, 2018. Disponível em: https://ideas.ted.com/opinion-data-isnt-the-new-oil-its-the-new-nuclear-power/. Acesso em 12/07/2019.

Esses danos são causados, pois a utilização desses dados, como elucida James Bridle, replicam as políticas racistas, sexistas e opressivas que outrora foram fixadas, uma vez que esses padrões já foram codificados na raiz dos algoritmos utilizados.

Tais padrões, segundo James Bridle, percorrem desde as relações sociais até a forma com a qual um consumidor escolhe um produto ou serviço em detrimento do outro, além da própria motivação da escolha. Inclusive, os padrões fixados por algoritmos conduzem a divisões na sociedade que classificam e promovem condutas fundamentalistas que agravam as desigualdades.

Nessa linha, Marcelo Pereira[47], ao analisar a privacidade sob a ótica da intimidade, elucida que "o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada das mesmas, podem revelar aspectos de sua personalidade".

Com base nessa revelação de traços importantes da personalidade, a atual sociedade de vigilância vai de encontro à noção de privacidade, de modo que não permite que o indivíduo exerça o controle sobre as suas informações pessoais. Isso porque, na maioria das vezes, os usuários sequer sabem quais os tipos de informações são coletados e qual a quantidade coletada, sejam dados referentes ao gosto musical, preferências em relação a um determinado produto ou serviço, dados de saúde, em que são atribuídas informações sobre eventuais doenças ou predisposição a desenvolvê-las, dentre outras informações.

Shoshana Zuboff[48] aponta que a economia movida a dados parte daquilo que chama de *extraction imperative*, em que há, na extração de dados pessoais dos usuários, um impulso incansável em suas operações que, na busca cada vez maior pela vigilância do comportamento dos usuários, coleta e trata diversas informações destes, tais como as suas buscas na internet, os e-mails, textos, fotos, sons, mensagens, vídeos, localização, padrões específicos de comunicação, atitudes dos usuários, preferências, interesses, suas emoções, se possuem alguma doença ou quais produtos e serviços que desejam adquirir.

Essa extração, como bem descreve a autora, exige o conhecimento e a posse do máximo de informação possível, de tal forma que os bens e os serviços se tornaram meros instrumentos utilizados pelo capitalismo de vigilância, que centraliza a sua atuação não mais no produto em si, como a venda de um carro ou na utilização de um mapa, mas no comportamento do indivíduo ao dirigir o carro e na interação dele com o mapa, que fornece a rota e as direções do destino solicitadas pelo usuário, mas, em troca, extrai informações sobre a residência dele, o local de

---

[47] PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet*. 2ª ed. Curitiba: Juruá Editora, 2004, p. 140.
[48] ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

trabalho, os horários em que costuma dirigir, se prevalece uma direção defensiva ou ofensiva e até mesmo indica caminhos tendenciosos, que não refletem necessariamente aqueles que possuem o menor tráfego ou a menor distância, mas aqueles que farão o usuário passar por determinado local ou loja.

Para se ter uma noção da carga de informação e do poder agregado ao capitalismo de vigilância por meio da coleta e do tratamento de dados pessoais, em 2015, foi realizado um estudo a respeito da extração de informações feitas pelo Google por meio da internet. Constatou-se que, entre 2012 e 2015, elevou-se pouco mais que o dobro o número de sites com 100 ou mais *cookies*[49], além de mais do que triplicar o número de *sites* que utilizam 150 ou mais *cookies.*

Ademais, concluiu-se que *sites* populares coletam mais de 6.000 *cookies*, dos quais 83% pertencem a terceiros que não estão relacionados à atividade fim do site visitado.[50] Nota-se, portanto, que a capacidade que tem o Google de rastrear usuários nesses sites é extraordinária e o acentuado nível de vigilância é impensável.

Shoshana Zuboff entende que esse tipo de vigilância é feito de forma descentralizada, de sorte que não haveria um *big brother*[51], mas sim um *big other*, modelo institucional onipresente que, ao atuar na rede, modifica e mercantiliza a experiência cotidiana com produtos, serviços, comunicação e outros aspectos a fim de estabelecer novas formas de geração de riqueza, ainda que tal atuação suprima a liberdade a ser garantida pelo Estado Democrático de Direito.

Segundo Bruce Schneier[52], essa vigilância descentralizada ocorre por meio dos inúmeros *little brothers*, isto é, os dispositivos, as redes sociais, as preferências e as interações que os indivíduos manifestam na internet e fora dela que, de forma escondida, coletam informações e vigiam o comportamento dos usuários.

---

[49] Cookies são alguns pequenos arquivos de texto que ficam gravados no dispositivo para serem recuperados posteriormente pelo *site*. Tal ferramenta permite que um processador relembre informações acerca da atividade do usuário. BBC News Brasil. *O que acontece quando você aceita os cookies de um site e por que é bom apaga-los de tempos em tempos*. [S.I.], 2017. Disponível em: https://www.bbc.com/portuguese/geral-40730996. Acesso em 01/08/2019.

[50] IBRAHIM, Altaweel; GOOD, Nathan; HOOFNAGLE, Chris Jay. *Web Privacy Census*. SSRN scholarly paper, Social Science Research Network, Decemb. 2015. Disponível em: https://papers.ssrn.com/abstract=2703814. Acesso em 04/05/2019.

[51] ZUBOFF, Shoshana. *The age of surveillance capitalism. The fight for a human future at the new frontier of power*. New York: Public Affairs, 2019, p. 20.

[52] SCHNEIER, Bruce. *Data and Goliath. The hidden battles to collect your data and control your world.* New York: W.W. Norton & Company, 2015, p. 57.

Um exemplo da constante vigilância a que os indivíduos e a sociedade estão submetidos, está o teste recente feito pelo aplicativo de *streaming* que oferta filmes e séries, Netflix, o qual passou a notificar alguns usuários acerca da necessidade do consentimento para que o aplicativo pudesse reconhecer e acompanhar as atividades físicas praticadas pelos usuários[53].

Ainda que o serviço ofertado pelo aplicativo não se relacione com exercícios e atividade física, a justificativa para a adoção da nova função foi a de que a plataforma estuda novas ferramentas para melhorar a qualidade de reprodução dos filmes e das séries no exato momento em que um usuário pratica algum exercício físico.

O capitalismo de vigilância também exerce a sua influência por meio da ameaça da invisibilidade nas redes sociais. Isto é, os usuários têm de aderir a certas lógicas da plataforma para, em troca, receberem visibilidade.

A existência dessa visibilidade coaduna-se com aquilo que Hannah Arendt[54] chamou de autoexposição, em que o indivíduo emite receptores para que outros indivíduos o reconheçam. A noção de "aparecer" está relacionada à existência do ser e de sua liberdade. Para a autora, a autoexposição é inerente ao fato de estar vivo e o indivíduo alcança a sua plena dignidade quando "aparece" para a sociedade por meio das suas ações, gestos e palavras:

> (...) nossa certeza de que o que percebemos tem uma existência independente do ato de perceber, depende inteiramente do fato de que o objeto aparece também para os outros e de que por eles é reconhecido. Sem esse reconhecimento tácito dos outros, não seríamos capazes nem mesmo de ter fé no modo pelo qual aparecemos para nós mesmos (2000, p. 37).

Ocorre que, em uma sociedade movida a dados, a aparência deixou de ser apenas uma percepção de outros seres humanos em relação a um indivíduo específico.

Com a aderência das pessoas naturais às redes sociais e por meio do conteúdo oriundo das suas postagens, repostagens e das suas interações na internet, esse reconhecimento, que Hannah Arendt define como tácito, passou a ser também expresso. Assim, os usuários passaram a se expor de forma excessiva na internet, o que alimenta exponencialmente a rede algorítmica e a base de dados das plataformas desses aplicativos.

---

[53] BROWN, Dalvin. *People watch Netflix while 'on the go' and the company reportedly wants that data.* USA TODAY, 2019. Disponível em: https://www.usatoday.com/story/tech/2019/08/01/why-does-netflix-app-want-access-your-physical-activity/1887032001/. Acesso em 04/09/2019.

[54] ARENDT, Hannah. *A vida do espírito.* Tradução de Antônio Abranches, Cesar Augusto R. de Almeida e Helena Martins Ed. 4ª. Rio de Janeiro: Editora Relume Dumará, 2000, p. 37.

Tais redes algorítmicas se utilizam do grande volume de dados e de informações que os usuários inserem e fornecem para modelar o próprio reconhecimento desses indivíduos e modificar a forma com que estes se auto reconhecem e se auto expõem.

Sob o prisma da vigilância, os algoritmos podem acessar algumas dimensões ocultas, as quais podem gerar padrões que classificam e segregam indivíduos e grupos sociais, de modo que padrões preconceituosos e intolerantes são reproduzidos.

Atualmente, portanto, o reconhecimento estudado por Hannah Arendt com aplicação na vida pública tornou-se muito mais incisivo, e o que a autora chama de "fé no modo pelo qual aparecemos para nós mesmos" se expressa, em tempos de era digital, de forma distorcida e tendenciosa, uma vez que a realidade da autoexposição atual se insere em todo o contexto potencialmente manipulador de uma economia movida a dados.

Esse contexto requer, portanto, um viés protetivo capaz de lidar com as mudanças trazidas por esse novo tipo de economia.

2.2. A proteção de dados como um direito fundamental

Visto como um direito fundamental que deve ser objeto de tutela, a proteção de dados está relacionada de maneira íntima à proteção não apenas da privacidade, mas também da liberdade e do desenvolvimento da pessoa natural. Stefano Rodotà[55] esclarece que a sociedade vive, atualmente, a reinvenção da proteção de dados e da gestão da informação, de modo que o tema deve ser visto como um direito fundamental autônomo:

> (...) a proteção de dados contribui para a "constitucionalização da pessoa" – o que pode ser considerado como uma das mais significativas conquistas, e não apenas da Carta. Estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio (2008, p. 17).

George Marmelstein[56] entende que os direitos fundamentais são essenciais para a existência de uma vida digna e, além disso, possuem um profundo conteúdo ético. Essas garantias estão ligadas à noção de limitação do poder e do fomento da dignidade da pessoa humana, que formam a base axiológica dos direitos fundamentais. Assim, o autor elenca quatro

[55] RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância: a Privacidade Hoje*. Tradução de Danilo Doneda e Laura Cabral Doneda. Rio: Renovar, 2008, p. 17.
[56] MARMELSTEIN, George. *Curso de Direitos Fundamentais*. São Paulo: Atlas, 2008, pp. 18-19.

atributos básicos da dignidade humana, quais sejam, (i) o respeito à autonomia da vontade; (ii) o respeito à integridade física e moral da pessoa; (iii) a não-coisificação do ser humano e (iv) a garantia do mínimo existencial.

Inicialmente, o princípio da autonomia da vontade se fundamenta na possibilidade que tem o indivíduo de fazer escolhas existenciais e morais que são capazes de promover o desenvolvimento da sua personalidade. Desse modo, é estritamente necessário que o Poder Público assegure as premissas mínimas para que o indivíduo possa se autodeterminar.

Esse desenvolvimento livre da personalidade do indivíduo foi levado em consideração pelo Tribunal Constitucional Federal alemão que, em 25 de março de 1982, julgou a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho"[57], oportunidade em que o referido tribunal assentou o conceito do livre controle do indivíduo sobre o fluxo de suas informações.

Ao apreciar a constitucionalidade da referida lei, o tribunal reconheceu a existência de um direito à autodeterminação informativa que fixou, a partir de então, critérios legais para o tratamento de dados pessoais na Alemanha.

Tais critérios são preciosos, pois o processamento de dados, de acordo com Laura Schertel[58], ameaça a personalidade do indivíduo, uma vez que possibilita a coleta e o armazenamento ilimitado de dados, além de viabilizar combinações que formam perfis e verdadeiros raios-x do indivíduo, sem que este possua conhecimento ou ingerência.

Desse modo, a autora aponta que o reconhecimento da autodeterminação informativa pela Corte alemã é pautado na ideia de "livre desenvolvimento da personalidade, segundo o qual, o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade"[59].

O referido tribunal também reconheceu como constitucionais os princípios da exatidão e da finalidade do uso de dados pessoais[60], além da noção de que a coleta deve se ater ao mínimo necessário para atingir a sua finalidade que, inclusive, deve estar clara ao usuário.

---

[57] A Lei do Recenseamento de População, Profissão, Moradia e Trabalho previa a coleta dos dados a respeito da profissão, da residência e do local de trabalho de cidadãos para que o Poder Público cruzasse esses dados e tivesse informações a respeito do crescimento e da distribuição da população no país, além de obter um panorama sobre as atividades econômicas realizadas no território. (SCHERTEL, 2008, p. 46).

[58] Op.cit., p. 47.

[59] Op.cit., p. 47.

[60] A LGPD foi inspirada nos princípios da finalidade, da adequação e da coleta e tratamento do mínimo necessário no que diz respeito aos dados pessoais.

Esse direito foi, inclusive, inserido pela Lei n. 13.709/2018[61] como um dos fundamentos basilares da proteção de dados pessoais no país. Assim, o legislador, ao importar o conceito, reconheceu a autodeterminação informativa como um direito subjetivo fundamental que figura o indivíduo como protagonista no processo do tratamento dos seus próprios dados pessoais, segundo Laura Schertel[62].

Em relação ao respeito à integridade física e moral da pessoa, além da ausência de patologias, os valores interligados à individualidade do ser humano também são essenciais ao desenvolvimento da personalidade, como o sentimento, a vontade, a igualdade e a segurança[63].

Nessa linha, José Camargo afirma que existem os direitos extrínsecos à personalidade, em que são tutelados o corpo, a imagem e a voz; e os direitos intrínsecos à personalidade, que abrangem os aspectos psíquicos, tais como as emoções e a inteligência[64]. Nota-se, portanto, que o tratamento de dados pessoais sensíveis abarca tanto os direitos extrínsecos quanto os intrínsecos, uma vez que dados a respeito do corpo, da imagem e da voz de um indivíduo são informações biométricas expressamente tuteladas pela LGPD e, no que diz respeito às emoções e à inteligência, determinados valores agregados, os posicionamentos político, cultural, religioso e filosófico também são objetos de tutela da lei.

As emoções, a inteligência, esses dados biométricos e até mesmo a vontade de um indivíduo servem de substrato para que os agentes manipuladores de dados pessoais passem a criar perfis que definirão o comportamento dos usuários ou passem a classificar determinadas pessoas ou grupos, o que, por conseguinte, leva à discriminação destes.

O registro e a manipulação dessas emoções por meio da interação em redes sociais ou de pesquisas em sites de busca podem, inclusive, refletir e propagar a intolerância de usuários a respeito de um tema como, por exemplo, o futebol, em que o chamado "Torcedor Artificial", um algoritmo que simula o comportamento dos torcedores, interage de acordo com as informações coletadas digitalmente[65].

---

[61] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...) II – a autodeterminação informativa.

[62] Op.cit., p. 48.

[63] LEITE, Rita de Cássia Curvo. *Transplantes de órgãos e tecidos e dos direitos da personalidade.* São Paulo: Juarez de Oliveira, 2000, p. 157.

[64] CAMARGO, José A. *O direito à integridade psicofísica nos direitos brasileiro e comparado.* Revista da Seção Judiciária do Rio de Janeiro, Rio de Janeiro, n. 26, 2009, p. 272.

[65] O algoritmo "Torcedor Artificial" foi criado pela cerveja Amstel após a realização de um estudo pelo Google em que restou demonstrado que o número de pesquisa acerca de temas relacionados à violência e futebol brasileiro cresceu mais de 30% entre 2018 e 2019. As primeiras interações entre a inteligência artificial e os torcedores revelou o esperado: o "Torcedor Artificial" se tornou agressivo, intolerante e que não expõe o espírito esportivo. Contudo, após esses resultados, a Amstel passou a convidar os internautas para interagirem amistosamente a fim de fomentar uma política mais amigável fora de campo. Máquina do esporte. *Por "comportamento on-line",*

A respeito da não-coisificação do ser humano, a economia digital tende a falhar. Isso porque, conforme explana Ana Frazão[66], com a crescente utilização do *Big Data*, do *Big Analytics* e da mineração desses dados, a "tarefa de obter, coletar, registrar e acessar dados" tornou-se muito mais eficiente, por agregarem mais veracidade, velocidade, variedade e volume ao tratamento de dados.

Dessa forma, o indivíduo tem se tornado cada vez mais o próprio produto, isto é, o alvo no qual os agentes econômicos direcionam as suas ações a fim de obterem subsídios – os dados coletados – para ofertarem outros bens e serviços.

Tal prática vai de encontro ao real significado de garantia fundamental, por violar frontalmente a dignidade humana e tornar o indivíduo uma coisa, um produto explorado para obter toda a sorte de informações a seu respeito.

Quanto ao mínimo existencial, consoante aponta Stefan Gosepath[67], tal garantia evidencia-se na medida em que o indivíduo passa a viver de forma digna, autodeterminada e livre, de sorte que, além do "mínimo vital", deve haver o mínimo de qualidade de vida, que fará com que o indivíduo exerça a sua liberdade individual perante a sociedade.

No plano da proteção de dados pessoais, a garantia do mínimo de qualidade de vida se relaciona com o princípio da liberdade que deve ser assegurado ao indivíduo para que este possa realizar escolhas de acordo com a sua própria manifestação de vontade e, ainda, segundo os parâmetros que considere mais adequados, ao contrário do modelo que a economia movida a dados propõe, qual seja um modelo tendencioso e pré-estabelecido, que padroniza as ações, condiciona as escolhas dos usuários e mitiga as suas próprias vontades.

Isso tudo sem contar a inclinação preditiva que refletirá sobre a vontade e a escolha de um indivíduo, vez que as opções apresentadas pelo algoritmo ou pelo dispositivo são previamente selecionadas pelo agente que disponibiliza o bem ou o serviço.

A Constituição da República não adotou um rol taxativo de direitos fundamentais, de modo que a interpretação conjunta do art. 1º, inciso III e do art. 5º, § 2º, da referida Constituição, abre margem para a inserção de outras garantias individuais que estejam atreladas à dignidade da pessoa humana. Isso é importante para o tema da proteção de dados pessoais no Brasil, pois,

---

Amstel cria "Torcedor Artificial": em parceira com o Google, marca pretende impactar torcidas de forma positiva. [S.I.], 2019. Disponível em: https://maquinadoesporte.uol.com.br/artigo/por-comportamento-line-amstel-cria-torcedor-artificial_38056.html. Acesso em 03/09/2019.

[66] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais* e suas repercussões no Direito Brasileiro. 1. Ed. Brasil: RT – Revista dos Tribunais, 2019, pp. 24-25.

[67] GOSEPATH, Stefan. *Uma pretensão de direito humano à proteção fundamental*. Tradução de Cláudia Toledo e Bráulio Borges Barreiros. In: TOLEDO, Cláudia (Org.). Direitos Sociais em debate. Rio de Janeiro: Elsevier, 2013, pp. 79-80.

conforme elucida David Pardo[68], "os direitos fundamentais não se esgotam naqueles direitos reconhecidos no momento constituinte originário, mas estão submetidos a um permanente processo de expansão".

Essa ideia de expansão se aplica às atuais transformações promovidas pela Quarta Revolução Industrial que, segundo Klaus Schwab[69], cria um mundo no qual sistemas físicos e virtuais cooperam entre si de maneira flexível e proporcionam a personalização de bens e serviços, além da criação de novos modelos operacionais.

Essa personalização é promovida pelos agentes econômicos por intermédio da utilização de dados pessoais e enseja a discussão a respeito da existência dos quatro atributos básicos da dignidade humana elencados por George Marmelstein[70] na regulação a respeito do tratamento de dados pessoais no Brasil.

Nesse ensejo, com a finalidade de robustecer ainda mais a proteção de dados pessoais e conferir *status* constitucional ao tema, o Senado Federal apresentou, no dia 12 de março de 2019, a Proposta de Emenda à Constituição n. 17/2019[71], que visa à inserção do inciso XII-A ao art. 5º, e do inciso XXX ao art. 22, ambos da Constituição da República. Assim, a PEC n. 17/2019 pretende incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e também pretende fixar a competência da União para legislar sobre o tema.

A constitucionalização do direito à proteção de dados pessoais configura-se, portanto, como uma forma de direcionar a atuação do Poder Judiciário e da Administração Pública e evitar abusos. Assim, caso o *status* constitucional à proteção de dados pessoais seja efetivado, cumprir-se-á principalmente a dimensão objetiva dos direitos fundamentais, assim entendida por Dirley Júnior[72].

2.3. A utilização dos algoritmos e as decisões automatizadas

[68] PARDO, David Wilson de Abreu. *Direitos fundamentais não-enumerados: justificação e aplicação*. Tese (Doutorado em Direito). Faculdade de Direito, Universidade Federal de Santa Catarina. Florianópolis, 2005, p. 12.
[69] SCHWAB, Klaus. *The Fourth Industrial Revolution.* World Economic Forum. Currency. 2017, pp. 7-8.
[70] Op.cit., pp. 18-19.
[71]Proposta de Emenda à Constituição n. 17/2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em 03/09/2019.
[72] Dirley Júnior entende que a moderna teoria dos direitos fundamentais reconhece uma dupla dimensão dessas garantias fundamentais, quais sejam, a dimensão subjetiva, essencial à proteção da pessoa e que lida com situações concretas de violações, e a dimensão objetiva, que impõe limites objetivos ao poder e direciona a sua atuação. (2015, p. 508).

Frank Pasquale entende que, por meio da utilização dos dados pessoais, os agentes responsáveis pelo tratamento possuem um conhecimento sem precedentes das minúcias da vida diária dos indivíduos e, em contrapartida, estes pouco ou nada sabem sobre como essas informações são utilizadas para influenciar a tomada de decisões importantes, o que contribui para a criação do que o autor chama de *one way mirror.*[73]

O autor expõe que, por meio da manipulação dos algoritmos e das suas decisões, *players* decidem sobre a distribuição de benefícios à sociedade como a concessão de crédito com juros baixos, o que faz com que as oportunidades oferecidas não sejam alocadas de maneira justa e satisfatória[74].

Essas decisões algorítmicas revestidas de opacidade, segundo Frank Pasquale, permitem que controladores e operadores encubram juízos de valor contestáveis, perigosos e até mesmo preconceituosos, de modo que cada vez mais há uma demanda por modelos matemáticos que projetam, reformulam e inclinam pressupostos e conclusões a respeito de temas como o valor do produto, do serviço ou do próprio trabalhador. Assim, as decisões orientadas pelo *Big Data* exercem não apenas poder sobre as coisas, mas sobre as pessoas[75].

Ainda sob o prisma da opacidade que reveste as decisões algorítmicas, Frank Pasquale[76] entende que cada vez mais a sociedade atual é governada pelo que Jeff Connaughton chamou de *The Blob*, ou seja, uma rede sombria de agentes que mobilizam dinheiro e informação a fim de obter vantagens tanto para agentes econômicos quanto para os governos.

Esse cenário obscuro, inclusive, forma um paradigma paradoxal com a sociedade de vigilância, uma vez que agentes de tratamento e titulares possuem um grande desequilíbrio no acesso às informações e ao tratamento desses dados pessoais.

A invisibilidade do poder contida nos algoritmos é efetiva para quem os controla e perigosa para quem se tornou alvo de suas ações. Dessa forma, softwares que funcionam a partir de predições fixadas e com base no aprendizado, isto é, o *machine learning*, podem representar ameaças a valores, a instituições e a direitos caros à sociedade, tal como a própria democracia, conforme expõe Itamar Veiga[77].

---

[73] PASQUALE, Frank. *The Black Box Society*. Harvard University Press. Cambridge, Massachusetts. London, England. 2015, pp. 9-10.
[74] Op.cit., p. 10.
[75] Op.cit., p. 10.
[76] Op.cit., pp. 9-10.
[77] VEIGA, Itamar Soares. *Democracia e Tecnologia: nos caminhos do ator não social.* Supere Aude, Belo Horizonte, v. 9, n. 17, 2018, p. 16, 26-27.

Essa predominância algorítmica está presente nas democracias existentes e pode funcionar como uma forma de direcionar ou manipular as ações daqueles que Itamar Veiga chama de "atores não sociais", quais sejam, os indivíduos.

De maneira prática, Itamar Veiga aponta dois procedimentos utilizados em relação a esses atores: (i) a coleta de dados e (ii) o direcionamento do foco, da atenção e da ação dos atores. Assim, os agentes que possuem essas informações e as ferramentas necessárias à manipulação criam um cenário potencialmente ameaçador ao desenvolvimento do sujeito enquanto um ator não social.

O primeiro passo é a captura de informações, que podem ser mineradas e utilizadas para fins de direcionamento e padronização política (incluem-se os dados pessoais sensíveis tratados pela Lei n. 13.709/2018 em seu art. 5º, inciso II). Após essa captura, a manipulação pode ser feita na rede por meio dos "robôs sociais", softwares que estimulam discórdias e polêmicas entre os usuários a fim de alcançarem um determinado objetivo inicial. Segundo Itamar Veiga, esses algoritmos se projetam como perfis e fazem inúmeras postagens em um curto período de tempo.[78]

Os algoritmos, portanto, proporcionaram uma forma de ingerência e manipulação de cenários estruturais no que diz respeito à manutenção da democracia, de tal forma que, diferentemente do século passado, em que surgiram ideias as quais contribuíram para a formação de regimes totalitários por meio de discursos expressivos e claros, o direcionamento e a manipulação da opinião pública é feita agora por agentes "invisíveis", os quais escondem a sua verdadeira atuação que, consequentemente, é ignorada pelos indivíduos.

Essa possibilidade de manipulação fica clara com a análise da utilização desses dados para fins eleitorais feita pela empresa de *machine learning*, a *Cambridge Analytica* que, segundo investigações jornalísticas do *The Guardian* e do *The New York Times*, coletou milhões de perfis de eleitores dos Estados Unidos da América na rede social *Facebook*, de modo que tais dados foram utilizados para se criar um poderoso programa de software que previu e influenciou a escolha nas urnas das eleições presidenciais dos Estados Unidos da América, em 2016.

[78] Op.cit., pp. 16, 26-27.

Tais dados, de acordo com o *The Guardian*[79], foram coletados sem a autorização dos usuários, no início de 2014, para viabilizar a construção de um sistema de perfilização dos eleitores e direcioná-los a um conteúdo eleitoral personalizado.

Nas palavras ditas ao *Observer*, Christopher Wylie, que trabalhou junto a um acadêmico da *Cambridge University* para obter os dados dos titulares alvos da ação, fez a seguinte afirmação: "*we exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on*".

Isto é, a exploração e a manipulação de dados pessoais e das decisões algorítmicas baseadas nesses dados, segundo as investigações do *The Guardian*, mostraram-se decisivas para o resultado das eleições presidenciais dos EUA, em 2016.

Ana Frazão[80] esclarece bem que a predição[81] e os julgamentos feitos por decisões algorítmicas classificam, perfilizam e desconsideram a individualidade do ser humano, além de resultarem uma diferenciação de tratamento que pode marginalizar alguns indivíduos.

Acerca dos resultados produzidos pelas decisões algorítmicas, a autora ressalta:

> (...) os algoritmos preocupam tanto quando acertam como quando erram. Preocupam quando acertam, pois podem revelar aspectos íntimos da nossa personalidade que gostaríamos de manter em segredo, até porque podem ser utilizados para nos tolher o exercício de direitos e oportunidades. Preocupam quando erram, pois desconfiguram a nossa individualidade, atribuindo-nos características que não temos e que também podem ser utilizadas para nos tolher direitos e oportunidades, com o agravante de que tais decisões são baseadas em juízos totalmente equivocados (2019, pp. 34-35).

O resultado dos processos decisórios de algoritmos já foi capaz de identificar a orientação sexual de uma pessoa por meio da análise de um tipo de dado pessoal sensível, o biométrico. A pesquisa indica que o algoritmo utilizado tem a capacidade de quantificar em até 81% a precisão acerca da orientação sexual de alguém por meio da análise de apenas uma foto de uma pessoa[82].

Ora, a partir da utilização de sistemas que, por meio de inteligência artificial, ditam comportamentos e elaboram predições capazes de interferir no âmago da pessoa, em sua

---

[79] CADWALLADR, Carole; HARRISON, Emma Graham. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 20/08/2019.

[80] Op.cit., pp. 35-36.

[81] Ana Frazão explana que, com base nos dados, a inteligência artificial atua para construir predições, considerada o "*input* central para os processos decisórios" (2019, p. 33).

[82] WANG, Yilun. KOSINSKI, Michal. *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.* Journal of Personality and Social Psychology, 2017, p. 16.

personalidade, suas convicções, gostos, preferências, opiniões e outros aspectos sensíveis, os agentes responsáveis por elaborarem as diretrizes do algoritmo poderão agravar situações que já são bastante desconfortáveis para indivíduos e grupos da sociedade, como é o caso dos homossexuais que se submetem ao algoritmo descrito acima.

As decisões tomadas por algoritmos, portanto, podem prejudicar e levar a resultados que podem refletir de maneira muitas vezes irreversível, causando dano ao titular que submeteu seus dados a determinado algoritmo, que pode ser tendencioso.

Os algoritmos, segundo Cathy O'Neil[83], são instrumentos por meio dos quais as opiniões dos seus criadores, sejam diretos ou indiretos, são embutidas. Isto é, o modelo criado por um algoritmo nada mais é que a opinião de alguém disfarçada na matemática capaz de criá-lo.

A autora cita a aplicação de modelos algoritmos no mercado financeiro, por exemplo, em que se descobre um padrão tido como uma anomalia. Após, reúne-se o grande volume de dados coletados e se treina um algoritmo que seja capaz de prever recorrentemente essa anomalia, como a oscilação de 50 centavos. Assim, a pessoa natural ou jurídica que tiver posse desse tipo de padrão pode lucrar muito, até que a anomalia se encerre ou até que o restante do mercado também entenda tal padrão[84].

Cathy O'Neil afirma que uma fórmula matemática pode ser inócua na teoria, mas, caso seja colocada em prática, pode se tornar um padrão nacional ou global, que cria a sua própria economia distorcida[85].

Outro aspecto importante e que cabe mencionar a respeito dos algoritmos é o princípio da confiança, que norteia a sociedade democrática e estabelece um vínculo essencial entre o governante e os governados, e que pode ser abalado ou reforçado de maneira estrutural em temas que envolvam a adoção de decisões automatizadas. Assim, caso esses algoritmos sejam utilizados de modo a reforçar caminhos democráticos, haverá a promoção de uma *better society*.

Contudo, se esse princípio é maculado por meio de governos repressivos, funcionários públicos dotados de más intenções ou se até mesmo a segurança da informação, que deve ser garantida pelo Estado, é enfraquecida, o que facilita a ação de *hackers*, os algoritmos podem se tornar mecanismos de vigilância que possuirão o escopo de limitar o exercício democrático

[83] O'NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* B\D\W\Y, Broadway Books, New York, 2016.
[84] Op.cit., pp. 34-35.
[85] Op.cit., pp. 47-48.

pleno. Por isso, como ressaltam Marijn Janssen e George Kuk[86] e conforme dito anteriormente, a *accountability* e a *transparency* são fundamentos importantes a serem utilizados no que diz respeito ao processamento de dados.

A governabilidade algorítmica dotada de *accountability* e *transparency*, portanto, mostra-se cada vez mais necessária, pois, nesse cenário, os cidadãos fornecem seus dados pessoais e, em troca, o governo deve tratar tais informações da melhor forma mais lícita e útil às finalidades que lhe foram conferidas.

Isso não exclui a possibilidade de o cidadão se envolver na discussão sobre as condutas algorítmicas, isto é, para a ocorrência de um exercício democrático minimamente equilibrado, a coleta, o tratamento e o armazenamento dessas informações pessoais não devem ser feitas de forma unilateral, em que os cidadãos não possuem qualquer ingerência ou compreensão real do tratamento dos seus dados e das decisões algorítmicas tomadas com base nesses dados.

Para viabilizar essa governabilidade, Marijn Janssen e George Kuk[87] propõem uma democratização dos algoritmos para que a maior gama de profissionais especializados possa contribuir com o desenvolvimento de softwares que ampliem soluções técnicas e divulguem potenciais decisões propostas por algoritmos da forma mais socialmente favorável possível.

Tal democratização passaria, portanto, por dois caminhos básicos, quais sejam (i) estabelecer rotas inclusivas e economicamente inteligentes e (ii) criar pontos de contato entre os cidadãos comuns e os profissionais engajados a fim de que haja o aumento do fluxo de conhecimento, o que, por conseguinte, iria diminuir o que os autores chamam de *a hidden and authoritarian enforcement of power*[88].

Desse modo, ao incluir o indivíduo enquanto titular dos dados pessoais coletados e enquanto agente não apenas passivo, mas também ativo das decisões tomadas por algoritmos, a geração de um fluxo de informações e de conhecimento diminuirá, aos poucos, a opacidade naturalmente presente nos algoritmos e em suas decisões e, por conseguinte, diminuirá o risco de se gerar dano ou de se criar cenários de discriminação entre indivíduos ou grupos sociais.

---

[86] JANSSEN, Marijn; KUK, George. *The challenges and limits of big data algorithms in technocratic governance.* Government Information Quarterly 33. Delft University of Technology, The Netherlands and Nottingham Trent University, UK article, 2016, p. 372.

[87] Op.cit., pp. 373-374.

[88] Para Marijn Janssen e George Kuk, essa imposição oculta e autoritária de poder gera a passividade dos cidadãos para aqueles modelos que lhes são impostos, o que retira a "rota proprietária" dos cidadãos em relação aos seus dados. Op.cit., p. 374.

2.4. A formação e a utilização dos perfis de comportamento

Roger Clarke define a técnica de *profiling*, ou perfilização, como aquela em que há um conjunto de características de um grupo específico de pessoas, de modo que tais características são constatadas a partir de experiências e interações anteriores, as quais são armazenadas e pesquisadas, posteriormente, por indivíduos perfeitamente ajustados a esse conjunto[89].

De acordo com Mireille Hildebrant[90], conforme citado por Rafael Zanatta[91], existem três tipos de perfilização, quais sejam, (i) a perfilização orgânica, que consiste no reconhecimento de padrões gerados por seres animados e vivos; (ii) a perfilização humana, que se trata da capacidade que tem o ser humano para construir padrões que funcionem no momento anterior à ação; e (iii) a perfilização automatizada, que atua por meio de máquinas ou dispositivos pré-programados para gerar conexões mais complexas e inesperadas em massa por meio de dados agregados.

Nesse último caso, para Mireille Hildebrant e conforme bem explana Rafael Zanatta, a mineração de dados tem papel importante e envolve seis etapas, quais sejam, (i) o registro dos dados e do seu conteúdo; (ii) a agregação e o monitoramento dessas informações; (iii) a identificação da existência de algum padrão contido nos dados coletados; (iv) a interpretação, a partir desses padrões, de resultados úteis; (v) o monitoramento dessas informações para averiguar resultados; e finalmente, (vi) a aplicação e a utilização desses perfis que foram formados[92].

Inclusive, em um cenário de coleta e tratamento massivos de dados pessoais, a perfilização é o instrumento pelo qual é formado, segundo Mireille Hildebrant, "um link entre uma overdose de dados triviais sobre nossos movimentos, temperatura e interação com outras pessoas e coisas e um conhecimento aplicável sobre nossos hábitos, preferências e o estado do ambiente" (*apud* ZANATTA, 2019, p. 5).

A respeito do tema, o *General Data Protection Regulation* define o *profiling* da seguinte forma:

> (4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural

[89] CLARKE, Roger. *Profiling: a hidden challenge to the Regulation of data surveillance.* Journal of Law & Information Science, v. 4, 1993, p. 403.
[90] HILDEBRANDT, Mireille. Defining profiling: a new type of knowledge?. In: Profiling the European citizen. Springer, Dordrecht, 2008, p. 58.
[91] ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais.* Universidade de São Paulo, São Paulo, fevereiro de 2019, p. 5.
[92] Op.cit., p. 5.

> person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Isto é, segundo o GDPR, o processo automatizado que busca avaliar aspectos pessoais de um indivíduo, seja para analisar ou prever aspectos relativos ao desempenho dele em seu local de trabalho, sua situação econômica, sua saúde, suas preferências e seus interesses pessoais, bem como o seu comportamento, sua localização e movimentos, com fins de classificar o indivíduo, constitui a chamada perfilização.

A definição de *profiling* utilizada pelo GDPR, portanto, abarca os dados pessoais sensíveis elencados pela LGPD, o que suscita a ideia principal deste trabalho, qual seja, a formação e a utilização desses perfis de comportamento criados a partir de informações a respeito do labor, da saúde, da condição econômica da pessoa, das suas preferências pessoais (pode-se abranger as preferências políticas, religiosas, filosóficas e sindicais), os movimentos (por exemplo, as informações coletadas a respeito do movimento da pessoa em uma atividade física), dentre outros aspectos comportamentais inferidos a partir dessas informações pessoais sensíveis dos indivíduos.

Contudo, o GDPR, além de prever a definição de *profiling* no artigo 4º/4, também determina, em seu artigo 22/1°, que o titular dos dados não ficará sujeito a uma decisão unicamente algorítmica, o que se inclui a criação de perfis[93]. Assim, o regulamento buscou tutelar o indivíduo que tem os seus dados coletados, tratados e utilizados para a perfilização, tutela que a LGPD não deixou clara.

Por outro lado, a menção da Lei n. 13.709/2018 a respeito da formação de perfis se encontra disposta no próprio conceito de tratamento previsto no art. 5º, inciso X, que elenca a classificação como uma forma de tratamento de dados pessoais, e o § 2º do art. 12, o qual prevê que os dados anonimizados podem ser considerados dados pessoais se forem utilizados para a formação de perfis comportamentais. Pode-se inferir, portanto, que tanto os dados pessoais quanto os dados anônimos que se tornam dados pessoais, com a utilização de perfis, são objetos de tutela da lei, o que atrai a incidência de toda a base principiológica proposta pela LGPD que, vale mencionar, rechaça a discriminação oriunda do tratamento dessas informações pessoais.

[93] Art. 22 GDPR. 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Essa ideia se torna ainda mais forte, como dito anteriormente, no caso dos dados pessoais sensíveis, que possuem um grau de proteção ainda mais robusto que os dados pessoais *stricto sensu.*

Em relação ao tratamento de dados pessoais sensíveis e à formação de perfis, destaca-se um estudo realizado pelo Massachusetts Institute of Technology (MIT), o qual revelou que é possível extrair informações aparentemente escondidas em vídeos, como fluxo sanguíneo no rosto e pequenos movimentos, sendo, inclusive, possível prever questões de saúde por meio de uma análise dos resultados[94].

Por intermédio de dispositivos de monitoramento, Deborah Lupton[95] esclarece que é possível aferir os níveis de glicose no sangue, a temperatura corporal, a pressão arterial, a saturação de oxigênio e a atividade cerebral de um indivíduo, bem como reconhecer o seu padrão de sono, detectar a frequência cardíaca, o tempo em que foi praticado um exercício físico, além do gasto calórico e do tempo em que a pessoa permaneceu em pé, de modo a comparar com o tempo em que permaneceu em repouso[96].

A coleta desse tipo de dado acende discussões incisivas a respeito da sua utilização. Assim, por meio dos princípios da finalidade, da adequação e da necessidade, abarcados pela LGPD, clínicas, hospitais e laboratórios deverão restringir o tratamento desse tipo de dado apenas à utilidade designada inicialmente ou, quando for necessário modificá-la, que o paciente seja comunicado a fim de se evitar desvios e propósitos excessivos.

Por outro lado, os dados a respeito da saúde do indivíduo também podem ser utilizados de uma forma diferente, para atender às exigências da Lei n. 13.709/2018, a fim de proporcionar maiores benefícios aos usuários, como é o caso do estudo feito pela *Apple*, a indústria farmacêutica *Eli Lilly* e a startup de saúde *Evidation*, em que foi analisado se os dados coletados pelo *iPhone* e pelo *Apple Watch* poderiam ser utilizados para detectar sinais precoces de demência, bem como diferenciá-los da doença de Alzheimer.[98]

A classificação dos indivíduos a partir dos dados de saúde, portanto, que seja destinada a finalidades específicas e lícitas, como o levantamento de dados a respeito de pessoas em uma

---

[94] WU, Hao-Yu. RUBINSTEIN, Michael. SHIH, Eugene. GUTTAG, John V. DURAND, Fredo. *Eulerian vídeo magnification for revealing subtle changes in the world.* ACM Transactions on Graphics 31, n. 4. Jul. 2012, pp. 1-8.

[95] LUPTON, Deborah. *Lively Data, Social Fitness and Biovalue: The Intersections of Health Self-Tracking and Social Media.* The Sage Handbook of Social Media, London, 2017, p. 5.

[96] O gasto calórico e o tempo em que um exercício físico foi praticado, bem como a frequência cardíaca de uma pessoa e o tempo em que permaneceu em pé são avaliados, inclusive, por meio dos relógios inteligentes, que facilitaram a medição e o acesso dos usuários a esses tipos de dados pessoais sensíveis.

[98] FARR, Christina. *Apple and Eli Lilly are studying whether data from iPhones and Apple Watches can detect signs of dementia*. CNBC, 2019. Disponível em: https://www.cnbc.com/2019/08/07/apple-eli-lilly-studying-if-iphones-apple-watches-can-spot-dementia.html. Acesso em 02/09/2019.

determinada região que possuem alta incidência de determinada doença, pode ser importante para o direcionamento de políticas públicas específicas, por exemplo, ainda que se trate da reunião de dados e informações pessoais que classificam e determinam um grupo de indivíduos.

Contudo, a formação desses perfis por meio de informações sensíveis dos usuários, acompanhada da geração de modelos preditivos que analisam e modelam o comportamento dos indivíduos, pode ser problemática, uma vez que tal modelagem e predição viabilizam a classificação dos indivíduos de acordo com a sua raça, etnia, opinião política, orientação sexual e outros campos delicados que possuem divergências sociais, disputas e preconceitos eivados.

No caso do estudo realizado pelo MIT, a extração e o compartilhamento dessas informações de saúde entre hospitais, clínicas, laboratórios, empresas que oferecem seguros de vida ou que ofertam planos de saúde, bem como a formação de perfis a partir dessas informações, pode fazer com que seguradoras aumentem ou diminuam o valor da oferta para determinado grupo de indivíduos ou que empresas ofertem valores mais altos para aqueles indivíduos que possuem "maiores propensões" a desenvolverem uma doença, baseado tão somente nas informações sensíveis coletadas por meio do vídeo.

A perfilização ainda restringe o acesso a produtos, serviços e conteúdos, e de acordo com Neil Richards e Jonathan King, consoante indica Alexandre Veronese, o *profiling* compõe um dos três paradoxos do *Big Data*[99].

O primeiro deles gira em torno da proteção à privacidade e da transparência. Isso porque o processamento cada vez mais amplo de dados pessoais, viabilizado pelo *Big Data*, impossibilita cada vez menos a preservação da privacidade, uma vez que controladores sabem cada vez mais dos usuários, enquanto estes pouco ou nada sabem da forma, da quantidade, da qualidade, da utilização e do armazenamento dos seus próprios dados.

O segundo paradoxo é o da identidade, pois os algoritmos, ao gerarem respostas e padrões customizados para os usuários, restringem o seu acesso a produtos, serviços, conteúdos, oportunidades de emprego, discussões políticas, filosóficas e sindicais, dentre outros inúmeros temas.

Assim, tal padronização, viabilizada pelo *profiling*, modela a identidade dos indivíduos e dos grupos sociais de acordo com as ideias e os valores impostos pelo controlador e tudo isso é feito sem que os usuários percebam.

---

[99] VERONESE, Alexandre. *Repercussões do RGPD sobre a responsabilidade civil.* In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, Revista dos Tribunais, 2019, pp. 393-395.

O terceiro e último paradoxo reside no poder. Neil Richards e Jonathan King, conforme explanado por Alexandre Veronese, sustentam que a internet e os seus gigantes "foram relevantes para o movimento na Tunísia, as autoridades sírias usaram essas redes sociais para mapear e perseguir os dissidentes políticos". Nesse caso, os dados coletados e as decisões automatizadas tomadas com base nesses dados podem reprimir e oprimir indivíduos contrários ao governo, isto é, a perfilização feita a partir de informações sobre a opinião política, e seus desdobramentos, de uma pessoa pode não só criar contextos discriminatórios, mas gerar fatalidades, como a perseguições políticas que resultam até mesmo em morte.

2.5. O potencial dano e o cunho discriminatório direcionado ao titular dos dados pessoais por meio da formação dos perfis de comportamento: uma análise do art. 11, § 1º e do art. 12, § 2º, da Lei Geral de Proteção de Dados Pessoais

Como dito anteriormente, a Lei Geral de Proteção de Dados Pessoais definiu o dado pessoal como a "informação relacionada à pessoa natural identificada ou identificável" e o dado pessoal sensível como aquele relacionado à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Nota-se o cuidado do legislador ao categorizar e tutelar de forma diferenciada os dados pessoais e os dados pessoais sensíveis. Assim, a Lei n. 13.709/2018 ampliou o seu alcance em relação à previsão trazida pela Lei de Cadastro Positivo (Lei n. 12.414/2011) que, em seu art. 3º, § 3º, inciso II, veda expressamente a anotação em bancos de dados de "informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

Desse modo, o referido dispositivo tenta coibir o tratamento discriminatório na análise de concessão de crédito, uma vez que tais informações sensíveis, se utilizadas, podem conceder ou rejeitar uma linha de crédito à determinada pessoa, determinar o valor a ser concedido e até mesmo as condições pré-estabelecidas para a concessão do crédito podem ser diferentes a partir da análise de informações como origem social ou étnica.

A manipulação de dados sensíveis podem, inclusive, gerar ou agravar outras realidades discriminatórias, como a seleção de candidatos a uma vaga de emprego com base na etnia e na

raça dos indivíduos; a interferência direta em processos eleitorais[100]; o oferecimento de planos de saúde com alta variação de preços para um determinado grupo de pessoas com base em dados de saúde coletados por farmácias, hospitais, clínicas e laboratórios e até mesmo o monitoramento da reação de usuários de metrô ao assistirem a determinadas propagandas[101].

Ainda no universo das propagandas e das relações de consumo, Julie Cohen[102] ressalta que os dados coletados e tratados, referentes a consumidores, muitas vezes são utilizados com propósitos que os usuários certamente não concordariam, ainda que, em contrapartida, sejam disponibilizados produtos e serviços vantajosos. Isso porque o preço a ser pago pelo tratamento de suas informações e pelas vantagens proporcionadas é caro, isto é, a violação da sua própria privacidade:

> (...) Consumer data can be used for many purposes to which consumers might not so (...) blithely agree: employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have-nots"; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences; and so on. Data processors have no particular interest in disclosing these uses, precisely because individuals are likely to find them so objectionable. And even many privileged individuals might not wish to trade their own privacy for the supposed advantages that privilege would confer; who knows, after all, to what uses seemingly innocuous information might be put in the future? (2000, pp. 1398-1399)

Julie Cohen elucida que por trás da "escolha" feita pelo consumidor, há um modelo oculto com a "real escolha" determinada previamente pelo algoritmo configurado pelo operador e que assim o faz por meio das determinações do controlador. Isto é, a preferência manifestada pelo consumidor não é individual e inédita, mas inserida em um rol pré-estabelecido por um processador que condiciona as escolhas do usuário a partir dos dados coletados sobre ele que, na maioria das vezes, sequer percebe que forneceu dados a seu respeito por meio das interações as quais protagonizou no meio digital.

Nesse caso, a falaciosa "liberdade" conferida ao consumidor também pode alcançar cenários em que há o desvio da finalidade do tratamento de dados, o que gera desigualdades estruturais e realça disparidades de renda como, por exemplo, quando determinado produto ou serviço é oferecido somente para indivíduos que se reconhecem pertencentes a uma

---

[100] A interferência direta em campanhas eleitorais é retratada no documentário "Privacidade Hackeada", documentário dirigido por Jehane Noujam e Karin Amer. A produção imerge principalmente na atuação da *Cambridge Analytica* nas eleições estadunidenses de 2016, além de abordar o papel das redes sociais na manipulação de opiniões quanto ao Brexit, que trata da saída do Reino Unido da União Europeia.

[101] Vide Ação Civil Pública n. 1090663-42.2018.8.26.0100, em que a empresa ViaQuatro recolhia dados biométricos dos usuários de metrô por meio das 'portas digitais'.

[102] COHEN, Julie E. *Examined lives: informational privacy and the subject as object*. Stanford Law Review, v. 52, 2000, pp. 1398-1399.

determinada raça ou etnia, em detrimento de outros indivíduos que se reconhecem inseridos em outros grupos.

A preservação da privacidade em relação aos dados pessoais dos indivíduos pode impedir que haja julgamentos probabilísticos feitos por algoritmos a respeito de inclinações, habilidades ou até mesmo a respeito dos defeitos de um indivíduo.

Ocorre que essa preservação não é observada de modo satisfatório no que Julie Cohen[103] chama de *attention economy*, pois esse tipo de fenômeno impõe a criação de perfis como tática de sobrevivência de mercado.

Essas e outras possibilidades que se abrem em virtude do tratamento de dados pessoais sensíveis podem ser realizadas em massa por meio desses perfis, que induzem e monitoram o comportamento dos usuários, bem como a tomada de decisões algorítmicas que influenciam e muito a sociedade, como quando um carro autônomo toma uma decisão inadequada e atropela alguém[104].

Em relação ao monitoramento do comportamento dos usuários enquanto consumidores, Cathy O'Neil descreve que estes, ao contribuírem com um volume infinito de dados pessoais, abrem uma via em que anunciantes são capazes de aprender sobre o público-alvo de forma fácil. Isso permite que esses anunciantes direcionem ofertas que chegam "no momento e no local corretos", como, por exemplo, sistemas que enviam cupons de desconto para alimentação com base nos pedidos anteriores e específicos de um mesmo indivíduo, o que pode aumentar a probabilidade de haver um novo pedido e diminui o intervalo para vinte minutos entre o envio do cupom e o efetivo pedido[105].

Esse tipo de informação, ainda que, inicialmente, refira-se apenas à preferência do indivíduo por um determinado tipo de alimento, caso seja utilizada para outras finalidades, pode definir se bairros mais ricos recebem os cupons dos melhores restaurantes ou se bairros que possuem renda per capita menor recebem apenas promoções, ofertas e propagandas que impedem o acesso a uma determinada dieta.

A coleta desses dados pessoais, acrescida da ingerência de algoritmos e das decisões automatizadas, formam o cenário perfeito para que sejam gerados perfis preditivos e influenciadores de comportamento, que determinam, ao fim, quais as áreas serão alvo de

---

[103] Op.cit., pp. 1400-1401.
[104] ROBERTO, Enrico; LOPES, Marcelo Frullani. *Quando um carro autônomo atropela alguém, quem responde? O verdadeiro tamanho do problema ainda é desconhecido, e as discussões a seu redor, incipientes*. El país, tecnologia, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/04/16/tecnologia/1523911354_957278.html. Acesso em 21/07/2019.
[105] Op.cit., pp. 61-62.

determinadas políticas públicas, quais os indivíduos terão maior ou menor acesso a determinadas oportunidades de trabalho, quais pessoas pagarão menos ou mais por convênios firmados com planos de saúde – a depender da quantidade e da qualidade de informações a respeito da saúde dos titulares de dados pessoais que detiver a empresa responsável pelo oferecimento do plano –, quais grupos de indivíduos, a depender do seu posicionamento político, receberão de maneira mais incisiva informações sobre movimentos contrários à sua opinião política, com a finalidade de incitar o ódio, a violência e a indiferença, dentre outras inúmeras situações.

Quanto às oportunidades de trabalho, Catarina Castro[106], conforme citado por Andréa Costa e Ana Gomes, entende que o empregador trata dos dados pessoais de possíveis candidatos em momento anterior ao contrato, na seleção, como dados a respeito da identificação pessoal, registros criminais e dados de saúde, por exemplo; e, durante o trabalho, tais dados são utilizados para medir a produtividade ou o estado de saúde do trabalhador.

Como explanado por Andréa Costa e Ana Gomes[107], os empregadores têm se utilizado de dados como a aplicação de testes genéticos e de exames toxicológicos, a investigação de informações de cunho pessoal nas redes sociais dos potenciais trabalhadores ou daqueles efetivamente contratados, como dados sobre a orientação sexual e a opinião política, considerados dados pessoais sensíveis.

Isto é, há claro desvio de finalidade dos empregadores, que buscam informações pessoais que vão muito além daquelas necessárias à seleção ou à admissão de uma pessoa. Além disso, a manutenção dessas informações após o encerramento do período de seleção ou após o encerramento do contrato podem causar graves danos aos seus titulares, que deixarão de ser contratados por determinadas empresas em decorrência da sua orientação sexual ou opinião política, por exemplo.

Os perfis podem, inclusive, influenciar internamente a organização de trabalhadores celetistas e estatuários que, independentemente de atuarem em empresas ou em repartições públicas, filiam-se ao respectivo sindicato de uma determinada categoria. Isso porque a informação a respeito da filiação de um empregado ou de um servidor ao sindicato pode servir como uma forma de o empregador ou de o Poder Público, na pessoa do superior hierárquico do servidor, categorizar e classificar empregados e servidores internamente e, assim, conferir a um

[106] COSTA, Andréa Dourado. GOMES, Ana Virginia Moreira. *Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis*. Scientia Iuris, Londrina, v. 21, n. 2, jul. 2017, p. 230.
[107] Op.cit., p. 230.

determinado grupo, geralmente aquele em que as pessoas que não são filiadas, um tratamento revestido de privilégios.

Ainda na esfera de atuação do Poder Público, especialmente no que diz respeito ao tratamento de dados pessoais sensíveis, menciona-se o Decreto n. 10.046/19, publicado no dia 10/10/2019, que dispõe sobre "a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados".

Tal decreto, em seu art. 2º, incisos II e IV, trata dos dados pessoais sensíveis ligados à biometria, uma vez que, em seu inciso II, os chamados atributos biométricos consistem naquelas "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar".

Já em seu inciso IV, o referido decreto conceitua os "atributos genéticos" como as "características hereditárias da pessoa natural, expedida, modificada ou destruída por uma determinada pessoa natural, ou por um determinado sistema, órgão ou entidade".

Isto é, antes mesmo do início da vigência da Lei Geral de Proteção de Dados, o Executivo Federal edita um decreto que dispõe sobre o compartilhamento de informações sensíveis a respeito das pessoas naturais.

Chama-se a atenção, portanto, para a expressão "reconhecimento automatizado" redigida no texto do mencionado inciso II, uma vez que o reconhecimento desse tipo de dado (biométrico) será feito, segundo o decreto, por meio de algoritmos, o que enseja toda a discussão acerca dos modelos preditivos, a possível formação de perfis comportamentais e outras técnicas de tratamento de dados realizadas, ou passíveis de serem realizadas, pelo Poder Público.

A fim de exemplificar a problemática da discriminação de pessoas e/ou de grupos por meio da definição de perfis e da manipulação de decisões algorítmicas, Cathy O'Neil cita o caso de Duane Buck, um homem afrodescendente que, em 1997, aguardava a pena que lhe seria aplicada pelo Tribunal do Júri no Texas, Estados Unidos, isto é, se Duane Buck seria condenado à morte ou à prisão perpétua, com a possibilidade de liberdade condicional[108].

Nesse caso, Cathy O'Neil menciona a adoção de modelos de reincidência para se medir e definir a pena mais adequada para casos como o de Duane Buck. Contudo, esses modelos, apesar de, em tese, serem livres de influência do humor e da opinião de seres humanos e, além

[108] ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais*. Universidade de São Paulo, fevereiro de 2019, pp. 22-23.

disso, economizarem dinheiro ao diminuírem a duração média de uma sentença, escondem o viés da opinião humana na tecnologia. Esta, por sua vez, aqui entendida como um sistema algorítmico é acessível apenas para uma parcela da sociedade, o que, no caso de Duane Buck, poderia potencializar o racismo.

Outra forma de discriminação por meio da manipulação de dados e de decisões tomadas por algoritmos, está a discriminação de mulheres que estejam em fase de "previsão de gravidez", ou seja, por meio de uma análise do comportamento de compra de algumas mulheres, é possível inferir se há a possibilidade de estarem grávidas e, portanto, a partir da extração de informações do perfil responsável por classificar essas mulheres, pode-se realizar toda sorte de discriminação possível, difícil de ser identificada.[109]

Frederik Borgesius[110] explica que a discriminação pode se inserir, inclusive, na tradução automatizada de certas expressões, isto é, caso a expressão "He is a doctor. She is a nurse" seja inserida no Google Tradutor para a tradução em turco, será gerada a expressão "O bir hemşire. O bir doktor".

Como a linguagem turca, nesse caso, é neutra e não possui gênero definido, isto é, o turco não diferencia as palavras "he" e "she", ao traduzir novamente a expressão para o inglês, tem-se sempre o resultado "He is a doctor. She is a nurse". Assim, Aylin Caliskan, Joanna Bryson e Arvind Narayanan[111] demonstram que o Google Tradutor exibe uma forte tendência a padrões masculinos e reforça estereótipos de gênero, de modo que, nesse caso, não haveria a possibilidade de a mulher ser a médica e o homem ser o enfermeiro.

A respeito da manipulação de dados sensíveis e da finalidade da formação de perfis, Ana Frazão bem descreve a possibilidade de a neurotecnologia utilizar-se de dados cerebrais para "fins de manipulação da opinião e da própria personalidade das pessoas, com objetivos econômicos, políticos, religiosos, dentre outros". Isto é, a utilização de dados cerebrais, por serem considerados dados pessoais sensíveis, segundo a autora, deve ser tratada apenas em "hipóteses específicas e, mesmo assim, sempre mediante a proteção dos titulares de dados", com o objetivo de frear o chamado "neurocapitalismo".[112]

---

[109] BORGESIUS, Frederik Zuiderveen. *Discrimination, artificial intelligence, and algorithmic decision-making.* Directorate General of Democracy, Concil of Europe, 2018, p. 13.
[110] BORGESIUS, Frederik Zuiderveen. Op.cit., pp. 17.
[111] CALISKAN, Aylin; BRYSON, Joanna J.; NARAYANAN, Arvind. *Semantics derived automatically from language corpora contain human-like biases*. Science, reports, psychology. 356(6334). 2017, pp. 183-186.
[112] FRAZÃO, Ana. *"Nerocapitalismo" e o negócio de dados cerebrais*. JOTA, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/neurocapitalismo-e-o-negocio-de-dados-cerebrais-25092019. Acesso em 25/09/2019.

Rafael Zanatta indica que a criação desses perfis origina obrigações de três naturezas distintas, quais sejam: (i) informacional, que se relaciona com a transparência da criação e da própria manutenção do perfil; (ii) dialógica[113], que está atrelada à fixação de um patamar mínimo de confiança entre o titular dos dados e os agentes que tratam os dados, que têm a incumbência de informar aos titulares a importância, a finalidade e o formato das decisões que envolvem a perfilização; e (iii) não discriminatória, que guarda correlação direta com o que é exposto pelo art. 5º, inciso II, da Lei n. 13.709/18, como o dado pessoal sensível[114].

De início, a necessidade de informar e conferir transparência ao tratamento de dados pessoais funciona como uma abertura para o processo dialógico de explicação, que partiria de uma "construção conjunta do conhecimento"[115].

Isto é, a fim de se evitar a criação de cenários discriminatórios e a prospecção de danos aos titulares dos dados pessoais, é de suma relevância que os agentes manipuladores dessas informações pessoais estabeleçam certa relação com o titular dos dados a fim de garantir uma comunicação que tenha como finalidade a compreensão de como o processo é feito, para quê e com qual finalidade, conforme elucida Rafael Zanatta:[116]

> Essa obrigação dialógica não é um simples ato de comunicação unilateral, como o envio de um relatório descritivo das fórmulas matemáticas utilizadas pelo controlador e as técnicas de estatísticas que permitem a inferência sobre um comportamento futuro a partir de um conjunto de dados pessoais e metadados. Na concepção da teoria pedagógica formulada por Paulo Freire no Brasil – com uma interessante mistura de conceitos de "emancipação" inspirados em Karl Marx (1818- 1883) e concepções democráticas e pedagógicas inspiradas em John Dewey (1859- 1952) –, o ato dialógico é aquele problematizante, que recusa o simples "depósito de uma informação" e se engaja em uma espécie de "trabalho em equipe"[117].

A LGPD prevê, em seu art. 11, § 1º, a possibilidade de causar dano ao titular quando a hipótese de tratamento se referir aos dados pessoais sensíveis. Isto é, os cenários discriminatórios acima explanados, ao gerarem dano ao titular das informações sensíveis, estarão enquadrados no dispositivo retromencionado e, para além, com a interpretação do art. 12, § 2º, da referida lei, pode-se inferir que o tratamento de dados pessoais utilizados com a finalidade de formar perfis de comportamento também é objeto de tutela.

---

[113] Renato Leite Monteiro e Bruno Bioni também sustentam que deve haver uma obrigação que sustente o diálogo entre o titular dos dados pessoais e dos agentes que os manipulam. (MONTEIRO, 2018, p. 11), (BIONI, 2018).

[114] Art. 5º Para os fins desta Lei, considera-se: (...)
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[115] Op.cit., pp. 23.

[116] Op.cit., pp. 22.

[117] FREIRE, Paulo. *Educação como Prática da Liberdade*. 26 ed. Rio de Janeiro: Paz e Terra, 2002.

Nesse caso, a interpretação em conjunta dos dois dispositivos mencionados, além de toda a base principiológica conferida pela Lei n. 13.709/2018, permite inferir que não só a utilização de dados pessoais *stricto sensu* na criação de perfis comportamentais está prevista na lei, mas, principalmente, a utilização de dados pessoais sensíveis na formação desses perfis, que geram danos aos titulares e criam ou fomentam cenários claramente discriminatórios.

Em decorrência do dano gerado pelo tratamento de dados pessoais sensíveis na formação de perfis comportamentais, emerge o direito à indenização em prol dos titulares que tiveram as suas informações sensíveis utilizadas indevidamente.

Contudo, aqui, a grande dificuldade reside na capacidade de o titular construir um conjunto probatório suficiente, em que possa ser analisada de maneira satisfatória a ocorrência de dano. Isso porque, quando se trata de dados, controladores e operadores possuem um denso volume de informações a respeito dos titulares e dos procedimentos adotados que geraram o dano, enquanto que os titulares são enfraquecidos, pois nada sabem ou sabem muito pouco a respeito do tratamento das suas informações sensíveis. Daí a necessidade do dever dialógico entre agente manipulador de dados e o titular, conforme dito anteriormente.

A ocorrência do dano propriamente dito e da possibilidade de inversão do ônus probatório serão analisadas no capítulo três.

Por fim, o problema central que surge é a maneira com a qual os agentes deverão formar perfis e produzir algoritmos que tomarão decisões de forma a não pactuar com esses vieses discriminatórios e cenários danosos e, caso o façam, de que modo haverá a responsabilização civil desses agentes, especialmente com base na aplicação da Lei Geral de Proteção de Dados.

Contudo, é cediço que não cabe apenas aos órgãos de *enforcement* a tarefa de mitigar danos e descontruir padrões discriminatórios, mas, principalmente, aos próprios agentes manipulares dos dados pessoais que, ao promoverem a autorregulação, alinham-se aos princípios elencados pela LGPD, especialmente ao princípio da não discriminação, em que Rafael Zanatta fundamenta a sua teoria.

Isso porque as ferramentas disponibilizadas pela heterorregulação podem ser utilizadas de forma interessante a fim de que se evite o dano e a geração do contexto discriminatório, mas a maior aposta está na tarefa de evitar a criação e a propagação desse tipo de viés que, uma vez concretizado, torna-se extremamente difícil minimizar e eliminar os seus efeitos, que se espalham pelas esferas sociais e até psicológica dos indivíduos.

Desse modo, o *Compliance* e a consciência social de controladores e de operadores terão papel fundamental para a coexistência das decisões algorítmicas, da formação de perfis comportamentais (salvo em relação aos dados pessoais sensíveis) e da preservação de direitos

fundamentais, direitos da personalidade e dos princípios basilares do tratamento de dados pessoais.

CAPÍTULO 3 – A RESPONSABILIZAÇÃO PELO EVENTUAL DANO CAUSADO EM VIRTUDE DA FORMAÇÃO DE PERFIS DE COMPORTAMENTO

3.1. Noções introdutórias a respeito da responsabilidade civil, segundo a Lei n. 13.709/2018, e a lesão aos direitos da personalidade, segundo o Código Civil

A Lei Geral de Proteção de Dados prevê, em seu art. 11, § 1º, que as hipóteses previstas para o tratamento de dados pessoais sensíveis são aplicadas ao tratamento de dados pessoais que revelem informações sensíveis a respeito do titular e que possam lhe causar dano.

Pela interpretação do dispositivo acima, portanto, é possível concluir que, para os controladores e operadores que coletarem, tratarem, utilizarem e armazenarem dados pessoais sensíveis, é de suma relevância que, ao fazerem, respeitem as hipóteses previstas pelo art. 11 da LGPD, sob pena de haver a configuração do dano ao titular.

Além disso, a interpretação do art. 11, § 1º em conjunto com o art. 12, § 2º, da mesma lei, vai além e robustece o nível de proteção ao titular, pois permite inferir que os dados utilizados para a formação do perfil comportamental de uma pessoa natural, se identificada, também serão objeto de tutela.

Isto é, os dados pessoais sensíveis, caso sejam utilizados na criação ou no aperfeiçoamento de perfis comportamentais, ao provocarem dano, gerarão o dever de ressarcimento em virtude dos danos materiais e, principalmente, o dever de reparação indenizatória em face dos danos à honra objetiva e/ou subjetiva da pessoa[130], seja no meio *on-line* ou *off-line*.

O direito de personalidade traduzido pelo direito à privacidade (art. 21 do Código Civil) já é previsto como aquele que, se lesado, acarretará a reparação por danos morais. Assim, a lesão à privacidade e o desrespeito à esta no tratamento de dados pessoais, especialmente os sensíveis, enseja, como dito, a reparação indenizatória.

Para Flávio Tartuce, o dano que fere os direitos de personalidade é chamado de dano moral impróprio e configura-se como uma lesão à liberdade, à opção sexual, e à opção religiosa

[130] A "honra objetiva", segundo Tartuce, é aquela que possui repercussão social e a "honra subjetiva" é aquela relacionada à maneira pela qual a própria pessoa se vê, relaciona-se à autoestima. Op.cit., p. 494.

e essas informações estão inseridas nos dados pessoais sensíveis, por caracterizarem informação sensível da pessoa[134].

Ou seja, no caso da atuação do controlador e/ou do operador que tratam informações a respeito dos direitos de personalidade, a aplicação do próprio Código Civil abre caminho para a reparação por danos morais, caso haja a lesão. Para além, no caso da formação de perfis comportamentais a partir dessas informações sensíveis, a interpretação do art. 11, § 1º em conjunto com o art. 12, § 2º mostra-se clara quanto à responsabilidade civil dos agentes que tratam os dados pessoais sensíveis e que causem danos aos titulares desses dados, como dito anteriormente.

Ademais, o art. 44, inciso II, da LGPD, considera irregular o tratamento de dados pessoais quando faltar-lhes a segurança necessária e esperada pelo titular e, além disso, quando não for observado "o resultado e os riscos que razoavelmente dele se esperam".

Desse modo, pode-se considerar que esse resultado e os riscos previstos no inciso II se inserem na ideia de dano ao titular e à criação ou agravamento de cenários discriminatórios, no caso do tratamento de dados pessoais sensíveis. Isso porque os agentes manipuladores, ao tratarem esses tipos de dados, que possuem um grau de tutela mais robusto, compreendem que se trata de informações delicadas referentes à pessoa e que podem, caso sejam manipuladas de forma inadequada, potencializar desigualdades e fomentar a cisão cada vez maior entre grupos sociais e até mesmo indivíduos.

Consequentemente, a manipulação de dados pessoais sensíveis para a formação de perfis comportamentais segrega a sociedade, estimula discussões em virtude das diferenças entre as pessoas e desestrutura o pacto social.

Em que pese à incidência dos dispositivos acima mencionados em um cenário em que controladores e/ou operadores manipulam dados pessoais sensíveis e os utilizam para a formação de perfis de comportamento, há, ainda, um vasto caminho a ser percorrido que será protagonizado pelas demandas concretas que serão enviadas ao Poder Judiciário e pela própria atuação deste a partir da vigência da Lei n. 13.709/2018.

Contudo, este caminho se faz necessário para tratar das situações geradoras de danos aos titulares e, o que é ainda pior, situações que criem ou que agravem discriminações profundas e estruturais na sociedade relacionadas à etnia, à raça, à religião, à política, à sindicalização, à saúde, à genética e à vida sexual.

---

[134] Op.cit., pp. 491.

3.2. Responsabilidade subjetiva e objetiva e a teoria do risco

Ainda que, na teoria, a autorregulação seja o melhor caminho até mesmo para facilitar a heterorregulação exercida pelos órgãos e pelas instituições de *enforcement*, na prática, a maior parte dos agentes econômicos e do próprio Estado não possui, atualmente, um aparato satisfatório, integrado e que atenda às necessidades já existentes e às necessidades que surgirão com a vigência da Lei Geral de Proteção de Dados.

Assim, faz-se de extrema relevância discorrer a respeito da responsabilização dos agentes que tratam dados pessoais, especialmente os dados sensíveis, e que, por intermédio desse tratamento, potencializam ou criam cenários discriminatórios, bem como causam danos aos titulares dos dados.

Caio Mário entende que a responsabilidade civil "consiste na efetivação da reparabilidade abstrata do dano em relação a um sujeito passivo da relação que se forma. Reparação e sujeito passivo compõem o binômio da responsabilidade civil"[138].

Para Rafael Corrêa[139], a responsabilidade civil no âmbito da proteção de dados possui dois vieses: a prevenção de danos e a recomposição ao *status quo ante* de cenários, conforme se verifica:

> Nesse quadrante de ideias, dois são os prismas que permitem a análise da responsabilidade civil e seu contributo no campo da proteção de dados pessoais: (i) a possível identificação de um repto que privilegie a prevenção de condutas que possam violar, sem a devida legitimidade, as liberdades que animam a autodeterminação informativa; e (ii) as formas de recomposição passíveis de observância em momento posterior à ocorrência da violação efetiva (2016, p. 141).

Esse posicionamento é importante, pois, quanto ao tratamento de dados pessoais sensíveis, a recomposição e a reparação do dano em si são dificultosas, uma vez que os titulares dos dados, na maioria das vezes, sequer possuem o conhecimento de que os seus dados são tratados com o objetivo de segregar e classificar os indivíduos, o que cria e/ou agrava situações discriminatórias.

Dessa forma, o primeiro ponto apresentado pelo autor, qual seja, o foco na prevenção de condutas, que têm o potencial de violar a liberdade, a privacidade e a autodeterminação

---

[138] PEREIRA, Caio Mário da Silva. TEPEDINO, Gustavo. *Responsabilidade Civil.* Editora Forensi, ed. 12ª. 2018, p. 14.

[139] CORRÊA, Rafael. *Responsabilidade civil e privacidade:* Autodeterminação informativa como expressão de liberdade positiva na construção da personalidade. Dissertação (Mestrado em Direito), Faculdade de Direito, Universidade Federal do Paraná. Curitiba, 2016, p. 141.

informativa, aliado a boas práticas de governança, podem ser o principal recurso da responsabilidade civil no que concerne à proteção de dados.

Quanto à reparabilidade do dano e a recomposição do *status quo ante*, cumpre discorrer acerca da responsabilidade subjetiva, pautada na culpa, e da responsabilidade objetiva, que será analisada à luz da teoria do risco.

De acordo com Sergio Cavalieri[140], "o desenvolvimento industrial, proporcionado pelo advento do maquinismo e outros inventos tecnológicos, bem como o crescimento populacional geraram novas situações que não podiam ser amparadas pelo conceito tradicional de culpa".

Nesse diapasão, no que diz respeito ao tratamento de dados pessoais, a noção de culpa em si demanda a própria evolução do conceito e da sua aplicação, uma vez que a construção de novos modelos de negócio gera novas demandas as quais a responsabilidade civil deverá incidir, o que se inclui a manipulação de softwares e algoritmos, que deverão se alinhar às novas perspectivas geradas pelo tratamento de dados pessoais.

O Código Civil brasileiro, por meio do seu art. 186, qual seja, "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilício" adotou a responsabilidade subjetiva como regra, uma vez que, conforme explicita Carlos Gonçalves[141], o dolo e a culpa são elementos fundamentais para a obrigação de reparar o dano.

Contudo, esclarece o autor, o referido diploma também estabeleceu a adoção da responsabilidade objetiva ao longo do seu texto, como é o caso da responsabilização do dono do animal, do dono do prédio em ruína, a responsabilização em virtude do estado de necessidade, a responsabilidade do credor que demanda o devedor em momento anterior ao vencimento da dívida ou até mesmo por dívidas pagas, dentre outras situações.

Há, ainda, autores que defendem que os dois tipos de responsabilidade não devem ser mirados de modo apartado. Miguel Reale entende que a responsabilidade subjetiva e a responsabilidade objetiva coexistem e se complementam, a depender da estrutura dos negócios:

> Responsabilidade subjetiva, ou responsabilidade objetiva? Não há que fazer essa alternativa. Na realidade, as duas formas de responsabilidade se conjugam e se dinamizam. Deve ser reconhecida, penso eu, a responsabilidade subjetiva como norma, pois o indivíduo deve ser responsabilizado, em princípio, por sua ação ou omissão, culposa ou dolosa. Mas isto não exclui que, atendendo à estrutura dos

[140] CAVALIERI, Sergio Filho. *Programa de responsabilidade civil*. 3ª ed. São Paulo: Malheiros, 2005, p. 18
[141] GONÇALVES, Carlos Roberto. *Responsabilidade civil.* São Paulo: Saraiva, 2019, p. 59.

> negócios, se leve em conta a responsabilidade objetiva. Este é um ponto fundamental.[142]

Ceez van Dam entende que, nas palavras de Ana Frazão, há uma interpenetrabilidade entre as responsabilidades subjetiva e objetiva[143]:

> Em sentido semelhante, Cees van Dam sustenta que a interpenetrabilidade entre os dois tipos de responsabilidade, que se acentua gradativamente com a ideia de culpa normativa, baseada na violação do dever de cuidado, faz com que não haja mais uma clara distinção entre ambos na prática, de forma que, quanto maior o dever de cuidado a ser aplicado em certos casos de culpa, menor será a diferença entre os dois. Consequentemente, o autor também compartilha da conclusão de que a distinção entre os dois tipos de responsabilidade é datada e que a responsabilidade civil do século XXI conceberá os dois sistemas em uma perspectiva de cooperação.

Essa ideia de culpa normativa, para Paula Bandeira[144], "afasta o subjetivismo inerente à concepção psicológica da culpa, fortemente atrelada à intenção e às circunstâncias pessoais do agente" e orienta a prova da culpa com base em um modelo geral de comportamento que o homem médio consiga seguir.

Geneviève Viney, Patrice Jourdain e Suzanne Carval[145] entendem que a culpa consiste na "violação de uma norma ou de um dever que se impõe ao agente" e, também, segundo Agostinho Alvim[146], essa violação de dever dedica-se a analisar o erro que tenha como parâmetro a conduta de um homem normal:

> (...) todo movimento se acentua no sentido de se objetivar, de se concretizar a noção de culpa. Afasta-se a imputabilidade moral para se apreciar tão somente o erro de conduta em face do comportamento do homem normal, excluindo-se, porém, as circunstâncias internas, pessoais, do agente e assim se proclama com fundamento na própria culpa dos que agem sem discernimento (1998, pp. 108-109).

Desse modo, a culpa normativa se orienta com base na violação do dever de cuidado que, na manipulação de dados pessoais, atrai o cumprimento do instrumento protetivo (LGPD) por parte dos agentes de tratamento.

Isto é, esses agentes possuem o dever de zelar pelo tratamento lícito e adequado aliado aos princípios e às diretrizes estabelecidas pela Lei Geral de Proteção de Dados, de modo que,

---

[142] REALE, Miguel. *Diretrizes gerais sobre o Projeto de Código Civil*. REALE, Miguel. Estudos de filosofia e ciência do direito. São Paulo: Saraiva, 1978, p. 176-177.
[143] FRAZÃO, Ana. *Risco da empresa e caso fortuito externo*. Civilistica.com. a. 5. n. 1. 2016, p. 17.
[144] BANDEIRA, Paula Greco. *A Evolução do Conceito de Culpa e o Artigo 944 do Código Civil*. Revista da Escola da Magistratura do Estado do Rio de Janeiro, v. 11, n. 42, 2008, p. 232.
[145] VINEY, Geneviève; JOURDAIN, Patrice; CARVAL, Suzanne. *Les conditions de la responsabilité*. 4ª ed. Paris: LGDJ, 2013, p. 445.
[146] ALVIM, Agostinho. *Culpa e risco*. 2ª ed. Ver. E atual. Por Ovídio Rocha Barros Sandoval. São Paulo: Revista dos Tribunais, 1998, pp. 108-109.

se houver violação, caberá à análise do cumprimento do dever de cuidado que, no caso específico da formação de perfis comportamentais, traduz-se no dever de não se utilizar dados pessoais sensíveis para a perfilização, sob pena de gerar um cenário discriminatório e causar dano aos titulares dos dados coletados.

Isso porque, ao analisar o princípio da não discriminação, previsto no art. 6º, inciso IX, da Lei n. 13.709/2018, conclui-se que os agentes de tratamento possuem o dever de realizar operações com base em dados pessoais sem que haja fins discriminatórios ilícitos ou abusivos.

Portanto, no que diz respeito à perfilização, a utilização de dados pessoais sensíveis afronta o princípio supramencionado e macula o dever de cuidado quando os agentes (controlador e operador) tratam informações pessoais a respeito da origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual e até mesmo a biometria do indivíduo.

Há a possibilidade, portanto, de se sustentar que os agentes, do ponto de vista econômico, devem saber identificar situações de tratamento que podem ser minimamente previsíveis, controláveis e, por conseguinte, também podem ser gerenciadas.

Ou seja, ao manipularem informações sensíveis, controladores e operadores têm ferramentas necessárias para calcularem os possíveis riscos e, ainda, para aqueles agentes que possuem modelos de negócios voltados à perfilização, também há como se sustentar que existem subsídios capazes de alertá-los sobre a utilização de dados pessoais sensíveis.

Inclusive, a própria utilização dos dados pessoais sensíveis, no caso do *profiling*, torna a atividade exercida pelos agentes extremamente perigosa e com a assunção de riscos enormes.

Isso porque, tanto na responsabilidade subjetiva quanto na objetiva, segundo Ana Frazão[147], "os elementos de previsibilidade do dano e do cumprimento do dever de cuidado" devem ser considerados, ainda que, para a responsabilidade objetiva, tais elementos sejam ainda mais importantes.

Quanto à previsibilidade para a responsabilidade objetiva, fundada na teoria do risco, para a autora, "quanto mais um dano for previsível, suscetível de cálculo e controle pelo empresário (alocação, transferência, gerenciamento), mais fácil é sustentar que se trata de algo inerente à empresa[148].

[147] Op.cit., pp. 17-18.
[148] Op.cit., pp. 12-13.

Para Ana Frazão, a responsabilidade objetiva analisada a partir da ótica de um "direito de danos", que focaliza na reparação dos danos sofridos pela vítima e não da repressão daquele que provoca o dano, é importante para a chamada "socialização de danos"[149]:

> Tal compreensão está igualmente relacionada à temática dos direitos fundamentais, seja porque a socialização de danos é importante instrumento de realização de justiça social, seja porque a própria responsabilidade civil passa a ser igualmente vista a partir da sua finalidade de proteger a pessoa humana. Isso obviamente amplia os deveres e responsabilidades de todos aqueles que exercem atividades de risco (2016, p. 9).

Isto é, para o tema da proteção de dados pessoais, a proteção da pessoa humana e a importância da responsabilização do agente que provocou o dano são instrumentos essenciais para a manutenção dos direitos fundamentais. Rememora-se, aqui, que o presente trabalho entende que a proteção de dados pessoais se encaixa como um direito fundamental e se alinha ao prisma constitucional.

É de suma relevância que seja feita uma análise a respeito da inclusão ou não na área de risco quando um agente de tratamento exerce determinada atividade, uma vez que, segundo Ana Frazão, "somente quando for alheio ao risco é que se poderá afastar a responsabilidade". As excludentes de responsabilidade seguem, também, a mesma linha de análise a respeito do risco[150].

Tal análise, portanto, auxilia na responsabilização daqueles agentes que efetivamente têm de ser responsabilizados segundo a responsabilidade subjetiva, amparada somente na noção de violação do dever e da culpa normativa, e daqueles que têm de ser responsabilizados de acordo com a responsabilidade objetiva, amparada na teoria do risco.

Ressalta-se que a teoria do risco é, inclusive, explanada no art. 927, parágrafo único do Código Civil, o qual dispõe que "aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. (...) Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

Nessa linha, Diogo de Melo[151] sustenta que o art. 927, parágrafo único, estabelece a "possibilidade de convivência harmônica" das responsabilidades subjetiva e objetiva, uma vez

---

[149] Op.cit., p. 9.
[150] Op.cit., p. 6.
[151] MELO, Diogo Leonardo Machado de. *Título III. Dos Atos Ilícitos.* In: NANNI, Giovanni Ettore (Org). *Comentários ao Código Civil: Direito Privado Contemporâneo.* Saraiva-jur, 2019, p. 1.275.

que ora exige-se "uma atuação culposa, ora cria-se uma imputação baseada em lei, ou quando a atividade normalmente desenvolvida envolve um risco".

Nota-se, portanto, que o referido diploma adotou também a responsabilidade objetiva sustentada pela teoria do risco que, de acordo com Miguel Reale[152], consubstancia-se em um negócio jurídico dotado da existência de "riscos inerentes à atividade desenvolvida", de modo que incidirá a "responsabilidade objetiva de quem dela (a atividade desenvolvida) tira proveito, haja ou não culpa".

Assim, tal responsabilidade, segundo Carlos Gonçalves[153], "representa risco para os direitos de outrem, (...) que possibilitara ao Judiciário uma ampliação dos casos de dano indenizável". Ainda segundo o autor, nesse caso, a existência do dano pressupõe a ausência da aplicação daquelas medidas entendidas como adequadas, que deveriam afastar o risco inerente à atividade.

Para o tratamento de dados pessoais, essas medidas adequadas envolvem toda a base principiológica abordada pela Lei n. 13.709/2018, bem como todos os deveres que os agentes de tratamento possuem.

No que diz respeito ao estudo do dano propriamente dito, o *General Data Protection Regulation,* segundo António Cordeiro[154], não apresentou um conceito específico, mas os Estados-Membros do Conselho da União Europeia, ao discutirem sobre o tema, manifestaram dois posicionamentos diferentes, quais sejam (i) caberia a cada Estado-Membro, no âmbito do seu próprio território e direito interno, definir e aplicar o conceito de dano; e (ii) caberia ao Tribunal de Justiça da União Europeia, TJUE, interpretar o artigo 82/1[155].

Contudo, o autor[156] aponta duas dificuldades inerentes à aplicação do artigo 82/1 pelo ordenamento jurídico interno dos países, quais sejam, (i) a complexidade e a subjetividade do próprio conceito de dano, enfrentadas normalmente pelos Estados-Membros; e (ii) a definição da competência jurisdicional dos tribunais desses Estados-Membros para enfrentarem casos concretos que abordem o tema e à luz do GDPR.

Quanto à aplicação do artigo supramencionado pelo TJUE, o autor esclarece que, quando se trata de responsabilidade civil, o referido tribunal tem imposto o cumprimento de

---

[152] Op.cit., pp. 176-177.
[153] Op.cit., p. 60.
[154] CORDEIRO, António Barreto Menezes. *Repercussões do RGPD sobre a responsabilidade civil.* In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato (Orgs). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, Revista dos Tribunais, 2019, pp. 780-781.
[155] O artigo 82/1 do GDPR dispõe sobre o direito de indenização que tem a pessoa caso sofra dano material ou moral como resultado de uma violação do regulamento. Essa indenização será paga pelo responsável pelo tratamento de dados pessoais que lhe tenha causado dano.
[156] Op.cit., pp. 780-781.

dois princípios, o da equivalência e o da efetividade. Dessa forma, impede-se que, ao aplicarem-se as normas de direito europeu, os jurisdicionados sejam mais prejudicados ou menos favorecidos do que se houvesse a aplicação de uma norma de direito interno e, além disso, garante-se o exercício efetivo dos direitos abarcados pelo direito europeu.

Já a LGPD prevê, em seu capítulo VI, assim intitulado como "Dos Agentes de Tratamento de Dados Pessoais", e, mais especificamente, em sua Seção III, "Da Responsabilidade e do Ressarcimento de Danos", as hipóteses em que controlador e operador serão responsabilizados em virtude de danos que possam causar aos titulares dos dados coletados.

Assim, paralelamente ao que dispõe o artigo 82/1 do GDPR, a LGPD prevê, em seu art. 42, *caput*, que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

Pode-se inferir, portanto, que o exercício da atividade do tratamento de dados pessoais atrai a noção de preservação e do cumprimento do dever de cuidado, de modo que a sua violação acarreta a responsabilização do agente de tratamento.

Tal preservação e cumprimento, aliados à previsibilidade mencionada anteriormente, formam parâmetros (qualitativos e quantitativos) mais objetivos a respeito da responsabilização dos agentes, de modo que princípios como o da razoabilidade e da proporcionalidade também deverão ser considerados na análise do caso concreto.

Tais parâmetros são importantes, também, quando o julgador entender pela aplicação da responsabilidade objetiva dos agentes de tratamento fundada na teoria do risco. Mais uma vez, princípios como o da razoabilidade e da proporcionalidade auxiliam na análise da assunção do risco em si, isto é, na definição da medida em que os elementos analisados foram de fato voluntariamente assumidos pelos agentes de tratamento e quais elementos fogem da configuração do risco, o que busca sustentar as excludentes de responsabilidade.

A título exemplificativo, cabe mencionar uma análise da responsabilidade civil a respeito dos dados pessoais, quando o titular figurar como consumidor.

No julgado do Tema n. 710 (REsp n. 1419697/RS), em que o Superior Tribunal de Justiça firmou, em sede de Recurso Repetitivo de Controvérsia, a tese de que, na hipótese de os dados pessoais serem coletados e tratados em uma relação firmada por meio de contrato, se configurada a relação de consumo caracterizada pela oferta e aquisição de bens e de serviços, a responsabilidade é objetiva, conforme expõe o excerto abaixo:

> RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL. (...). 5. O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do Código Civil), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados. (...) (STJ, 2014, *on-line*)

Isto é, tal análise pode ser sustentada na responsabilização de agentes de tratamento das informações pessoais dos usuários quando estes estiverem na condição de consumidores. Inclusive, como exposto no capítulo dois, os perfis de comportamento também podem ser utilizados para a criação e a manutenção de anúncios publicitários comportamentais.

No caso concreto, o Tribunal, ao indicar que a "utilização de informações excessivas ou sensíveis" enseja a condenação ao pagamento de indenização por danos morais e que tal responsabilidade é objetiva, reconhece, ainda que de maneira setorial, isto é, para o sistema de *credit scoring*, a ausência de equidade entre os agentes que manipulam os dados pessoais e os titulares desses dados.

Desse modo, no caso de a responsabilização em decorrência da formação de perfis de comportamento por meio da utilização de dados pessoais sensíveis ser analisada à luz da violação do dever de cuidado e da culpa normativa (calcada na conduta diversa daquela esperada do homem médio), haverá a configuração da responsabilidade subjetiva, pois se considera o elemento culpa como necessário para a configuração do dano.

Por outro lado, caso o *profiling* seja analisado à luz não só da violação do dever de cuidado, mas também sob a ótica da teoria do risco (em que a perfilização é considerada como uma atividade que possui riscos e que estes possuem certo grau de previsibilidade), a responsabilidade será objetiva, de modo que o elemento culpa do agente causador do dano não será necessário para a geração da reparabilidade. Inclusive, quando o titular figurar como consumidor, há uma tendência de que a análise de responsabilidade também seja feita sob o prisma objetivo.

Há, portanto, um cenário desafiador com o qual a Lei Geral de Proteção de Dados Pessoais deverá lidar, de modo que, inicialmente, ambos os tipos de responsabilidade podem ser aplicados à perfilização, a depender do caso concreto, pois, como entende Miguel Reale, a responsabilidade subjetiva deve ser entendida como norma. Contudo, a depender da estruturação do negócio, a responsabilidade objetiva deverá ser aplicada, especialmente se o profiling for considerado como uma atividade que assume a geração de potenciais riscos (de

acordo com a previsibilidade que devem ter os agentes acerca do tratamento das informações pessoais, especialmente as sensíveis).

3.3. Responsabilidade solidária, reparação por dano coletivo e ausência de responsabilidade

O *General Data Protection Regulation* estabeleceu, em seu artigo 82, a noção do *data controller* e do *data processor* (subcontratante), ambos agentes envolvidos no tratamento de dados pessoais. A LGPD, por sua vez, estipulou as figuras do controlador e do operador, respectivamente.

A Lei n. 13/709/2018 dispõe que o controlador será responsabilizado quando, em razão do exercício das atividades de tratamento de dados, causar danos de cunho patrimonial, moral, individual ou coletivo, em violação à própria lei.

A expressão "em razão do exercício das atividades de tratamento de dados" abre margem para a interpretação tanto para a responsabilidade subjetiva, fundada na previsibilidade, no cumprimento do dever de cuidado e na ocorrência de culpa normativa, quanto para a responsabilidade objetiva, quando o julgador entender que tal atividade de tratamento pressupõe o risco.

Já no que diz respeito aos operadores, a LGPD dispõe que haverá a responsabilização destes em duas situações: (i) quando os preceitos estabelecidos pela lei não forem observados e/ou (ii) quando o operador deixar de seguir orientações lícitas oriundas do controlador.

A Lei Geral de Proteção de Dados ainda prevê a ocorrência de responsabilização solidária entre o controlador e o operador ou entre controladores, nos seguintes casos e de acordo com o art. 42, § 1º, incisos I e II: (i) o operador, quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador; e (ii) na hipótese de haver mais de um controlador evolvido no tratamento dos dados que originou o dano, todos os controladores também responderão solidariamente.

Nesse diapasão, importa mencionar o art. 942, parágrafo único, do Código Civil, que dispõe, inclusive, sobre a responsabilidade solidária de autores e coautores dos danos praticados.

Logo, caso fique claro que o operador atuou no sentido de também causar o dano, seja por meio do desrespeito dos preceitos trazidos pela LGPD, seja pela violação das instruções lícitas do controlador, ou, ainda, quando mais de um controlador estiver envolvido no tratamento, haverá a sua responsabilização também à luz do Código Civil.

Quanto à reparação por dano coletivo, em seu art. 42, § 3º, a legislação de proteção de dados pessoais dispõe que tal ação de reparação poderá ser ajuizada coletivamente em juízo. Nesse caso, os danos decorrentes de cenários discriminatórios criados por meio da manipulação de dados pessoais sensíveis, quando gerados em desfavor de um determinado grupo de indivíduos, enseja a possibilidade de estes ingressarem juntos em juízo a fim de obterem a reparação pelos danos que lhes foram causados.

Tal previsão se constitui como uma importante ferramenta instituída pela LGPD, principalmente em relação àqueles danos causados aos titulares por meio da manipulação de dados pessoais sensíveis, pois estes se referem muitas vezes à etnia, raça, filiação partidária e sindical dos indivíduos, temas que, naturalmente, pressupõem a formação de grupos representativos. A lei, portanto, preocupou-se em tutelar coletivamente essas situações.

Contudo, antes mesmo da vigência da referida norma, destaca-se, por exemplo, a Ação Civil Pública ajuizada pelo Instituto Brasileiro de Defesa ao Consumidor, IDEC, contra a ViaQuatro, a concessionária responsável pela linha amarela do metrô de São Paulo.

O instituto pediu a condenação da concessionária ao pagamento de indenização coletiva em valor não inferior a 100 milhões de reais, que deveria ser revertido para o Fundo de Defesa de Direitos Difusos, FDD.

A ação foi ajuizada, portanto, para que a ViaQuatro cesse a coleta de dados biométricos dos consumidores, que não consentiam com a extração e o tratamento dos seus dados pessoais sensíveis[158].

Por fim, a LGPD prevê as hipóteses em que não haverá o dever de indenizar por parte dos controladores e operadores, isto é, quando: (i) os agentes de tratamento provarem que não realizam o tratamento dos dados envolvidos na ocorrência do dano; (ii) os agentes, ainda que tenham realizado o tratamento dos dados, provarem que não houve violação à norma protetiva (aqui, a noção de cumprimento do dever de cuidado é de suma relevância); e (iii) houver a prova de que o dano é decorrente da culpa exclusiva do titular ou de terceiro.

Nota-se que a Lei n. 13.709/2018 procurou dispor a respeito da responsabilização que tem o controlador e/ou operador quando causarem danos aos titulares de dados pessoais e, ainda que não haja uma menção direta e clara acerca da reparação por danos decorrentes da formação de perfis comportamentais que modelam, classificam e impõem condições preditivas aos usuários por meio da manipulação de informações sensíveis a respeito deles, há instrumentos

[158] BRASIL. Tribunal de Justiça de São Paulo. Ação Civil Pública n. 1090663-42.2018.8.26.0100. Requerente: IDEC – Instituto Brasileiro de Defesa do Consumidor. Requerido: Concessionária da Linha 4 do Metrô de São Paulo S. A. (Via Quatro). Magistrada: Patrícia Martins Conceição. DJe: 29 de novembro de 2018.

capazes de viabilizar o ajuizamento de ações a respeito do tema, como é o caso do instituto da inversão do ônus probatório e da própria elaboração de relatórios de impacto, bem como a imposição do dever de registro de todas as operações de tratamento de dados feitas pelo controlador e pelo operador.

3.4. Inversão do ônus probatório

O Código de Processo Civil de 2015 dispõe que o ônus da prova incube ao autor quanto ao fato constitutivo do seu direito. Contudo, em uma sociedade caracterizada pelo que Frank Pasquale chamou de *one way mirror*[159], em que os titulares nada sabem a respeito da extração, do tratamento, da utilização e do armazenamento dos seus dados pessoais, a Lei n. 13.709/2018, sabidamente, prevê a inversão do ônus probatório quando o juiz constatar que a alegação for verossímil e quando houver hipossuficiência para fins de produção de prova, bem como quando a produção desta for excessivamente onerosa ao titular.

Tal previsão corrobora a inversão do ônus probatório, disposta no art. 373, § 1º, do Código de Processo Civil, que determina a inversão também quando há a impossibilidade ou a excessiva dificuldade de o autor produzir as provas necessárias ao caso concreto, isto é, ocorre o que Tartuce chama de "carga dinâmica da prova": o Juízo sopesa as condições de produção de prova no caso concreto e determina a sua inversão.

Para o tema da proteção de dados pessoais, a previsão de inversão é de suma relevância, uma vez que o controle dos dados pessoais coletados reside quase que totalmente no controlador e no operador, o que dificulta muito o acesso do titular dos dados.

O GDPR prevê, em seu art. 21/1, que o titular dos dados tem o direito de contestar, a qualquer momento, o tratamento de dados pessoais que lhe digam respeito, incluindo a criação de perfis. Dessa forma, os responsáveis pelo tratamento dos dados ficarão impedidos de processarem os dados, salvo se demonstrarem motivação legítima e convincente capaz de justificar o tratamento dos dados em detrimento dos interesses, direitos e da própria liberdade dos titulares, ou até mesmo para o estabelecimento do exercício de defesa.

Tal dispositivo pode indicar a previsão da inversão do ônus probatório, pois, num primeiro momento, o direito de oposição ao tratamento dos dados pelo titular deve ser observado, a menos que, em contrapartida, o agente responsável pelo tratamento dos dados demonstre satisfatoriamente que o tratamento realizado e justificável.

---

[159] Op.cit.,

Essa ferramenta prevista pelo GDPR é importante para preservar a autonomia e a gestão do titular sobre os seus próprios dados, além de reconhecer a dificuldade que tem o titular de reunir documentos necessários que comprovem o tratamento irregular dos seus dados e até mesmo a geração de dano causado por meio do tratamento.

Para a LGPD, a inversão do ônus probatório é viabilizada caso os agentes responsáveis pelo tratamento de dados observem e cumpram o que prediz o art. 37 da lei: "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse". Isto é, com a imposição clara do dever de registro, o arcabouço probatório é facilitado, uma vez que, o Juízo, ao determinar a inversão do ônus, fará com que o agente de tratamento apenas apresente a documentação preparada desde a gênese do tratamento de dados pessoais.

Nesse mesmo sentido, o art. 38 determina que a Autoridade Nacional de Proteção de Dados poderá, também, determinar a elaboração de um relatório de impacto à proteção de dados pessoais, inclusive os dados sensíveis, de modo que fiquem claras as operações de tratamento de dados, observados os segredos comercial e industrial.

Nota-se que a Lei n. 13.709/2018 trouxe mais uma ferramenta importante para mitigar o tratamento irregular de dados pessoais, especialmente os dados sensíveis, o que se inclui, também, a própria formação de perfis e de modelos preditivos a partir de dados sensíveis. Isso porque, ao exigir-se a elaboração de um relatório de impacto, abre-se o caminho para a produção de um documento que indicará a regularidade ou não do tratamento de dados pessoais, de sorte que tal documentação será importante em uma eventual inversão do ônus probatório em Juízo, pois demonstrará, inclusive, a eventual ocorrência de dano.

A exigência da elaboração desse relatório de impacto também é prevista, pela LGPD, em relação ao Poder Público, conforme consta no art. 32 da lei. Assim, a autoridade, além de solicitar, aos agentes do Poder Público, a elaboração e a publicação desses relatórios para o conhecimento de toda a sociedade, poderá sugerir a adoção de padrões e de boas práticas para o tratamento de dados pessoais.

Novamente, a necessidade de se comprovar o tratamento regular dos dados pessoais é viabilizada, dessa vez na esfera de atuação do Poder Público, pois a previsão de que esses relatórios sejam publicados evidencia a preocupação do legislador em construir um cenário de tratamento de dados pessoais calcado no princípio da transparência e na facilitação da comprovação do tratamento regular ou na demonstração da ocorrência de eventuais danos aos titulares.

Dessa forma, o instituto da inversão do ônus probatório, consagrado também pelo art. 6º, inciso VIII, do Código de Defesa do Consumidor, que reconhece a ausência de paridade processual entre o consumidor e o fornecedor, também foi positivado pela Lei Geral de Proteção de Dados, que, além desse instituto, conferiu outras ferramentas e previsões para a elaboração de documentos que comprovem a regularidade do tratamento de dados pessoais.

Assim, retomam-se os dois prismas da responsabilidade civil mencionados por Rafael Corrêa, quais sejam, a reparação do dano e retomada do *status quo ante* e a própria ideia de prevenção do dano, que é fomentada pela imposição cada vez maior dos princípios da transparência e do livre acesso dos titulares aos seus dados pessoais tratados, especialmente os dados sensíveis.

Na prática, com a entrada em vigor da Lei n. 13.709/2018, espera-se que haja a aplicação do instituto da inversão do ônus probatório de forma aproximada ao que já é realizado no que diz respeito à atuação do Código de Defesa do Consumidor, ainda que, ao longo do tempo, a jurisprudência se desenvolva cada vez mais para conferir uma identidade e para fixar parâmetros para se identificar a verossimilhança e a ausência de paridade processual entre as partes, a fim de que haja a inversão do ônus probatório especificamente voltado para o tema da proteção de dados pessoais.

CAPÍTULO 4 – DESAFIOS DE ORDEM PRÁTICA

4.1. A regulação da proteção de dados na prática

No que diz respeito à aplicação prática da Lei Geral de Proteção de Dados no Brasil, especialmente em relação à técnica de perfilização e ao tratamento de dados pessoais sensíveis, o presente capítulo buscará abordar algumas ferramentas que possuem as empresas e o Poder Público para se alinharem à Lei n. 13.709/2018 e evitarem ao máximo a ocorrência de dano e a geração e/ou o fomento de cenários discriminatórios.

Para tanto, inicialmente, tratar-se-á da autorregulação por meio da implementação de programas de *Compliance*, que auxiliarão os agentes de tratamento no cálculo e na gestão do risco relacionado à atividade de tratamento, especialmente a perfilização.

Após, as instituições e os órgãos de *enforcement* serão apresentados como uma forma externa de fiscalização, de modo que tais agentes terão papeis muito além daquela perspectiva tradicional de comando e controle baseada na imposição do dever coercitivo.

Ademais, será abordado um modelo de gestão de softwares e algoritmos que coloca a privacidade em sua espinha dorsal e, por último, a gestão do consentimento será tratada a fim de fornecer ao leitor a noção de que tal hipótese de tratamento, para os casos em que houver a manipulação de dados pessoais sensíveis, deverá ser mais robusta. Inclusive, *players* que adotam a técnica da perfilização também deverão se ater ao consentimento e às demais hipóteses de tratamento a fim de evitar a ocorrência de dano.

4.2. Os resultados do *General Data Protection Regulation*

Em fevereiro de 2019, o *European Data Protection Board,* EDPB, publicou o relatório anual de atividades a fim de uniformizar o entendimento exarado pelas diversas autoridades supervisoras da proteção de dados pessoais, à luz da incidência do *General Data Protection Regulation.*

Os números revelam que, dos 206.326 casos recebidos pelas autoridades, entre maio de 2018 e janeiro de 2019, 94.622 são oriundos de reclamações dos próprios titulares dos dados pessoais, 64.684 são oriundos de notificações dos agentes de regulação acerca de violações à segurança da informação e os demais casos versam sobre consultas formuladas às autoridades, uma vez que pairam diversas dúvidas a respeito da adequação de agentes responsáveis pelo tratamento de dados pessoais às diretrizes, princípios e imposições do GDPR[160].

Dentre as reclamações dos titulares, estão as violações aos princípios do livre acesso e da finalidade; o compartilhamento indevido dos dados, sem que o consentimento tenha sido requerido ou atualizado; o vazamento de dados; o marketing direto feito por meio da formação de perfis comportamentais e o uso indevido de câmeras de segurança, potenciais extratoras de dados biométricos.

Em relação às notificações acerca de violações à segurança da informação, estão o *hacking,* o *phishing,* o *malware* e a revelação não autorizada de dados.

52% dos casos tratados pelas autoridades foram solucionadas, à época da divulgação dos relatórios, em fevereiro de 2019, e apenas 1% dos conflitos foi objeto de tutela do Judiciário.

---

[160] SATO, Luiza. Um ano depois, GDPR mostra que adequação à LGPD é obrigatória. Convergência digital, maio de 2019. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=50616&sid=15. Acesso em 12/09/2019.

Nota-se, portanto, a existência de inúmeros desafios à adequação dos responsáveis pelo tratamento pessoais ao que dispõe o GDPR, na União Europeia. Contudo, o fato de apenas 1% das ocorrências ter se transformado em litígios que foram levados ao Judiciário invoca o papel fundamental da autorregulação e do *Compliance* na política de coleta, gestão e armazenamento de dados pessoais.

Somado à autorregulação, a heterorregulação trazida, principalmente, pela figura das autoridades responsáveis pela regulação e pela supervisão de atividades que envolvam o tratamento de dados pessoais, forma a corregulação como a melhor maneira de se garantir o respeito à liberdade, à privacidade e à proteção de dados pessoais.

Inclusive, com a finalidade de fomentar a corregulação, o *Observatorio Latinoamericano de Regulación Medios y Convergencia,* Observacom, o Instituto Brasileiro de Defesa do Consumidor, IDEC, o *Desarrollo Digital* e o Intervozes elaboraram um documento intitulado como "Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet", que tem como objetivo indicar princípios, padrões e medidas específicas para se estabelecer formas de corregulação e de regulação pública no que diz respeito às plataformas de internet[161].

É nesse cenário desafiador, em que a autorregulação e a heterorregulação deverão atuar a fim de viabilizar a aplicação satisfatória dos preceitos e das diretrizes invocadas pela Lei Geral de Proteção de Dados, que também representa um avanço imensurável no que diz respeito à proteção dos dados de titulares brasileiros.

No que se refere à formação de perfis por meio da utilização de dados pessoais sensíveis, a autorregulação deverá exercer papel fundamental a fim de se evitar a geração de danos e de cenários discriminatórios, uma vez que, em sua estrutura interna, o *player* responsável pelo tratamento desse tipo de dado aplicará normas éticas e praticará boas condutas a fim de evitar a técnica da perfilização direcionada a informações sensíveis.

Já a heterorregulação deverá fiscalizar os agentes que se utilizam da técnica de *profiling* a fim de evitar a ocorrência de dano por meio da manipulação de dados pessoais sensíveis.

---

[161] PALLERO, Javier. BARATA, Joan. BETANCOURT, Valeria. PIAZZA, Andrés. MASTRINI, Guillermo. BECERRA, Martín. FREULER, Juan Ortiz. *Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet. Uma perspectiva latino-americana para alcançar processos de moderação de conteúdo compatíveis com os padrões internacionais de direitos humanos.* Elaboração: Intervozes, coletivo Brasil de comunicação social, Observacom, Desarrollo Digital, IDEC, agosto de 2019. Disponível em: https://www.observacom.org/wp-content/uploads/2019/08/Contribuições-para-uma-regulação-democrática-das-grandes-plataformas-que-garanta-a-liberdade-de-expressão-na-internet.pdf. Acesso em 24/09/2019.

Com a aproximação do início da vigência da Lei n. 13.709/2018, em agosto de 2020, os agentes responsáveis pelo tratamento de dados, sejam agentes privados ou públicos, deverão, portanto, promover uma série de ajustes em seu modo de pensar e agir acerca da proteção de dados pessoais, tema que ganha um novo e importante foco no Brasil.

4.3. *Compliance* e a autorregulação no cenário de proteção de dados pessoais: a mitigação de danos e de contextos discriminatórios

A autoridade europeia da proteção de dados pessoais, a *European Data Protection Supervisor* (EDPS) insere a ideia da ética digital e busca fomentar o ideário de proteção da dignidade humana, da autonomia e do funcionamento democrático das sociedades. Tal iniciativa busca fazer com que a comunidade europeia reflita sobre os direitos e valores inseridos pela economia movida a dados e que, assim, sejam desenvolvidas posturas mais incisivas nas discussões que envolvem o tema[172].

A ideia principal do EDPS é promover o debate público acerca da maneira pela qual a ética digital pode fortalecer os princípios inseridos pelo GDPR. Assim, René Mahieu, Nees Eck, David Putten e Jeroen Hoven[173] indicam que a ética utilizada pela autoridade europeia está pautada na ética da informação, ramo da ética aplicada que estuda e analisa os impactos sociais das tecnologias da informação e da comunicação.

Para os autores, os aspectos éticos do domínio digital são discutidos em vários debates científicos. Os profissionais da computação discutem técnicas para salvaguardar a privacidade e a segurança, os juristas debatem as legislações da proteção de dados pessoais existentes e seus aspectos essenciais, tais como o direito à privacidade, traduzido na transparência, no consentimento, na finalidade e na adequação dos dados pessoais coletados. Enquanto isso, médicos discutem a autonomia dos seus pacientes em relação aos dados fornecidos, especialmente os dados pessoais sensíveis.

René Mahieu, Nees Eck, David Putten e Jeroen Hoven apontam que a discussão sobre a ética na economia movida a dados é importante, pois, em aplicações de mineração de dados pessoais, as definições de privacidade e de discriminação são tecnologicamente definidas, isto é, desde sua gênese, os softwares podem fixar discriminações à grupos sociais e a indivíduos.

---

[172] European Data Protection Supervisor. The EU/s independent data Protection authority. Disponível em https://edps.europa.eu/data-protection/our-work/ethics_en. Acesso em 06/05/2019.
[173] MAHIEU, René; ECK, Nees Jan van; PUTTEN, David van; HOVEN. Jeroen van den. *From dignity to security protocols: a scientometric analysis of digital ethics*. Ethics and Information Technology, 2018, pp. 175-187

É nesse contexto que Ann Cavoukian[174] aponta a importância do *privacy by design*, que possui princípios de gerenciamento de informações que se aplicam a algumas tecnologias específicas, operações de negócios, arquiteturas físicas, infraestrutura das redes e aos próprios modelos de governança.

A chamada ética digital tem como seu grande aliado os programas de *Compliance*, ou os programas de conformidade, assim entendidos como "instrumentos de governança corporativa tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência"[175].

Nesse cotejo, a Lei n. 13.709/2018, dispõe, em seu art. 50, que controladores e operadores poderão formular regras de boas práticas e programas de governança que estabeleçam mecanismos internos de supervisão e de mitigação de riscos relacionados ao tratamento de dados pessoais[176]. Pode-se incluir, portanto, práticas que evitem a formação de perfis comportamentais por meio de informações pessoais sensíveis.

A implementação desses programas, segundo Ana Frazão, Milena Oliva e Viviane Abilio[177], traz vantagens no que diz respeito à manipulação de dados pessoais, tais como:

> (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas –, na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais.

Tais vantagens, para os autores, podem ser materializadas por meio da adoção de requisitos mínimos que viabilizam a efetividade dos programas de *Compliance*, como: (i) a

---

[174] CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Information & Privacy Commissioner, Ontario, Canadá, 2009.

[175] CUEVA, Ricardo Villas Bôas. *Funções e finalidades dos programas de Compliance.* In: CUEVA, Ricardo Villas Bôas. FRAZÃO, Ana. *Compliance:* perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 53.

[176] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

[177] FRAZÃO, Ana. OLIVA, Milena Donato. ABILIO, Viviane da Silveira. *Compliance de dados pessoais*. In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, ed. Revista dos Tribunais, 2019, p. 686.

avaliação contínua de riscos da atividade e a atualização do próprio programa de acordo com essa avaliação; (ii) a elaboração de Códigos de Ética e de Conduta, que devem ser observados por todos, inclusive por terceiros; (iii) o estabelecimento de uma organização com procedimentos e controles internos que estejam em consonância com a avaliação de risco; (iv) o comprometimento da chamada alta administração para que haja a real aderência ao programa; (v) a garantia de que o setor de *Compliance* terá autonomia e independência para a implantação das políticas necessárias, bem como o livre acesso aos procedimentos e aos recursos necessários; (vi) o fornecimento adequado de treinamento aos funcionários da empresa ou do agente que integra a Administração Direta ou Indireta; (vii) a instituição de uma cultura de *Compliance* que direcione sempre a organização para que cumpra as normas legais; (viii) a vigilância constante dos controles internos e procedimentos, para que não caia no esquecimento ou seja apenas um "programa de papel"; (ix) a implementação de um sistema de comunicação direcionado e que assegure a proteção dos informantes; e (x) a auditoria e punição de condutas que não estejam em conformidade com o programa[178].

No que diz respeito à formação de perfis comportamentais, a gestão ativa do risco, aliada à pronta identificação e à sua minoração, formam uma importante ferramenta que facilita a previsão do risco e do potencial dano que pode ser causado, bem como auxilia na preservação e no cumprimento do dever de cuidado, mencionado no capítulo três.

Além disso, todas as vantagens mencionadas acima podem contribuir para que a empresa ou o Poder Público se alinhem ao que dispõe a Lei n. 13.709/2018 e realizem o tratamento de dados pessoais de forma lícita.

A Blackberry Cylance, por exemplo, criou um Código de Conduta a fim de que seus funcionários comecem a observar os princípios, os fundamentos e os dispositivos trazidos pela Lei Geral de Proteção de Dados, como no caso do tratamento de dados pessoais sensíveis, que serão manipulados somente por uma pequena lista de membros da equipe de ciência de dados, que foram aprovados e que possuem permissão para acessar esse tipo de dado[179].

Para implementar diretrizes efetivamente éticas por meio de programas de *Compliance* aplicados aos agentes que extraem, tratam, utilizam e armazenam dados pessoais, busca-se o que Ana Frazão[180] chama de "situação ideal", em que tais agentes desenvolvem,

---

[178] Op.cit., pp. 686-693.
[179] CIO From IDG. *Como a Blackberry Cylance aplica Ciência de Dados para atender a LGPD*. [S.I.] 2019. Disponível em: https://cio.com.br/como-a-blackberry-cylance-aplica-ciencia-de-dados-para-atender-a-lgpd/. Acesso em 21/09/2019.
[180] FRAZÃO, Ana. *Corrupção e Compliance*. Jota, julho de 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/corrupcao-e-compliance-03072018. Acesso em 21/09/2019.

simultaneamente, dois tipos de conduta, quais sejam, (i) o cumprimento dos parâmetros legais e éticos fixados por esses programas como um fim em si mesmo; e (ii) o exercício desses parâmetros com a finalidade de não sofrerem possíveis sanções decorrentes de condutas diametralmente opostas.

O primeiro tipo de conduta repousa sobre o que Immanuel Kant chamou de imperativo categórico, assim definido: "aja segundo uma máxima que possa valer ao mesmo tempo como lei universal"[181]. Tal imperativo define que a ação praticada deve ser boa por si só e que tenha como objetivo a sua própria existência, sem que seja almejada outra finalidade a ser alcançada.

Já o segundo tipo de conduta aproxima-se do chamado imperativo hipotético, vislumbrado por Immanuel Kant como "o resultado da ordenação para se fazer ou realizar algo, isto é, visa uma ação como meio para se ter o que se almeja: evoca interesses e, portanto, a instrumentalidade"[182].

Independentemente do tipo de conduta adotada, a adoção de programas de *Compliance*, especialmente antes da entrada em vigor da Lei Geral de Proteção de Dados, traz vantagens competitivas aos agentes econômicos, que constroem um ambiente de confiança entre controladores e titulares, que terão o conhecimento de que aqueles controladores específicos adotam boas práticas de governança[183].

Ademais, a implementação desses programas pode salvaguardar agentes econômicos e o próprio Poder Público perante a atuação da Autoridade Nacional de Proteção de Dados, uma vez que não se sabe ao certo qual será a sua margem de atuação.

Por fim, a própria elaboração de Códigos de Ética e Conduta, como mencionado no caso da Blackberry Cylance, pode vir a se configurar como um mecanismo de autorregulação regulada, em que os próprios agentes se antecipam e cumprem de forma efetiva e materializada os preceitos legais fixados[184].

4.3.1. *Data Protection Officer* e o modelo *privacy by design*

[181] KANT, Immanuel. *Fundamentação da metafísica dos costumes.* Petrópolis, RJ: Editora Vozes. Bragança Paulista, SP: Editora Universitária São Francisco, 2013.
[182] SALOMÃO, Kátia Rocha. JUNIOR, Waldomiro Salles Svokinski. *KANT: Os fundamentos da dignidade da pessoa humana como condição para uma hermenêutica do dever.* E-Civitas. Revista Científica dos Cursos de Direito e Relações Internacionais do UNIBH, Belo Horizonte, ISSN: 1984-2716. Disponível em: www.unibh.br/revistas/ecivitas. Acesso em 21/09/2019.
[183] FRAZÃO, Ana. OLIVA, Milena Donato. ABILIO, Viviane da Silveira. Op.cit., p. 712.
[184] FRAZÃO, Ana. OLIVA, Milena Donato. ABILIO, Viviane da Silveira. Op.cit., p. 712.

A Comissão Europeia define a figura do *Data Protection Officer,* ou do encarregado, como o profissional responsável pelo tratamento de dados pessoais que tem como atribuições informar e aconselhar o controlador ou o operador acerca das obrigações previstas em lei, bem como controlar e averiguar o cumprimento das normas legais, além de atuar como ponte entre a autoridade responsável pela proteção de dados e os agentes responsáveis pelo tratamento dos dados e atuar como ponte entre a atividade de tratamento dos dados, os próprios titulares e o exercício dos seus direitos[185].

A Lei n. 13.709/2018, por sua vez, define, em seu art. 41, *caput*, que o controlador deverá indicar o encarregado, que terá as seguintes atribuições: (i) aceitar reclamações e comunicações dos titulares, prestar esclarecimento e adotar providências; (ii) receber comunicações da autoridade nacional e adotar providências; (iii) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e (iv) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A figura do encarregado foi alvo de vetos impostos pela Lei n. 13.853/2019, isto é, anteriormente, o encarregado deveria ser detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados pessoais.

Outro ponto vetado consistia na previsão de que a Autoridade Nacional de Proteção de Dados deveria dispor sobre os casos em que o operador deveria indicar o encarregado e, além disso, a autoridade também deveria regulamentar a garantia da autonomia técnica e profissional do exercício do cargo.

Contudo, com os vetos mencionados, o papel do encarregado, que possui grande relevância para a aplicação tanto dos programas de *Compliance* mencionados anteriormente, quanto no atendimento das normas e sanções propostas pela heterorregulação, tornou-se mais abstrato e nebuloso.

O *Data Protection Officer* (DPO) é, inclusive, crucial para a implementação do modelo *privacy by design* (PbD), outrora mencionado. Isso porque, de acordo com Ann Cavoukian[186], tal modelo se inicia com o reconhecimento explícito do valor e dos benefícios da implementação proativa de práticas concisas e precoces de privacidade.

---

[185] Comissão Europeia. *Quais são as responsabilidades de um encarregado da proteção de dados (EPD)?* Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_pt. Acesso em 21/09/2019.

[186] CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Information & Privacy Commissioner, Ontario, Canadá, 2009.

Segundo a autora, o encarregado, ao configurar-se como um agente responsável pela fruição de direitos dos titulares, contribui para que o agente econômico, ao adotar o modelo PbD, firme compromissos claros para estabelecer e fazer cumprir os mais altos níveis de privacidade fixados pelas normas legais, de modo que a antecipação de resultados permite a correção de impactos negativos.

Nessa linha, um dos princípios do PbD é o chamado *privacy by default*, que trabalha com os seguintes pilares: (i) a definição de um propósito para o tratamento de dados pessoais e a comunicação desse propósito aos titulares dos dados antes ou no mesmo momento em que as suas informações pessoais forem coletadas, observando sempre a clareza da finalidade, o limite e a relevância das circunstâncias; (ii) a limitação da coleta de informações pessoais, que deve ser justa, legal e limitada àquela necessária às finalidades específicas; (iii) a redução mínima da coleta de informações; e (iv) a retenção e a limitação da divulgação dos dados pessoais apenas àqueles propósitos relevantes ao titular e pelos quais ele consentiu, salvo as finalidades previstas em lei.

A definição de um propósito para o tratamento de dados pessoais e a sua comunicação se alinham as obrigações informativa e dialógica, assim entendidas por Rafael Zanatta, expostas no capítulo dois.

Para o PbD, a *accountability* e o *Compliance* invocam o zelo em relação à proteção de dados pessoais e demonstram a preocupação com a gênese da produção de softwares passíveis de serem utilizados economicamente ou para finalidades públicas, sem que acarrete prejuízos aos titulares dos dados tratados.

Ann Cavoukian[187] entende que o *privacy by design* exige que controladores e operadores mantenham os interesses do titular de dados em primeiro plano, de modo que sejam inseridos padrões fortes de privacidade e que sejam oferecidas informações suficientemente esclarecedoras aos titulares acerca do tratamento dos seus dados pessoais.

Para a autora, os melhores resultados do PbD são aqueles em que os titulares são capacitados para desempenharem papeis ativos e autônomos de gerenciamento dos seus próprios dados.

Isso porque, com a primazia das necessidades e dos interesses individuais dos titulares e coletivos, quando se tratar de grupos sociais, a possibilidade de ocorrerem danos e abusos em relação à privacidade dos titulares é reduzida, pois são considerados e postos em evidência quatro aspectos primordiais: (i) a qualidade do consentimento conferido pelo titular, de modo

[187] Op.cit., p. 5.

que seja livre e específico, especialmente quando se tratar de dados pessoais sensíveis; (ii) a precisão das informações pessoais, que também devem ser completas e atualizadas, observando os limites da finalidade do tratamento, conferida pelo consentimento; (iii) o livre acesso, em que os indivíduos terão acesso às suas informações pessoais e à sua utilização e eventuais compartilhamentos, bem como terão o direito de contestar as informações coletadas, além de poderem alterar o seu teor, conforme entenderem como necessário; e (iv) a efetiva atuação do *Compliance*, de modo que os agentes responsáveis pelo tratamento de dados pessoais devem estabelecer mecanismos que prestem as informações necessárias aos titulares, respeitados os segredos comercial e industrial[188].

Tal modelo, aplicado à técnica de perfilização e às decisões automatizadas, também pode impedir a ocorrência de dano e a concretização de cenários discriminatórios, pois a privacidade, enquanto pilar essencial do PbD, limitará o tratamento de dados pessoais, especialmente os sensíveis, à finalidade lícita, comunicada ao titular e anuída por este (ressalta-se, aqui, a importância do consentimento mais robusto para o tratamento de informações sensíveis).

Portanto, a implementação do *privacy by design* significa inserir a privacidade na arquitetura do software, dispositivo ou algoritmo que será desenvolvido, o que representa maior segurança, maior adequação à norma protetiva de dados pessoais e um melhor gerenciamento dos dados pessoais.

4.4. A heterorregulação: instituições e órgãos de *enforcement*

Os órgãos de *enforcement* são fundamentais para a manutenção da tutela de dados pessoais, uma vez que estabelecem diretrizes e limites práticos aos agentes responsáveis pelo tratamento, seja pelo medo de sofrerem sanções em decorrência do desrespeito às regras, seja pelo respeito aos ditames da legislação de proteção de dados sem que haja necessariamente outro fim por trás das ações, o que já foi mencionado anteriormente na abordagem dos imperativos hipotético e categórico, de Immanuel Kant.

Repisa-se, também, a importância da autorregulação dos controladores para que seja alcançada de maneira efetiva as premissas, condições e imposições previstas na LGPD, uma vez que o Estado não possui a infraestrutura adequada e suficiente para fiscalizar, direcionar e,

[188] Op.cit., p. 5.

eventualmente, punir agentes que violarem a norma protetiva de dados pessoais e causarem danos aos titulares.

Essa infraestrutura já é caracterizada em alguma medida, antes mesmo do início das discussões sobre a Lei n. 13.709/2018, por agentes como o órgão de Proteção e Defesa do Consumidor, PROCON, a Secretaria Nacional do Consumidor, SENACON, e o Ministério Público. Isso porque, como dito no capítulo um, já existiam algumas normas esparsas e setoriais que protegiam os dados dos titulares em situações específicas.

A atuação do PROCON, por exemplo, ocorreu no caso do aplicativo *FaceApp*[189], que foi notificado para prestar esclarecimentos a respeito da política de coleta, tratamento e armazenamento de dados dos consumidores que utilizam o aplicativo.

Posteriormente, o mesmo órgão aplicou uma multa severa ao Google e à Apple em virtude de o idioma utilizado na política de privacidade do aplicativo não ser o português[190].

O Ministério Público, por sua vez, ajuizou, em julho de 2019, uma ação civil pública contra uma empresa de telefonia que, segundo o MP, coleta e trata informações sobre o perfil, a geolocalização, o histórico de navegação e de locais frequentados pelos usuários da empresa, para traçar o comportamento destes de acordo com os interesses da empresa[191].

A Autoridade Nacional de Proteção de Dados, a ANPD, instituída pela Lei n. 13.853/2019, terá papel primordial no fomento e na fiscalização de agentes de tratamento, que deverão adotar medidas de segurança para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de tratamento de dados pessoais, consoante dispõe o art. 46, § 1º, da LGPD.

Ressalta-se que tais instituições responsáveis pela heterorregulação, relacionada à proteção de dados, devem agir para além da perspectiva de comando e controle, em que prevalece a imposição de deveres coercitivos.

---

[189] ARAÚJO, Priscila. *O aplicativo que 'envelhece' e a coleta de dados pessoais sensíveis.* JOTA, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-aplicativo-que-envelhece-e-a-coleta-de-dados-pessoais-sensiveis-28072019. Acesso em 09/09/2019.

[190] BAQUI, Maria. *PROCON multa Google e Apple por causa de termos do aplicativo FaceApp.* Correio Brasiliense, 30/08/2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2019/08/30/interna-brasil,779977/as-multas-tem-valor-de-r-9-964-615-77-e-r-7-744-320-00.shtml. Acesso em 08/09/2019.

[191] Ministério Público do Distrito Federal e Territórios. *MPDFT pede à justiça a suspensão de serviço da operadora Vivo.* MPDFT, jul. 2019. Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/11076-mpdft-pede-a-justica-a-suspensao-de-servico-da-operadora-vivo. Acesso em 06/09/2019.

Ademais, a Lei Geral de Proteção de Dados dispõe, no art. 52 e seguintes, sanções e advertências que sofrerão os agentes de tratamento de dados, caso não observem os preceitos instituídos pela lei.

A autoridade irá compor a administração pública federal, será integrante da Presidência da República e terá natureza jurídica transitória, o que importa dizer que, em até dois anos, o Poder Executivo deverá avaliar a transformação da ANPD em entidade da administração pública feral indireta, submetida ao regime autárquico especial vinculado, também, à Presidência da República.

Beto Vasconcelos e Felipe de Paula[192], inclusive, ressaltam que elementos como a garantia da independência, da autonomia e da elevada *expertise* técnica serão essenciais para a autoridade nacional alcançar até mesmo padrões internacionais de regulação, além de assegurar a existência de "mecanismos eficazes de participação e controle social".

Espera-se, portanto, que a Autoridade Nacional de Proteção de Dados inspecione, avalie e fiscalize agentes que realizarem o tratamento irregular de dados pessoais, especialmente os dados pessoais sensíveis, a fim de mitigar danos e a formação de cenários discriminatórios a partir da formação de perfis comportamentais que têm como base dados pessoais sensíveis.

4.5. O consentimento e o tratamento de dados pessoais sensíveis

O *General Data Protection Regulation* define o consentimento como "(...) uma manifestação de vontade, livre específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento", consoante disposto no artigo 4 (11).

Já a LGPD prevê, em seu art. 7º, inciso I, o consentimento, assim entendido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[193] como uma das hipóteses para o tratamento de dados pessoais.

O requisito "livre" orienta-se no sentido de dar ao titular a oportunidade de escolha entre aceitar ou recusar o tratamento dos seus dados. Assim, a liberdade de escolha dada ao indivíduo

---

[192] VASCONCELOS, Beto. PAULA, Felipe de. *A autoridade nacional de proteção de dados: origem, avanços e pontos críticos.* In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, ed. Revista dos Tribunais, 2019, p. 734.

[193] Definição de consentimento conforme o art. 5º, inciso XII, da lei Geral de Proteção de Dados.

deve ser analisada à luz da eventual vulnerabilidade presente na relação entre o controlador e a pessoa, pois tal assimetria pode gerar um vício de consentimento, que mitiga a liberdade prevista na lei[194].

Paul Reynolds[195] entende que o consentimento informado deve ser dado por pessoas que sejam capazes de consentir, que essa concessão deve ser feita de forma voluntária e que deve haver a informação a respeito do objeto a ser concedido, bem como o entendimento das pessoas sobre a mensagem transmitida pelo controlador a respeito da utilização desses dados e da necessidade de se consentir.

Tal visão coaduna-se com aquela defendida por Eugenia Politou, Efthimios Alepis e Constantinos Patsakis[196], os quais defendem que os requisitos do consentimento são a última defesa para os usuários contra a perda de controle no que diz respeito ao processamento dos seus dados e das suas informações pessoais, de modo que, reduzir ou eliminar a necessidade de consentimento informado não pode ser aceito em uma sociedade caracterizada pela valorização de ideais democráticos.

Para o tratamento dos dados pessoais sensíveis, aqueles que integram o que Gustavo Tepedino e Chiara Teffé[197] chamam de "núcleo duro" da privacidade, o consentimento deve ser analisado segundo critérios mais rígidos.

Dessa forma, segundo a LGPD, o tratamento de dados pessoais sensíveis pode ocorrer: "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas" e "sem o fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (...); e) proteção da vida ou da incolumidade física do titular ou de terceiro" f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da preservação à fraude e à segurança do titular,

---

[194] TEFFÉ, Chiara Spadaccini de. TEPEDINO, Gustavo. *Consentimento e proteção de dados pessoais na LGPD*. In: TEPEDINO, Gustavo. FRAZÃO, Ana. OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.* Thomson Reuters, ed. Revista dos Tribunais, 2019, p. 299.

[195] Reynolds, PD. *Ethical Dilemmas and Social Science Research*. San Francisco, USA: Jossey-Bass Inc Pub, 1979.

[196] POLITOU, Eugenia. ALEPIS, Efthimios. PATSAKIS, Constantinos. *Forgetting personal data and revoking consente under the GDPR: Challenges and proposed solutions.* Journal of Cybersecurity, Greece, 2018, Vol. 0, N. 0. p. 5.

[197] Op.cit., p. 307.

nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

A primeira hipótese de tratamento de dados pessoais sensíveis elencada pela Lei n. 13.709/2018 invoca o consentimento o titular ou do responsável legal, de forma específica e destacada, além da finalidade específica de tratamento. Diferentemente da previsão do art. 7º, inciso I, que trata do consentimento para os dados pessoais que não são sensíveis, há a necessidade de haver o destaque do consentimento, isto é, a norma robusteceu o arcabouço protetivo para os dados pessoais sensíveis a fim de se evitar que a utilização desse tipo de dado restrinja o acesso a bens, serviços e ao exercício de direitos fundamentais[198].

Desse modo, o consentimento, além de ser livre, informado e inequívoco, deve, também, ser específico e destacado quando o tratamento se referir aos dados pessoais sensíveis. Isto é, o legislador inseriu a ideia de um consentimento expresso e mais assertivo, de modo a proporcionar um nível de cautela muito maior para o tratamento de dados pessoais sensíveis[199].

Tal inserção foi necessária, pois existem instituições públicas e agentes econômicos que, em sua gênese, foram criados para tratarem diretamente ou indiretamente dados que dizem respeito à origem racial ou étnica, como algumas pesquisas feitas Instituto Brasileiro de Geografia e Estatística, o IBGE; dados relacionados à convicção religiosa, como aqueles utilizados em levantamentos da Confederação Nacional dos Bispos do Brasil, CNBB; dados sobre opinião política, como aqueles empregados pelo Datafolha; dados relacionados à filiação a sindicato, como as diversas associações e entidades associativas de servidores públicos; dados referentes à saúde, como aqueles usados pelo Sistema Único de Saúde, SUS; dados genéticos manipulados por laboratórios, dentre outras inúmeras situações que abarcam, necessariamente, o tratamento de dados pessoais sensíveis.

O destaque do consentimento é importante, também, para ater o tratamento de dados apenas à finalidade específica invocada pelo agente de tratamento, que informou sobre a manipulação de dados de maneira clara o titular, inclusive na hipótese de formação de perfis, e que cumpriu as obrigações informacional e dialógica, defendidas por Rafael Zanatta.

Um modelo de gerenciamento de dados, que visa à conformidade à noção de proteção de dados por meio do consentimento informado, foi desenvolvido por Kaniz Fatema, Ensar Hadziselimovic, Harshvardhan Pandit, Christophe Debruyne, Dave Lewis e Declan O'Sullivan,

[198] Op.cit., p. 308.
[199] Op.cit., p. 309.

pesquisadores irlandeses que defendem o investimento em ferramentas que dão suporte à obtenção do consentimento informado por agentes manipuladores de dados pessoais[200].

Dessa forma, para uma boa ingerência do consentimento informado, informações como a data, hora, local, o formato da coleta e as próprias informações fornecidas, quando o consentimento for solicitado, permitem a modelagem e a tomada de providências pelo controlador, que terá o consentimento mapeado[201].

A gestão correta do consentimento, segundo os pesquisadores, ajuda a produzir uma representação inteligível e fácil de ser utilizada, de modo que auxilia, ainda, na migração do modelo de consentimento de um domínio para outro a depender da escolha do controlador.[202]

Essa escolha, por fim, deve respeitar os princípios, fundamentos, requisitos e hipóteses autorizadoras de tratamento de dados elencados pela Lei Geral de Proteção de Dados e a gestão do consentimento deve ser feita de maneira ainda mais prudente quando se tratar de dados pessoais sensíveis, a fim de se evitar a criação ou o agravamento de cenários discriminatórios, preconceituosos e até mesmo a geração de danos aos titulares desses dados.

Por todo o exposto, a Lei n. 13.709/1018 deverá reformular, na prática, o que se entende por consentimento e até mesmo as demais hipóteses autorizadoras do tratamento de dados pessoais.

---

[200] FATEMA, Kaniz. HADZISELIMOVIC, Ensar. PANDIT, Harshvardhan. DEBRUYNE, Christophe. LEWIS, Dave. O'SULLIVAN, Declan. *Compliance through Informed Consent: Semantic Based Consent Permisson and Data Management Model.* ADAPT Centre, Trinity College Dublin, Ireland, 2019.
[201] Op.cit., pp. 5-6.
[202] Op.cit., pp. 8.

CONCLUSÃO

A utilização de dados pessoais, em especial os dados sensíveis, suscita inúmeras discussões em uma economia movida a dados, que versa sobre o paradoxo da constante vigilância dos agentes de tratamento em detrimento da constante opacidade enfrentada pelos titulares desses dados pessoais, que pouco ou nada sabem a respeito da coleta, do tratamento, do armazenamento e da eliminação das suas informações.

Como exposto no presente trabalho, a Lei Geral de Proteção de Dados, Lei n. 13.709/2018, buscou introduzir preceitos, fixar diretrizes, estabelecer a base principiológica e prever situações, bem como determinar funções a determinadas figuras e impor sanções aos agentes de tratamento que não observarem a referida lei.

Desse modo, princípios como o da adequação, da necessidade e da finalidade; definições relevantes como os conceitos de dados pessoais, dados pessoais sensíveis, tratamento, os agentes de tratamento, quais sejam, o controlador e o operador, além do encarregado (ou *Data Protection Officer*) são essenciais para a aplicação da norma, que terá o início da sua vigência em agosto de 2020.

Outro preceito fixado pela LGPD que possui extrema importância é o princípio da não discriminação, que terá papel fundamental no tratamento de dados pessoais que abranjam questões de saúde, biometria, filiação partidária ou sindical, temas religiosos, dados a respeito da orientação sexual dos indivíduos, dentre outras informações sensíveis e íntimas dos usuários, que demandam um nível protetivo ainda maior, a fim de se evitar a configuração de dano ou de cenários preconceituosos, classificatórios e discriminatórios, que segregam indivíduos e grupos sociais.

Nessa linha, o conhecimento do "poder dos algoritmos" e das suas decisões é estrutural para o entendimento do presente trabalho, que busca abordar situações as quais, revestidas de opacidade pelos agentes de tratamento de dados pessoais, não costumam ser claras aos usuários, que fornecem seus dados sem terem o suficiente e necessário entendimento a respeito da utilização e da finalidade para qual as suas informações são tratadas.

Por isso, inclusive, buscou-se exemplificar situações em que os agentes de tratamento extraem e utilizam tais dados, como o exemplo da plataforma de *streaming;* a coleta de dados de saúde por meio de vídeos; o reconhecimento facial protagonizado pela concessionária da Linha 4 do metrô de São Paulo; a atuação do "Torcedor Artificial", inteligência artificial desenvolvida para interagir com os torcedores de times que disputam a Libertadores da América; a definição da orientação sexual de um indivíduo apenas por meio da análise de fotos

por algoritmos específicos; a utilização de dados pessoais sensíveis e de informações disponíveis em redes sociais por parte de empregadores ou de potenciais empregadores, que não mais promovem processos seletivos e a manutenção de trabalhadores apenas com base no desempenho destes, entre outros.

Dessa forma, além de suscitar e desenvolver temas extremamente delicados a respeito das informações pessoais sensíveis dos usuários, entende-se que um dos objetivos do estudo foi alcançado, qual seja, alertar para a ocorrência de dano ao titular e para a configuração de cenários de discriminação por meio da manipulação de dados pessoais sensíveis na formação de perfis de comportamento.

Isso porque, tais perfis baseados em informações sensíveis segregam grupos étnicos e raciais, marginalizam pessoas que não possuem condições financeiras elevadas, impõe a orientação sexual que deve ser predominante em detrimento de toda a diversidade humana a respeito do tema, permite que agentes econômicos voltados para o setor da saúde ofereçam produtos e serviços mais caros a um determinado grupo de indivíduos, que foram classificados e colocados em "caixinhas" específicas como, por exemplo, a oferta de seguros de vida muito mais caros para indivíduos que, em tese, possuem maior predisposição a desenvolverem problemas cardíacos.

Nota-se que a formação de perfis, ainda que seja feita em prol da publicidade comportamental, restringe a oferta de produtos e serviços aos usuários, de sorte que abre discussões a respeito da medida em que a publicidade direcionada se constitui como um avanço tecnológico que facilita as compras e a contratação de serviços pelos usuários ou apenas promove a limitação de bens e serviços.

O presente trabalho buscou, também, abordar questões a respeito da responsabilidade civil dos agentes de tratamento de dados, de modo que esses agentes possuem toda a informação a respeito desse tratamento, inclusive por meio do dever de registro que será imposto, principalmente, pela Autoridade Nacional de Proteção de Dados.

Dessa forma, buscou-se integrar as responsabilidades subjetiva e objetiva, com base na análise da previsão, do cumprimento do dever de cuidado, da culpa normativa e da teoria do risco, uma vez que o Judiciário deverá se deparar, com o advento efetivo da LGPD, com situações em que haverá o tratamento de dados pessoais, especialmente os sensíveis, e que as soluções dadas formarão, aos poucos, a jurisprudência que tratará do tema, seja na forma da responsabilidade subjetiva, seja na forma da responsabilidade objetiva.

O instituto da inversão do ônus probatório também foi tratado como uma importante ferramenta, que terá o titular dos dados pessoais coletados, em Juízo para pleitear por reparações indenizatórias dadas em decorrência de danos.

Ademais, tentou-se abordar a importância da autorregulação e da promoção de programas de *Compliance* nas organizações, a fim de que o tratamento de dados pessoais seja feito por meio de boas e lícitas práticas, que tenham como base a boa-fé dos agentes.

Para tanto, o modelo *privacy by design* é colocado como um instrumento capaz de, aliado às boas práticas, introduzir algoritmos, softwares e dispositivos que tenham a privacidade como ponto estrutural em sua arquitetura, trabalho que deverá ser fomentado pelos desenvolvedores desses algoritmos, pelos operadores, pelos controladores e pelo próprio encarregado.

A perfilização é, portanto, uma ferramenta poderosa para os *players* e para o Poder Público, a depender da atividade que exercem, e constitui-se como um instrumento de padronização da sociedade, que possui uma vasta diversidade a qual proporciona, desde o início, a produção de novos pensamentos, movimentos políticos e culturais, ideias, projetos científicos e outras tantas situações viabilizadas por meio da criatividade e das diferenças entre indivíduos e grupos sociais.

Desse modo, classificar as pessoas de acordo com a sua cultura, crenças, orientação sexual, cor dos olhos ou do cabelo, formato do rosto, estatura, de acordo com a intensidade em que praticam atividade física, com a qualidade da sua alimentação e com outras tantas informações coletadas de cada indivíduo único, seria negar o impulso à evolução humana, ao avanço civilizatório e seria negar até mesmo a própria democracia, que também é ameaçada por meio da manipulação de dados e da tomada de decisões algorítmicas.

REFERÊNCIAS

ALVIM, Agostinho. *Culpa e risco.* 2ª ed. Ver. E atual. Por Ovídio Rocha Barros Sandoval. São Paulo: Revista dos Tribunais, 1998, pp. 108-109.

ARAÚJO, Priscila. *O aplicativo que 'envelhece' e a coleta de dados pessoais sensíveis.* JOTA, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-aplicativo-que-envelhece-e-a-coleta-de-dados-pessoais-sensiveis-28072019. Acesso em 09/09/2019.

ARENDT, Hannah. *A vida do espírito.* Tradução de Ant&onio Abranches, Cesar Augusto R. de Almeida e Helena Martins Ed. 4ª. Rio de Janeiro: Editora Relume Dumará, 2000, p. 37.

ARTHUR, Charles. *Tech gigants may be huge, but nothing matches big data: When Nasdaq stopped trading this week, it again showed how global firms are at the mercy os a power that created them.* The Guardian, 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em 12/07/2019.

BANDEIRA, Paula Greco. *A Evolução do Conceito de Culpa e o Artigo 944 do Código Civil.* Revista da Escola da Magistratura do Estado do Rio de Janeiro, v. 11, n. 42, 2008, p. 232.

BAQUI, Maria. *PROCON multa Google e Apple por causa de termos do aplicativo FaceApp.* Correio Brasiliense, 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2019/08/30/interna-brasil,779977/as-multas-tem-valor-de-r-9-964-615-77-e-r-7-744-320-00.shtml. Acesso em 08/09/2019.

BBC News Brasil. *O que acontece quando você aceita os cookies de um site e por que é bom apaga-los de tempos em tempos*. [S.I.], 2017. Disponível em: https://www.bbc.com/portuguese/geral-40730996. Acesso em 01/08/2019.

BENNETT, Colin. *Regulating Privacy: data Protection and public policy in Europe and the United State.* Cornell University Press, Ithaca and London, 1992, pp. 98-99.

BENNETT, Colin J; RAAB, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective.* Massachusetts Institute of Technology, 2006.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento.* Rio de Janeiro: Editora Forense, 2018.

BORGESIUS, Frederik Zuiderveen. *Discrimination, artificial intelligence, and algorithmic decision-making.* Directorate General of Democracy, Concil of Europe, 2018.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14/09/2019.

BRASIL. Decreto n. 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.in.gov.br/web/dou/-/decreto-n-10.046-de-9-de-outubro-de-2019-221056841. Acesso em 12/10/2019.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. *Código de Defesa do Consumidor*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/l8078.htm. Acesso em 24/04/2019.

BRASIL. Lei n. 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm. Acesso em 28/04/2019.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. *Código Civil*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em 22/04/2019.

BRASIL. Lei n. 12.414, de 9 de junho de 2011. *Lei do Cadastro Positivo*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 01/05/2019.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. *Lei de Acesso à Informação*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 01/05/2019.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01/05/2019.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais*. Dispõe sobre a proteção de dados pessoais e altera a Lei N. 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 15/05/2019.

BRASIL. Projeto de Lei da Câmara n. 53/2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em 01/07/2019.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1419697/RS. Recorrente: Boa Vista Serviços S.A. Recorrido: Anderson Guilherme Prado Soares. 2ª Seção, Relator: Min. Paulo de Tarso Sanseverino, DJe em 17/11/2014. Disponível em: http://www.stj.jus.br. Acesso em 12/09/2019.

BRIDLE, James. Opinion: *Data isn't the new oil – it's the new nuclear power*. Ideas.Ted.Com, 2018. Disponível em: https://ideas.ted.com/opinion-data-isnt-the-new-oil-its-the-new-nuclear-power/. Acesso em 12/07/2019.

BROWN, Dalvin. *People watch Netflix while 'on the go' and the company reportedly wants that data*. USA TODAY, 2019. Disponível em: https://www.usatoday.com/story/tech/2019/08/01/why-does-netflix-app-want-access-your-physical-activity/1887032001/. Acesso em 04/09/2019.

BUSSCHE, Axel von dem; VOIGT, Paul. *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Springer Verlag NY, 2017.

CABAÑAS, José González; CUEVAS, Ángel; CUEVAS, Rubén. *Facebook use of sensitive data for Advertising in Europe.* Computer Science, Social and Information Networks. Cornell University, New York, 2018. Disponível em: https://arxiv.org/abs/1802.05030. Acesso em 01/05/2019.

CADWALLADR, Carole; HARRISON, Emma Graham. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 20/08/2019.

CALISKAN, Aylin; BRYSON, Joanna J.; NARAYANAN, Arvind. *Semantics derived automatically from language corpora contain human-like biases*. Science, reports, psychology. 356(6334). 2017, pp. 183-186.

CAMARGO, José A. *O direito à integridade psicofísica nos direitos brasileiro e comparado*. Revista da Seção Judiciária do Rio de Janeiro, Rio de Janeiro, n. 26, 2009, p. 272.

CARVALHO, Victor M. Barros de. *O direito à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória.* Dissertação (mestrado em direito). Centro de Ciências Sociais aplicadas, Universidade Federal do Rio Grande do Norte. Natal, 2018.

CASTELLS, Manuel. *A sociedade em rede*. Vol. 1. 8ª ed. Trad.: Roneide Venancio Majer. São Paulo: Paz e Terra, 2005.

CAVALIERI, Sergio Filho. Programa de responsabilidade civil. 3. ed. São Paulo: Malheiros, 2005. p. 18.

CAVOUKIAN, Ann. *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Information & Privacy Commissioner, Ontario, Canadá, 2009.

CHENEY-LIPPOLD, John. *We are data. Algorithms and the making of our digital selves.* New York: New York University Press, 2017.

CHIRONI, Giampietro P. *La colpa nel diritto civile odierno: colpa extra-contrattuale.* 1925, p. 5.

CIO From IDG. *Como a Blackberry Cylance aplica Ciência de Dados para atender a LGPD*. [S.I.] 2019. Disponível em: https://cio.com.br/como-a-blackberry-cylance-aplica-ciencia-de-dados-para-atender-a-lgpd/. Acesso em 21/09/2019.

CLARKE, Roger. *Profiling: a hidden challenge to the Regulation of data surveillance.* Journal of Law & Information Science, v. 4, 1993, p. 403.

COHEN, Julie E. *Examined lives: informational privacy and the subject as object*. Stanford Law Review, v. 52, 2000, pp. 1373-1438.

Comissão Europeia. *Quais são as responsabilidades de um encarregado da proteção de dados (EPD)?* Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_pt. Acesso em 21/09/2019.

Committed to Improving the State of the World. World Economic Forum. Insight Report. *Our Shared Digital Future: Building an Inclusive, Trustworthy and Sustainable Digital Society.* Decem. 2018. Disponível em: http://www3.weforum.org/docs/WEF_Our_Shared_Digital_Future_Report_2018.pdf. Acesso em 05/09/2019.

CORRÊA, Rafael. *Responsabilidade civil e privacidade:* Autodeterminação informativa como expressão de liberdade positiva na construção da personalidade. Dissertação (Mestrado em Direito). Faculdade de Direito, Universidade Federal do Paraná. Curitiba, 2016, p. 141.

COSTA, Andréa Dourado; GOMES, Ana Virginia Moreira. *Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis*. Scientia Iuris, Londrina, v. 21, n. 2, jul. 2017.

CUEVA, Ricardo Villas Bôas. *Funções e finalidades dos programas de Compliance.* In: CUEVA, Ricardo Villas Bôas. FRAZÃO, Ana. *Compliance:* perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018, p. 53.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; PEREIRA DE LIMA, Cíntia Rosa. *Direito e Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, 2015.

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

DONEDA, Danilo. *A proteção de dados pessoais no ordenamento brasileiro e a ação de Habeas Data*. Rev. Democracia Digital e Governo Eletrônico. Universidade Federal de Santa Catarina, 2009, p. 128-142.

DONEDA, Danilo. *A tutela da privacidade no código civil de 2002.* Revista eletrônica do curso de direito. Centro Universitário UniOpet.

EPSTEIN, Robert; ROBERTSON, Ronald E. *The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections*. *PNAS.* Disponível em: https://papers-gamma.link/static/memory/pdfs/9-Epstein_Search_Engine_Manipulation_Effect_2015.pdf. Acesso em 10/05/2019.

EUBANKS, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* St. Martin's Press, New York. 2017.

FARR, Christina. *Apple and Eli Lilly are studying whether data from iPhones and Apple Watches can detect signs of dementia*. CNBC, 2019. Disponível em: https://www.cnbc.com/2019/08/07/apple-eli-lilly-studying-if-iphones-apple-watches-can-spot-dementia.html. Acesso em 02/09/2019.

FATEMA, Kaniz; HADZISELIMOVIC, Ensar; PANDIT, Harshvardhan; DEBRUYNE, Christophe; LEWIS, Dave; O'SULLIVAN, Declan. *Compliance through Informed Consent: Semantic Based Consent Permisson and Data Management Model*. ADAPT Centre, Trinity College Dublin, Ireland, 2019.

FERNÁNDEZ,Vicente J. Baixauli; SÁNCHEZ, Fernando Abellán-García. *El consentimiento y el tratamiento de los datos sanitários del paciente en la prestación y realización de estúdios de investigación de servicios profesionales farmacéuticos asistenciales.* Farmacéuticos comunitarios. Sociedad Española de Farmacia Familiar y Comunitaria. Volume 11, n. 1, mar. 2019.

FRAZÃO, Ana. *A nova Lei Geral de Proteção de Dados: Repercussões para a atividade empresarial: o tratamento dos dados pessoais sensíveis.* JOTA, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 20/07/2019.

FRAZÃO, Ana. *Corrupção e Compliance*. JOTA, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/corrupcao-e-compliance-03072018. Acesso em 21/09/2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. *Lei Geral de Proteção de Dados Pessoais* e suas repercussões no Direito Brasileiro. 1. Ed. Brasil: RT – Revista dos Tribunais, 2019.

FRAZÃO, Ana. *"Neurocapitalismo"e o negócio de dados cerebrais*. JOTA, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/neurocapitalismo-e-o-negocio-de-dados-cerebrais-25092019. Acesso em 25/09/2019.

FRAZÃO, Ana. *Nova LGPD: o tratamento de dados pessoais sensíveis*. JOTA, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em 03/06/2019.

FRAZÃO, Ana. *Risco da empresa e caso fortuito externo.* Civilistica.com. a. 5. n. 1. 2016.

GARFINKEL, Simson. *Database Nation: The Death of Privacy in the 21th Century*. O'Reilly Media: California, 2000, p. 5.

GONÇALVES, Carlos Roberto. *Responsabilidade civil.* São Paulo: Saraiva, 2019, p. 59.

GOSEPATH, Stefan. *Uma pretensão de direito humano à proteção fundamental*. Tradução de Cláudia Toledo e Bráulio Borges Barreiros. In: TOLEDO, Cláudia (Org.). Direitos Sociais em debate. Rio de Janeiro: Elsevier, 2013, pp. 79-80.

HILDEBRANDT, Mireille. *Defining profiling: a new type of knowledge*?. In: Profiling the European citizen. Springer, Dordrecht, 2008, p. 58.

IBRAHIM, Altaweel; GOOD, Nathan; HOOFNAGLE, Chris Jay. *Web Privacy Census*. SSRN scholarly paper, Social Science Research Network, Decemb. 2015. Disponível em: https://papers.ssrn.com/abstract=2703814. Acesso em 04/05/2019.

JANSSEN, Marijn; KUK, George. *The challenges and limits of big data algorithms in technocratic governance.* Government Information Quarterly 33. Delft University of Technology, The Netherlands and Nottingham Trent University, UK article, 2016, pp. 371-377.

JÚNIOR, Dirley da Cunha. *Curso de Direito Constitucional*. 9ª Ed. Salvador: Editora JusPodivm, 2015, p. 508

KANT, Immanuel. *Fundamentação da metafísica dos costumes.* Petrópolis, RJ: Editora Vozes. Bragança Paulista, SP: Editora Universitária São Francisco, 2013.

LEITE, Rita de Cássia Curvo. *Transplantes de órgãos e tecidos e dos direitos da personalidade.* São Paulo: Juarez de Oliveira, 2000, p. 157.

LESSIG, Lawrence. *Code and other laws of cyberspace*. New York: Basic Books, 1999.

LUPTON, Deborah. *Lively Data, Social Fitness and Biovalue: The Intersections of Health Self-Tracking and Social Media*. The Sage Handbook of Social Media, London, 2017, p. 5.

LYON, David. *Surveillance Technologyand Surveillance.* Modernity and Technology. Cambrige, Massachusetts: MIT Press, 2003, pp. 161-164.

MACEDO JR., Ronaldo Porto. *Privacidade, mercado e informação*. *Justitia*, São Paulo, n. 61 (185/188), jan/dez 1999, pp. 245-259, p. 247.

MAHIEU, René; ECK, Nees Jan van; PUTTEN, David van; HOVEN, Jeroen van den. *From dignity to security protocols: a scientometric analysis of digital ethics*. Ethics and Information Technology, 2018, pp. 175-187.

Máquina do esporte. *Por "comportamento on-line", Amstel cria "Torcedor Artificial": em parceira com o google, marca pretende impactar torcidas de forma positiva*. [S.I.], 2019. Disponível em: https://maquinadoesporte.uol.com.br/artigo/por-comportamento-line-amstel-cria-torcedor-artificial_38056.html. Acesso em 03/09/2019.

MARMELSTEIN, George. *Curso de Direitos Fundamentais*. São Paulo: Atlas, 2008.

MAYER-SHÖNBERGER, Viktor; RAMGE, Thomas. *Reiventing capitalism in the age of big data.* New York: Basic Books, 2008.

MELO, Diogo Leonardo Machado de. *Título III. Dos Atos Ilícitos.* In: NANNI, Giovanni Ettore (Org). *Comentários ao Código Civil: Direito Privado Contemporâneo.* Saraiva-jur, 2019, p. 1.275.

Ministério Público do Distrito Federal e Territórios. *MPDFT pede à justiça a suspensão de serviço da operadora Vivo.* MPDFT, jul. 2019. Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/11076-mpdft-pede-a-justica-a-suspensao-de-servico-da-operadora-vivo. Acesso em 06/09/2019.

MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais*?, Instituto Igarapé, Artigo Estratégico n. 39, dez. 2018, p. 11.

NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, California, 2010.

O'NEIL, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* B\D\W\Y, Broadway Books, New York, 2016.

PALLERO, Javier; BARATA, Joan; BETANCOURT, Valeria; PIAZZA, Andrés; MASTRINI, Guillermo; BECERRA, Martín; FREULER, Juan Ortiz. *Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet.* Uma perspectiva latino-americana para alcançar processos de moderação de conteúdo compatíveis com os padrões internacionais de direitos humanos. Elaboração: Intervozes, coletivo Brasil de comunicação social, Observacom, Desarrollo Digital, IDEC, agos. 2019. Disponível em: https://www.observacom.org/wp-content/uploads/2019/08/Contribuições-para-uma-regulação-democrática-das-grandes-plataformas-que-garanta-a-liberdade-de-expressão-na-internet.pdf. Acesso em 24/09/2019.

PARDO, David Wilson de Abreu. *Direitos fundamentais não-enumerados: justificação e aplicação*. Tese (Doutorado em Direito). Faculdade de Direito, Universidade Federal de Santa Catarina. Florianópolis, 2005, p. 12.

PASQUALE, Frank. *The Black Box Society*. Harvard University Press. Cambridge, Massachusetts. London, England. 2015.

PEREIRA, Caio Mário da Silva. TEPEDINO, Gustavo. *Responsabilidade Civil.*12ª ed. Rio de Janeiro: Editora Forensi, 2018, p. 14.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet.* 2ª ed. Curitiba: Juruá Editora, 2004, p. 140.

POLITOU, Eugenia; ALEPIS, Efthimios; PATSAKIS, Constantinos. *Forgetting personal data and revoking consente under the GDPR: Challenges and proposed solutions*. Journal of Cybersecurity, vol. 0, n. 0. 2018, pp. 1-20.

POULLET, Yves. *Is the general data protection regulation the solution?* Computer law & security review. Namur Digital Institute, University of Namur, Belgium, 2018, pp. 774-778.

PRESS, Gil. *12 Big Data Definitions: what's yours?* FORBES, 2014. Disponível em https://www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/#75a4dde313ae. Acesso em 01/05/2019.

Privacidade Hackeada. Direção de Jehane Noujam e Karin Amer. Estados Unidos da América: Netflix, 2019. 1 vídeo (114 min). Disponível em: https://www.netflix.com/watch/80117542?trackId=13752289&tctx=0%2C0%2Ccdd45955fcb2b2da595cef43785703207c9fcd1b%3Aeec9be793be34ecf74be7d5026f277a0ad7aefd4%2C%2C. Acesso em 23/09/2019.

REALE, Miguel. *Diretrizes gerais sobre o Projeto de Código Civil*. REALE, Miguel. Estudos de filosofia e ciência do direito. São Paulo: Saraiva, 1978, p. 176-177.

REYNOLDS, PD. *Ethical Dilemmas and Social Science Research*. San Francisco, USA: Jossey-Bass Inc Pub, 1979.

ROBERTO, Enrico; LOPES, Marcelo Frullani. *Quando um carro autônomo atropela alguém, quem responde? O verdadeiro tamanho do problema ainda é desconhecido, e as discussões a seu redor, incipientes*. El país, tecnologia, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/04/16/tecnologia/1523911354_957278.html. Acesso em 21/07/2019.

RODOTÀ, Stefano. *A Vida na Sociedade da Vigilância: a Privacidade Hoje.* Tradução de Danilo Doneda e Laura Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SALOMÃO, Kátia Rocha; JUNIOR, Waldomiro Salles Svokinski. *KANT: Os fundamentos da dignidade da pessoa humana como condição para uma hermenêutica do dever.* E-Civitas. Revista Científica dos Cursos de Direito e Relações Internacionais do UNIBH, Belo Horizonte, ISSN: 1984-2716. Disponível em: www.unibh.br/revistas/ecivitas. Acesso em 21/09/2019.

SATO, Luiza. *Um ano depois, GDPR mostra que adequação à LGPD é obrigatória.* Convergência digital, maio de 2019. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=50616&sid=15. Acesso em 12/09/2019.

SCHERTEL, Laura. *Habeas data e autodeterminação informativa. Os dois lados de uma mesma moeda.* Direitos Fundamentais & Justiça, v. 39, 2018, p. 350.

SCHERTEL, Laura. *Privacidade, Proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental*. 1ª ed. São Paulo: Saraiva, 2014.

SCHERTEL, Laura. *Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo*. Dissertação (Mestrado em direito), Faculdade de Direito, Universidade de Brasília. Brasília, 2008.

SCHNEIER, Bruce. *Data and Goliath. The hidden battles to collect your data and control your world*. New York: W.W. Norton & Company, 2015.

SCHWAB, Klaus. *The Fourth Industrial Revolution.* World Economic Forum. Currency. 2017. Secretaria de Governo Digital do Ministério da Economia, Administração dos Recursos de Tecnologia da Informação do Governo Federal (SISP) *Estudo sobre o compartilhamento de dados em outros países.* Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/Relatorio%20Estudo%20Troca%20Informacoes%20Outros%20Paises.pdf. Acesso em 04/09/2019.

SOLOVE, Daniel. *Understanding privacy*. Cambridge: Harvard University Press, 2008, p. 8.

SOMERS, Geert. BOGHAERT, Liesa. *The California Consumer privacy Act and The GDPR: two of a kind?* Expert briefin, Data privacy. Financier worldwide. Disponível em: https://www.financierworldwide.com/the-california-consumer-privacy-act-and-the-gdpr-two-of-a-kind#.XW2CuJNKh-U Acesso em 02/09/2019.

TAMBOU, Olivia; BERNAL, Paul; HU, Margaret; MOLINARO, Carlos Alberto; NEGRE, Elsa; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; WITZLEB, Normann; YGER, Florian. *The Regulation of Commercial Profiling: a Comparative Analysis.* European Data Protection Law Review, v. 2, 2016, p. 535-554.

TAPSCOTT, Don. *The Digital Economy: Promise and Peril in the Age os Networked Intelligence.* McGraw-Hill, 1995.

TARTUCE, Flávio. *Direito Civil: Direito das Obrigações e Responsabilidade Civil.* 12ª edição. Rio de Janeiro: Editora Forense, 2017, p. 434.

U. S. Department of Health, Education and Welfare. *Report of the Secretary's Advisory Committe on Automated Personal Data Systems*, 1973. Disponível em: www.justice.gov/opcl/docs/rec-com-rights.pdf. Acesso em 10/09/2019.

UNIÃO EUROPEIA. Regulamento (UE) n. 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em 16/04/2019.

VINEY, Geneviève; JOURDAIN, Patrice; CARVAL, Suzanne. *Les conditions de la responsabilité.* 4ª ed. Paris: LGDJ, 2013, p. 445.

VEIGA, Itamar Soares. *Democracia e Tecnologia: nos caminhos do ator não social.* Supere Aude, Belo Horizonte, v. 9, n. 17, 2018, p. 16, 26-27.

WACHTER, Sandra. *Normative challenges os identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR.* Computer Law & Security Review 34. Oxford Internet Institute, University of Oxford and The Alan Turing Institute, British Library, London, United Kingdom Keywords, 2018, pp. 436-449.

WANG, Yilun. KOSINSKI, Michal. *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.* Journal of Personality and Social Psychology, 2017, p. 16.

World Economic Forum. Committed to Improving the State os the World. *An Initiative of the World Economic Forum January 2011*. In Collaboration with Bain & Company, Inc. Disponível em: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf Acesso em 20/04/2019.

WU, Hao-Yu. RUBINSTEIN, Michael. SHIH, Eugene. GUTTAG, John V. DURAND, Fredo. *Eulerian vídeo magnification for revealing subtle changes in the world.* ACM Transactions on Graphics 31, n. 4. Jul. 2012, pp. 1-8.

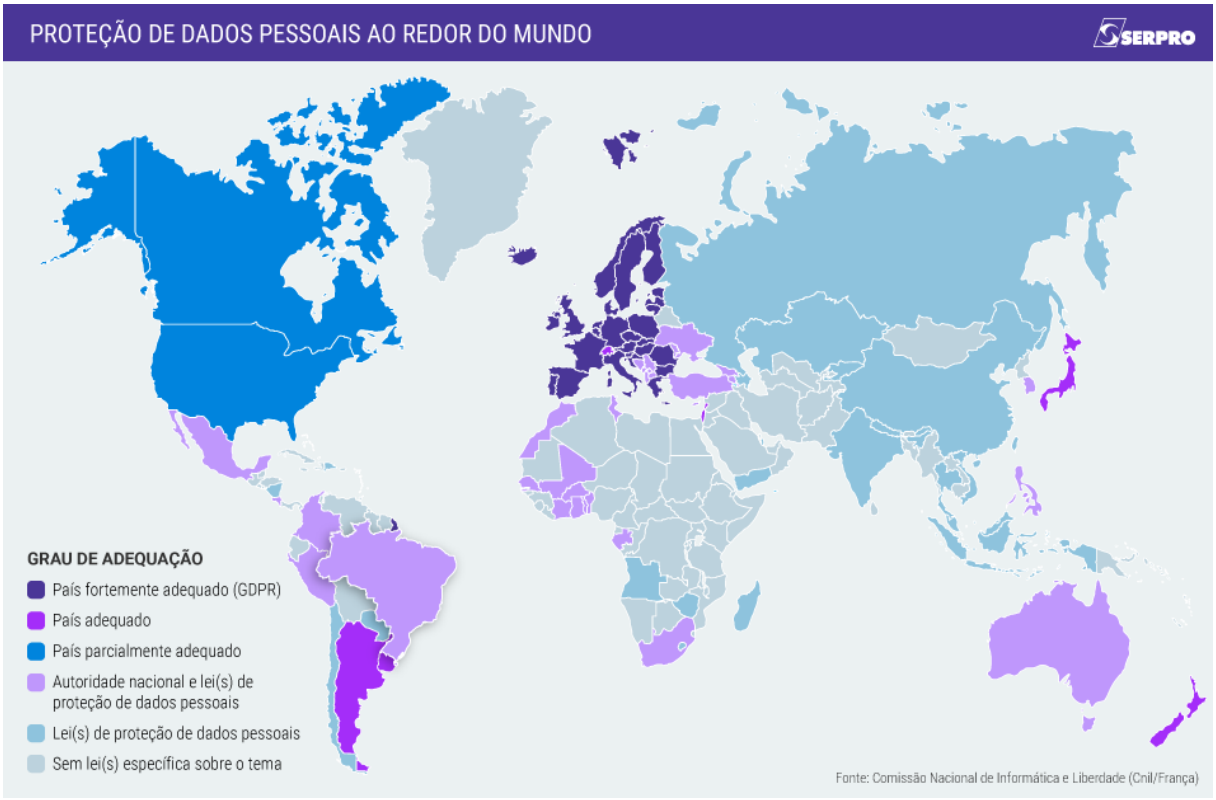
ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais.* Universidade de São Paulo, São Paulo, fev. 2019, pp. 1-26.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs, 2019.

ZUBOFF, Shoshana. *Big other: surveillance capitalism and the propects of an information civilization.* Journal of Information Technology, 30, 2015, pp. 75-89.

ANEXOS

ANEXO A – MAPA SOBRE A PROTEÇÃO DE DADOS PESSOAIS AO REDOR DO MUNDO



Fonte: Comissão Nacional de Informática e Liberdade (Cnil/França)