UNIVERSIDADE FEDERAL DE MINAS GERAIS
Faculdade de Direito e Ciências do Estado
Programa de Pós-Graduação em Direito

Gustavo Duarte Vieira

PROTEÇÃO DE DADOS PESSOAIS EM PRÁTICAS DE *PROFILING* NO SETOR PRIVADO

Belo Horizonte
2019

Gustavo Duarte Vieira

PROTEÇÃO DE DADOS PESSOAIS EM PRÁTICAS DE *PROFILING* NO SETOR PRIVADO

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do título de Mestre em Direito (versão final).
Linha de Pesquisa: História, Poder e Liberdade
Área de Estudo: Direito Civil na Interdisciplinaridade
Orientador: Prof. Dr. Fabio Queiroz Pereira

Belo Horizonte
2019

Vieira, Gustavo Duarte
V658p Proteção de dados pessoais em práticas de profiling no setor privado / Gustavo Duarte Vieira. — 2019.

Orientador: Fábio Queiroz Pereira.
Dissertação (mestrado) – Universidade Federal de Minas Gerais, Faculdade de Direito.

1. Direito civil – Teses 2. Direito à privacidade 3.Big data 4. Proteção de dados 5. Discriminação – Teses I. Título

CDU(1976) 347.121.1

Ficha catalográfica elaborada pelo bibliotecário Junio Martins Lourenço CRB 6/3167.

DEFESA DE DISSERTAÇÃO DE MESTRADO
ÁREA DE CONCENTRAÇÃO: DIREITO E JUSTIÇA
BEL. GUSTAVO DUARTE VIEIRA

Aos quatorze dias do mês de janeiro de 2020, às 14h00, no Auditório Francisco Luiz da Silva Campos da Faculdade de Direito da Universidade Federal de Minas Gerais, reuniu-se, em sessão pública, a Banca Examinadora constituída de acordo com o art. 73 do Regulamento do Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, e das Normas Gerais de Pós-Graduação da Universidade Federal de Minas Gerais, integrada pelos seguintes professores: Prof. Dr. Fabio Queiroz Pereira (orientador do candidato/UFMG); Prof. Dr. Giordano Bruno Soares Roberto (UFMG) e Prof. Dr. Felipe Quintella Machado de Carvalho (Faculdade Milton Campos), designados pelo Colegiado do Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, para a defesa de Dissertação de Mestrado do **Bel. GUSTAVO DUARTE VIEIRA**, matrícula nº **2018653142**, intitulada: **"PROTEÇÃO DE DADOS PESSOAIS EM PRÁTICAS DE PROFILING NO SETOR PRIVADO"**. Os trabalhos foram iniciados pelo Presidente da mesa e orientador do candidato, Prof. Dr. Fabio Queiroz Pereira, que, após breve saudação, concedeu ao candidato o prazo máximo de 30 (trinta) minutos para fins de exposição sobre o trabalho apresentado. Em seguida, passou a palavra ao Prof. Dr. Giordano Bruno Soares Roberto, para o início da arguição, nos termos do Regulamento. A arguição foi iniciada, desta forma, pelo Prof. Dr. Giordano Bruno Soares Roberto, seguindo-se-lhe, pela ordem, os Professores Doutores: Felipe Quintella Machado de Carvalho e Fabio Queiroz Pereira. Cada examinador arguiu o candidato pelo prazo máximo de 30 (trinta) minutos, assegurando ao mesmo, igual prazo para responder às objeções cabíveis. Cada examinador atribuiu conceito ao candidato, em cartão individual, depositando-o em envelope próprio. Recolhidos os envelopes, procedeu-se a apuração, tendo se verificado o seguinte resultado:

Prof. Dr. Fabio Queiroz Pereira (orientador do candidato/UFMG)
Conceito: APROVADO COM NOTA 100 (CEM)

Prof.Dr. Giordano Bruno Soares Roberto (UFMG)
Conceito: APROVADO COM NOTA 100 (CEM)

Prof.Dr. Felipe Quintella Machado de Carvalho (Faculdade Milton Campos)
Conceito: aprovado com nota cem

A Banca Examinadora considerou o candidato.....APROVADO....., com nota.....Nada mais havendo a tratar, o Professor Doutor Fabio Queiroz Pereira, Presidente da Mesa e Orientador do candidato, agradecendo a presença de todos, declarou encerrada a sessão. De tudo, para constar, eu, Fernanda Bueno de Oliveira, Servidora Pública Federal lotada no Programa de Pós-Graduação em Direito da UFMG, mandei lavrar a presente Ata, que vai assinada pela Banca Examinadora e com o visto do candidato.

BANCA EXAMINADORA:

Prof. Dr. Fabio Queiroz Pereira (orientador do candidato/UFMG)

Prof.Dr. Giordano Bruno Soares Roberto (UFMG)

Prof.Dr. Felipe Quintella Machado de Carvalho (Faculdade Milton Campos)

- CIENTE: Gustavo Duarte Vieira (Mestrando)

RESUMO

O advento da internet e a difusão de tecnologias digitais nos últimos anos resulta em grandes mudanças nas relações econômicas e sociais. O *profiling* é uma espécie de tratamento de dados pessoais que se torna cada vez mais comum nesse contexto, em que surge uma economia baseada em dados. Esse procedimento envolve a construção de perfis a partir da análise automatizada de grandes quantidades de dados coletados acerca de um indivíduo ou de um grupo, com o objetivo de se tomar uma decisão em relação ao sujeito perfilado. Assim como a maioria das tecnologias, observa-se ganhos importantes com seu uso, principalmente em termos de eficiência e eficácia de análises preditivas. Porém, o uso irrestrito pode significar importantes efeitos prejudiciais ao desenvolvimento da vida privada dos indivíduos, por possibilitar previsões de comportamento ou de características de um sujeito de maneira invasiva à sua privacidade, assim como a discriminação de pessoas submetidas a um perfil estereotipado. Nesse sentido, o presente trabalho visa identificar quais devem ser os limites legais do *profiling* feito por agentes do setor privado, de forma a se mitigar as mazelas que decorrem desse tipo de tratamento de dados. Partindo-se da ideia proposta por Daniel Solove, de que existe uma burocracia no fluxo de dados pessoais entre atores do setor privado, observa-se a necessidade de uma arquitetura de controle que integre leis e tecnologias, para alterar significativamente as estruturas que envolvem o tratamento de informações. Portanto, busca-se demonstrar que é necessário que as legislações relativas à proteção de dados pessoais criem formas controle sobre dados de diversos níveis para se garantir efetiva privacidade e igualdade dos sujeitos cujos dados são utilizados para definição de perfis. Tendo em vista a Lei Geral de Proteção de Dados, aprovada no Brasil em 2018, e a *General Data Protection Regulation*, que entrou em vigor no mesmo ano na União Europeia, são analisados aspectos das regulações que hoje compõe a arquitetura de controle sobre dados e que efetivamente definem os limites legais do *profiling*.

Palavras Chave: *Profiling.* Proteção de dados pessoais. Privacidade. Discriminação.

ABSTRACT

The advent of the Internet and the spread of digital technologies in recent years has resulted in major changes in economic and social relations. Profiling is a kind of personal data processing that is becoming increasingly common in this context, in which a data-based economy arises. This procedure involves the construction of profiles based on the automated analysis of large amounts of data collected about an individual or a group, in order to make decisions regarding the profiled subject. As with most technologies, there are significant gains from its use, especially in terms of the efficiency and effectiveness of predictive analytics. However, its unrestricted use can mean important detrimental effects on the development of the individual's private life, as it allows predictions of behavior or characteristics of a subject that is invasive to their privacy, as well as the discrimination of people subjected to a stereotyped profile. In this sense, the present work aims to identify what should be the legal limits of profiling done by private sector agents, in order to mitigate the problems that result from this type of data processing. Based on the idea proposed by Daniel Solove that there is a bureaucracy in the flow of personal data between private sector actors, there is a need for a control architecture that integrates laws and technologies to significantly change the structures that involve the treatment of information. Therefore, we seek to demonstrate that it is necessary that the laws related to the protection of personal data should create ways to control data at various levels to ensure effective privacy and equality of subjects whose data are used for profiling. In view of the General Data Protection Act, approved in Brazil in 2018, and the General Data Protection Regulation, which came into force in the same year in the European Union, it will be examined aspects of the regulations that make up the data control architecture today and that effectively define the legal limits of profiling.

Keywords: Profiling. Personal data protection. Privacy. Discrimination.

AGRADECIMENTOS

Agradeço ao Prof. Dr. Fábio Queiroz, pelos dois anos de orientação paciente e dedicada, cujos ensinamentos muito contribuíram para meu crescimento, pessoal e acadêmico, e que foram essenciais na construção deste trabalho.

Aos demais professores e funcionários do programa de Pós-Graduação da UFMG, agradeço por todo o trabalho que propicia o desenvolvimento da educação superior gratuita e de alta qualidade.

Aos colegas de pós-graduação agradeço pelos diálogos e compartilhamento de ideias e experiências vivenciadas ao longo do processo de pesquisa. Aos amigos da graduação, Caio, Felipe, Gustavo, Juliana, Júlias, Matheus, Thiago, Toledo e Rodrigo, agradeço por me lembrarem dos bons frutos que nascem da Universidade:

Aos meus pais, Pedro e Juliana, por sempre proverem toda a estrutura que me permitiu a dedicação aos estudos.

Agradeço à Dani, por estar sempre ao meu lado e aguentar todos os momentos difíceis dessa jornada, tornando-a muito mais fácil.

SUMÁRIO

INTRODUÇÃO

Por volta do ano de 2012, a empresa de lojas de varejo "Target" elaborou uma campanha para direcionar anúncios de acessórios para bebês para mulheres no segundo trimestre de gravidez. Por meio da análise de dados dos produtos recém consumidos pelas clientes da loja, a empresa foi capaz de estimar aquelas que se encontravam naquele estágio de gestação para assim enviar a elas anúncios promocionais. Cerca de um ano após a criação do modelo que previa a gravidez de consumidoras, um homem adentrou uma das lojas irritado e demandando falar com o gerente. O homem brandia cupons de desconto para roupas de bebês e outros itens relacionados à maternidade, que foram endereçados a sua filha adolescente. Ele questionou se a rede queria encorajar adolescentes a engravidar. O gerente se desculpou e não soube explicar a situação. Alguns dias depois, ao ligar novamente para se desculpar, o gerente foi quem ouviu desculpas do pai, que afirmou ter conversado com sua filha e ela lhe revelou que estava realmente grávida. Ele disse: "Acontece que tem havido algumas atividades na minha casa que eu não conhecia completamente" [1].

Kevin D. Johnson, cidadão norte-americano negro, apesar de possui um histórico impecável de adimplemento de suas contas, foi um dia surpreendido por uma carta de seu banco lhe informando que seu crédito seria drasticamente reduzido. A razão dada para a redução de seus limites foi o histórico de inadimplência de outros consumidores que costumavam utilizar cartão de crédito nos mesmos estabelecimentos que ele frequentava[2].

Apesar das notórias diferenças entre as histórias, ambos os casos possuem como origem comum uma mesma técnica de tratamento de dados pessoais. Ainda que a primeira história não passe de uma anedota, pois, apesar de noticiada, nunca foi confirmada por representantes da empresa, não parece irreal que os atuais sistemas de processamento de dados detidos por grandes empresas possam ocasionar situações de constrangimento semelhante. A história real de Kevin Johnson, por sua vez, levantou a possibilidade problemática de consumidores serem penalizados por atividades associadas

---

[1] DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times Magazine**, Nova Iorque, 16 fev. 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Acesso em: 19 jun. 2019.

[2] HURLEY, Mikella; ADEBAYO,Julius. *Credit scoring* in the age of big data. **The Yale Journal of Law & Technology, v. 18, p.148-216,2016.** Disponível em <https://yjolt.org/credit-scoring-era-big-data>. Acesso em: 09 nov. 2018.

a uma raça, etnia ou classe socioeconômica em particular. Ambos os casos ilustram um importante desafio a ser enfrentado para garantia do pleno desenvolvimento da vida privada no século XXI. O mundo conectado permite aos indivíduos acesso facilitado à grandes quantidades de informação, ao mesmo tempo que qualquer atividade realizada por meios digitais deixa uma espécie de "rastro", que pode ser convertido e armazenado como mais informação por uma série de agentes. Assim, as empresas são capazes de coletar facilmente grandes quantidades de informação acerca dos indivíduos. Com base nos dados coletados, podem conhecer características íntimas de consumidores e influenciar cada vez mais aspectos de suas vidas.

É no contexto de uma economia baseada em dados que se desenvolve a espécie de tratamento de dados que será objeto do presente estudo. Esse procedimento, denominado "*profiling*" envolve a construção de perfis pessoais a partir da análise automatizada de grandes quantidades dados coletados acerca de um indivíduo ou de um grupo, com o objetivo de se tomar uma decisão em relação ao sujeito perfilado (por exemplo, enviar um anúncio direcionado ou aprovar ou negar crédito).

Assim como a maioria das tecnologias, observam-se ganhos importantes com essa prática, principalmente em termos de eficiência e eficácia de análises preditivas para o mercado. Porém, seu uso irrestrito pode significar importantes efeitos prejudiciais ao desenvolvimento da vida privada dos indivíduos, por possibilitar previsões de comportamento ou de características de um sujeito de maneira invasiva à sua privacidade e pela possibilidade de enquadramento do indivíduo em um perfil historicamente determinado, estereotipado e, potencialmente, discriminatório.

Nesse sentido, o presente trabalho visa identificar quais devem ser os limites legais do *profiling* feito por agentes do setor privado, de forma a se mitigar as mazelas que decorrem desse tipo de tratamento de dados. Partindo-se da teoria da existência de uma burocracia no fluxo e no tratamento dados por grandes organizações, proposta por Daniel Solove, que pode ser solucionada por meio arquitetura de controle que integre leis e tecnologias e altere significativamente as estruturas dos fluxos de informações, busca-se demonstrar que é necessário que as legislações relativas à proteção de dados pessoais criem formas controle sobre dados de diversos níveis, de maneira a se garantir efetiva privacidade e igualdade dos sujeitos cujos dados são utilizados para definição de perfis.

Para tanto, foi conduzida uma pesquisa teórica jurídica-dogmática de dois tipos: jurídico-compreensiva, a fim de se decompor o problema jurídico de dados pessoais frente

a práticas de *profiling* em seus diversos aspectos, relações e níveis; e jurídico-comparativa com objetivo de se compreender diversas abordagens acerca dos temas que envolvem o *profiling.*

O texto se divide em três capítulos. No primeiro capítulo, é feita uma contextualização do ambiente social, econômico e tecnológico em que o *profiling* surge como uma prática altamente lucrativa, servindo de base para grandes modelos de negócio ao custo de riscos relativos ao desenvolvimento da personalidade individual. No segundo capítulo, o conceito de *profiling* é explorado em diálogo interdisciplinar com especialistas da área da computação e de análise de dados. É visto como o conceito técnico se transpõe para o jurídico, bem como os principais problemas jurídicos que emergem da prática. No terceiro e último capítulo, discutem-se os limites que a privacidade, a igualdade e a proteção de dados pessoais impõem ao *profiling*, de maneira a se tornar necessária a construção de uma arquitetura de controle sobre o fluxo de dados capaz de conjugar diversos elementos para garantia desses direitos, e como tudo isso se traduz nos normativos que regulam a proteção de dados no Brasil e na Europa. Trata-se da *General Data Protection Regulation* (GDPR), regulamento do Parlamento Europeu aprovado no ano de 2016, que entrou em vigor em 2018, e da Lei Geral de Proteção de Dados (LGPD), aprovada no Brasil em 2018 e que entrará em vigor em 2020, legislação cuja tramitação foi fortemente influenciada pela mudança no paradigma europeu.

1. ASPECTOS SOCIAIS, ECONÔMICOS E TECNOLÓGICOS DA SOCIEDADE DA INFORMAÇÃO

Na primeira parte deste estudo, busca-se compreender algumas questões essenciais que emergem em nossa sociedade nos últimos anos, principalmente no que tange ao atual modelo de economia baseado na informação. Compreender o contexto social e econômico em que as práticas de *profiling* se desenvolveram e se tornaram usuais é fundamental para se chegar às conclusões de como o direito deve lidar com esse tema, que é o principal ponto da presente pesquisa.

O desenvolvimento e a difusão das tecnologias digitais nos últimos anos operam uma das maiores mudanças nas relações econômicas e sociais observadas na história recente. O mundo encontra-se hoje conectado de maneira que não era imaginável há poucas décadas. O termo "Sociedade da Informação" vem sendo utilizado amplamente para se referir a esse contexto, em que o acesso e o uso de informação se tornam um dos aspectos centrais da sociedade. Não é possível apontar uma origem clara[3] para a expressão, e existem variados termos que, talvez, reflitam melhor as mudanças sociais provocadas pelas novas tecnologias[4]. Porém, "Sociedade da Informação" se tornou de uso corrente, e pode se afirmar que a expressão se refere adequadamente a uma era em que a informação flui em rápida velocidade e assume valores sociais e econômicos fundamentais[5].

A formação e o desenvolvimento desse contexto pode ser atribuído a três fatores: a convergência da base tecnológica, a dinâmica da indústria e o crescimento da internet[6]. O primeiro fator se refere à possibilidade de se processar qualquer tipo de informação por meio de uma única forma, qual seja, a digital. Assim, palavras, imagens, comunicação por voz e quaisquer outros tipos de dados podem ser transmitidos e estão disponíveis em

---

[3] Aparentemente o termo foi largamente utilizado em debates acadêmicos nos Estados Unidos e no Japão, sem que um teórico específico o desenvolvesse de forma dogmática. DUFF, A. S.; CRAIG, D; MCNEILL, D. A. A note on the origins of the "information society.". **Journal of Information Science**, v.22, n.2, p.117–122, abr.1996.

[4] Por exemplo, o sociólogo Daniel Bell utiliza o termo "sociedade pós industrial", enquanto Castells fala em "Sociedade em Redes". BELL, Daniel. **The coming of post-industrial society**. New York: Basic Books, 1999. CASTELLS, Manuel. **A galáxia internet. Reflexões sobre internet, negócios e sociedade**. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004, p.3.

[5] TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000. p.3.

[6] TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000. p.4.

um mesmo aparelho, seja no clássico computador de mesa ou no telefone móvel. A dinâmica da indústria, por sua vez proporcionou contínua queda dos preços de aparelhos de informática em relação à sua potência computacional, permitindo sua difusão crescente na população. Por fim, e como resultado dos outros dois fatores, tem-se a rápida propagação do acesso à internet, que cresce vertiginosamente ao redor do mundo[7].

No Brasil, pesquisas realizadas pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), relativa aos domicílios no Brasil[8], apontam que a porcentagem de domicílios com acesso à internet subiu de 27% para 61% entre os anos de 2010 e 2017. Entre 2016 e 2017, em razão da facilitação ao acesso à internet móvel, o Brasil ganhou cerca de 10 milhões de novos usuários, chegando ao número de 126,3 milhões segundo dados do IBGE[9].

Pode-se afirmar que a "Sociedade da Informação" implica num fenômeno global que estabelece um novo paradigma técnico-econômico, com forte dimensão política, econômica e social[10]. O conceito de paradigma econômico e tecnológico envolve um insumo chave, de disponibilidade universal que gera uma série de inovações técnicas e organizacionais inter-relacionadas[11].

No atual contexto, a informação faz o papel de insumo chave, é a própria matéria prima tratada pelas novas tecnologias. Além disso, conforme aponta Castells[12], as novas tecnologias possuem forte penetrabilidade na população, uma vez que a informação é parte integral da atividade humana. Assim, os processos de nossa existência individual e coletiva acabam moldados pelos novos meios tecnológicos. Basta observar como, até poucos anos atrás, fotos eram compartilhadas em encontros pessoais por meio de álbuns impressos e hoje estão espalhadas por redes sociais acessadas diariamente pela maioria das pessoas, ou como grande parte da população aderiu rapidamente aos aplicativos de mensagem instantânea em celulares.

---

[7] TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000. p.4.
[8] CETIC.br, **Pesquisa TIC Domicílios**. Disponível em: http://cetic.br/pesquisa/domicilios/. Acesso em 01 de jul. 2018.
[9] EDITORIA: ESTATÍSTICAS SOCIAIS. PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país. **Agência IBGE Notícias**, Rio de Janeiro, 20 dez. 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais. Acesso em: 18 jun. 2019.
[10] TAKAHASHI, Tadao (Org.). Sociedade da informação no Brasil: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. p.3
[11] CASTELLS, Manuel. **A Sociedade em rede**. São Paulo: Paz e Terra, 2011, p.107.
[12] CASTELLS, Manuel. **A Sociedade em rede**. São Paulo: Paz e Terra, 2011, p. 108.

Hoje, a maioria dos cidadãos consegue acessar diversos canais de informação de forma instantânea e, sob demanda, se comunicar facilmente com outros indivíduos ao redor do mundo e um número cada vez maior de transações comerciais são feitas no meio digital. Ao mesmo tempo, praticamente toda a atividade dos usuários na Internet gera uma espécie de "rastro", que pode ser convertido e armazenado como mais informação por uma série de agentes. Assim, além dos indivíduos terem acesso facilitado a grandes quantidades de informação, empresas e governos são capazes de coletar facilmente dados pessoais em massa acerca dos indivíduos.

É a partir da coleta massificada de dados de usuários das novas tecnologias da informação, no contexto de uma Sociedade da Informação, que o *profiling*, tema da presente dissertação, se desenvolve e se difunde, tanto no setor público como no setor privado. Nos últimos anos, a maneira como compramos, utilizamos bancos e praticamos atividades cotidianas mudou significativamente, de maneira a resultar em aumento sem precedente de registros e bancos de dados. De acordo com Daniel Solove[13], somos hoje confrontados com o surgimento de verdadeiros dossiês digitais, que são uma coleção detalhada de dados acerca de um indivíduo. Atualmente, esses dossiês são construídos para cada um de nós e por múltiplos agentes. O problema se agrava uma vez que os dossiês se tornam muito extensos e são usados de maneira que afeta profundamente nossas vidas, sem que tenhamos poder para exercer alguma influência[14]. Nos próximos tópicos serão analisados alguns aspectos essenciais acerca da Sociedade da Informação que explicam como chegamos em um ponto de desenvolvimento da sociedade e das tecnologias em que é possível se estabelecer perfis de pessoas com baixos custos e de maneira rápida e, ao menos em tese, precisa.

1.1 A "quarta revolução industrial"

Klaus Schwab, fundador e presidente executivo do Fórum Econômico Mundial, identifica que vivenciamos uma "quarta revolução industrial", que denota uma mudança abrupta e radical, causada pelas novas tecnologias[15]. Segundo o autor[16], entre 1760 e 1840, ocorreu a primeira revolução industrial, baseada na produção mecânica

[13] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: NEW YORK UNIVERSITY PRESS, 2004, p.2.
[14] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: NEW YORK UNIVERSITY PRESS, 2004, p.3
[15] SCHWAB, Klaus**. A quarta revolução industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016, p.18.
[16] SCHWAB, Klaus**. A quarta revolução industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016, p.18.

possibilitada pela invenção de ferrovias e da máquina a vapor. Entre o final do século XIX e início do século XX, houve a segunda revolução industrial, ocasionada pela invenção da eletricidade e pela organização da indústria em linhas de montagem. A terceira revolução industrial ocorre entre 1960 e 1990, baseada nas tecnologias digitais, com as invenções consecutivas da computação em *mainframe* (computadores de grande porte); computação pessoal e da internet. É na esteira dessa terceira revolução industrial que a Sociedade Da Informação se desenvolve e o potencial da grande quantidade de informações disponíveis no meio digital fomenta uma quarta revolução.

Conforme caracterizado por Schwab, a quarta revolução industrial é baseada em uma revolução digital que combina diversas tecnologias, ocorrendo uma evolução em ritmo exponencial, com amplitude, profundidade e impacto sistêmico[17]. É uma forma de descrever o conjunto de transformações em nossos sistemas, que, segundo o autor, representa um novo capítulo no desenvolvimento humano.

Nesse contexto, a internet se tornou ubíqua, não sendo mais acessada somente através de computadores, mas também em aparelhos móveis e, mais recentemente, passa a ser integrada em uma grande variedade de objetos domésticos, automóveis, relógios, dentre outros. Como exemplo dessa ubiquidade, observa-se que o número de smartphones, no Brasil, ultrapassou o número de habitantes no ano de 2018, conforme aponta pesquisa realizada pela FGV[18].

Além disso, o desenvolvimento da inteligência artificial e aprendizagem da máquina possibilita o processamento de dados para fins diversos, cada vez mais avançados. Destaca-se o seguinte trecho da obra de Schwab que descreve alguns aspectos da quarta revolução industrial e como ela representa uma ruptura com o contexto que a antecede:

> Ao permitir "fábricas inteligentes", a quarta revolução industrial cria um mundo onde os sistemas físicos e virtuais de fabricação cooperam de forma global e flexível. Isso permite a total personalização de produtos e a criação de novos modelos operacionais.
>
> A quarta revolução industrial, no entanto, não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Ondas de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis à computação quântica. O que torna a quarta revolução industrial

[17] SCHWAB, Klaus**. A quarta revolução industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016, p.15-16.

[18] MEIRELLES, Fernando. **Pesquisa anual do uso de TI.** Disponível em: https://eaesp.fgv.br/ensinoeconhecimento/centros/cia/pesquisa . Acesso em: 18 de jun. 2019

> fundamentalmente diferente das anteriores é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos
>
> Nessa revolução, as tecnologias emergentes e as inovações generalizadas são difundidas muito mais rápida e amplamente do que nas anteriores, as quais continuam a desdobrar-se em algumas partes do mundo. A segunda revolução industrial precisa ainda ser plenamente vivida por 17% da população mundial, pois quase 1,3 bilhão de pessoas ainda não têm acesso à eletricidade. Isso também é válido para a terceira revolução industrial, já que mais da metade da população mundial, 4 bilhões de pessoas, vive em países em desenvolvimento sem acesso à internet. O tear mecanizado (a marca da primeira revolução industrial) levou quase 120 anos para se espalhar fora da Europa. Em contraste, a internet espalhou-se pelo globo em menos de uma década[19].

Na esteira dessa revolução estão 12 conjuntos de tecnologias que possuem potencial disruptivo[20]. Dentre elas, destacam-se para a presente pesquisa as chamadas tecnologias digitais extensíveis e a inteligência artificial, que se utilizam de quantidades massivas de dados como combustível.

A partir delas, surge uma das mudanças apontadas por Schwab que caracterizam a quarta revolução industrial. Trata-se do uso do *Big Data* na tomada de decisões de empresas e do governo. Essa mudança traz como principal preocupação para os indivíduos o estabelecimento de perfis individuais a partir da coleta massiva de seus dados pessoais. Schwab caracteriza essa prática como de impacto desconhecido ou impacto positivo e negativo[21]. Para melhor compreensão dessa mudança, é preciso que se entenda o que é o *Big Data* e como ele vem alterando o mundo nos últimos anos.

1.2 O advento do *Big Data* e suas implicações

O termo *Big Data* não possui uma definição única e constante. É possível se observarem três definições que aparecem recorrentemente em documentos oficiais de governos e entre especialistas que buscam regular o tema[22]: *Big Data* pode ser referir ao crescimento exponencial na disponibilidade e no uso automatizado da informação; às grandes quantidades de dados diferentes produzidos rapidamente por fontes múltiplas, cujo manejo e análise requerem novos algoritmos e processadores mais poderosos; ou ao

---

[19] SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016, p.19-20.

[20] São elas: as novas tecnologias da computação, *blockchain* e tecnologias de registro distribuído, internet das coisas, inteligência artificial e robótica, materiais modernos, fabricação de aditivos e impressão multidimensional, biotecnologias, neurotecnologias, realidades virtual e aumentada, captura, armazenamento e transmissão de energia, geoengenharia e tecnologias espaciais. SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a quarta revolução industrial**. São Paulo: Edipro, 2018.

[21] SCHWAB, Klaus. **A quarta revolução industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016. p.113-114.

[22] SLOOT, Bart van der; SCHENDEL; Sacha van. Ten questions for future regulation of big data: a comparative and empirical legal study. **Journal of Intellectual Property, Information Technology and Eletronic Commerce Law,**v7,n.2, o.110-145, 2016.

modelo dos três "Vs", que descreve o *Big Data* como um fenômeno de aumento no volume, na velocidade de processamento e na variedade dos dados.

Viktor Mayer-Schonberger e Kenneth Cukier solidificam diversos conceitos, aplicações e impactos do *Big Data* na sociedade. Os autores afirmam que a ideia de *Big Data* é definida como a capacidade da sociedade de aproveitar as informações de maneiras inovadoras para produzir *insights* úteis ou bens e serviços de valor significativo[23]. Observa-se, portanto, que o termo "*Big Data*" faz referência não somente aos grandes bancos de dados construídos pelos atores do mercado e governamentais, mas a toda a tecnologia de captura de dados, o crescimento, a disponibilidade e o uso de informações estruturadas e não estruturadas que se difundem em meio eletrônico[24], de forma que a partir desse sistema, é possível o cruzamento de dados em alta velocidade para diversos fins.

Os desenvolvimentos tecnológicos, tais quais processadores mais rápidos e *hardrives* com maior capacidade de armazenamento não são a única razão que possibilita a formação do *Big Data*[25]. O crescimento na quantidade de dados acontece porque a sociedade passa a registrar e catalogar muitos diferentes aspectos da realidade na forma de dados, a fim de melhor compreendê-los. Nesse sentido, Granz e Reinsel apontam que o volume de informações no planeta tem dobrado a cada dois anos, de forma que o volume de dados digitais existentes, em 2020, será de 40.000 hexabytes (40 trilhões de gigabytes), o que representará 5.200 gigabytes para cada homem, mulher ou criança em 2020[26].

> Não somente o mundo está inundado com mais informação do que nunca antes, mas essa informação está crescendo mais rapidamente. A mudança em escala resulta numa mudança de estado. A mudança quantitativa resultou em uma qualitativa. Ciências como a astronomia e genômica, que primeiro experenciaram a explosão nos anos 2000, cunharam o termo "*Big Data*". O conceito está agora migrando para todas as áreas de empreendimento humano. *Big Data* refere a coisas que podem ser feitas em larga escala que não podem ser feitas numa escala menor, de se extrair novos *insights* ou criar novas formas de valor, em maneiras que alteram mercados, organizações, a relação entre cidadãos e governos e mais[27].

---

[23] MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*. p.7.

[24] SIMÃO FILHO, A.; SCHWARTZ, G. A. D. Big Data em tempos de internet das coisas. In: PARENTONI, L.; GONTIJO, B.M.; LIMA, H.C.S. **Direito, Tecnologia e Inovação** . Belo Horizonte: D'Placido, cap. 2.2, p. 217-246. v. I. 2018.

[25] MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*,.

[26] GANTZ, John; REINSEL, David. The digital universe in 2020: big data, bigger digital shadows, and biggest growth in the far east. IDC iView - Analyze the Future, 2012. Disponível em: https://www.emc.com/leadership/digital-universe/2012iview/index.htm. Acesso em: 5 jul. 2019.

[27] No original: "Not only is the world awash with more information than ever before, but that information is growing faster. The change of scale has led to a change of state. The quantitative change has led to a

O processo de transformar um aspecto da realidade em um formato numericamente quantificável é o que Mayer-Schonberger e Cukier chamam de "datification". "Datificar" um fenômeno é colocá-lo em um formato quantificado para que ele possa ser tabulado e analisado[28]. Processos de datificação foram desenvolvidos durante toda a história humana, mas sempre foram muito custosos e ineficientes. O desenvolvimento da informática, que possibilita a medição e o armazenamento digitais, tornou o processo de datificação muito menos dispendioso.

A quarta revolução industrial permite que a datificação ocorra em campos que antes não podiam ser explorados. Assim, novas tecnologias permitiram que, recentemente, muitos aspectos da vida cotidiana passassem a sofrer datificação para fins comerciais e de políticas públicas, por exemplo.

> As novas fronteiras da datificação são mais pessoais: nossos relacionamentos, experiências e humores. A ideia de datificação é a espinha dorsal de muitas das companhias de mídia social da Web. Plataformas de redes sociais não oferecem simplesmente uma maneira de encontrar e manter contato com amigos e colegas, elas são capazes de coletar elementos intangíveis da nossa vida e transformá-los em dados que podem ser utilizados para fazer coisas novas.[29]

A integração de dispositivos de geolocalização em *smartphones* permite constante rastreamento dos deslocamentos do usuário, fonte constante de dados que servem para avaliação de seu comportamento. Do mesmo modo as interações em redes sociais são constantemente quantificadas e analisadas para fins de exibição de anúncios direcionados. Sites de comércio eletrônico podem avaliar diversos aspectos da navegação dos usuários (cliques, tempo de visualização, rolagem do mouse) por suas páginas para melhor definir os hábitos de consumo de seu público. Ainda mais recentemente, novas tecnologias

---

qualitative one. The sciences like astronomy and genomics, which first experienced the explosion in the 2000s, coined the term "big data." The concept is now migrating to all areas of human endeavor. Big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value, in ways that change markets, organizations, the relationship between citizens and governments, and more". MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*,p.9.

[28] MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p. 46.

[29] No original: "The next frontiers of datafication are more personal: our relationships, experiences, and moods. The idea of datafication is the backbone of many of the Web's social media companies. Social networking platforms don't simply offer us a way to find and stay in touch with friends and colleagues, they take intangible elements of our everyday life and transform them into data that can be used to do new things." MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p.53.

permitem a datificação através de reconhecimento facial ou mesmo da postura corporal de pessoas em diversos ambientes[30].

A principal mudança de paradigma ocasionada pelo advento do *Big Data* é que dados não são mais vistos como algo estático, cuja utilidade se encerra uma vez que o propósito da coleta seja atingido. Atualmente, dados se tornaram a matéria prima de modelos de negócios, como ativo econômico vital utilizado para se criar formas de se extrair valor, e que podem ser reutilizados constantemente como fonte de inovação e criação de novos serviços.

A ascensão do *Big Data* representa três mudanças na maneira de analisar as informações. A primeira mudança é que o uso de pesquisas por amostragens é diminuído, uma vez que é possível se utilizar de grandes escalas de números de dados. Acerca de algumas matérias, é possível analisar virtualmente todo o universo de dados que as compõem. Usando todos os dados é possível enxergar detalhes que antes eram impossíveis de serem vistos. A segunda mudança é uma flexibilização no desejo por exatidão. Com menos informação disponível, aquilo que era quantificado deveria ser exato, para não haver grandes distorções no resultado final. Porém, quando é possível a coleta e análise de um número imenso de dados, o fato de pequenas partes do todo conterem erros gera uma perda menor do que o ganho de se analisar maiores quantidades. Por exemplo, ao se contabilizar o caixa de um pequeno negócio, pequenos erros irão se refletir no balanço final, enquanto ao se contabilizar o tesouro de um Estado, pequenas inexatidões são aceitáveis para que se consiga apreender o todo. O mesmo ocorre na análise de quantidades massivas de dados. O que se perde em exatidão no nível micro é compensado por revelações no nível macro[31].

---

[30] No Brasil, a rede de lojas de roupa Hering inaugurou uma unidade em São Paulo em que câmeras de reconhecimento facial identificam as reações dos clientes às peças em exposição e disponibilizam opções personalizadas com base na análise feita. Também em São Paulo, o reconhecimento facial foi utilizado em painéis de publicidade que identificavam emoções, gênero e faixa etária de quem parasse para observar o anúncio. Nesse último caso, o Tribunal de Justiça de São Paulo determinou a suspensão do uso da tecnologia. Ver: CASEMIRO, Luciana. Hering terá que explicar o que faz com dados de reconhecimento facial de clientes. **O Globo**, Rio de Janeiro, 26 fev. 2019. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23482114. Acesso em: 19 jun. 2019; FARIAS, Adriana. Justiça proíbe uso de câmeras de reconhecimento facial no Metrô. **Veja São Paulo**, São Paulo, 15 set. 2018. Disponível em: https://vejasp.abril.com.br/cidades/justica-proibe-uso-de-cameras-de-reconhecimento-facial-no-metro/. Acesso em: 19 jun. 2019.

[31] MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p.16-31.

Durante a maior parte de sua história, a humanidade teve que lidar com as limitações físicas do processamento de informações. A dificuldade de se coletar dados em massa e de organizá-los de maneira a gerar informação útil fez com que fossem desenvolvidas técnicas avançadas de se fazer estimativas com a maior precisão possível, usando o mínimo de informação necessária, técnicas consolidadas na ciência da Estatística. Esse tipo de análise demonstra que, selecionar aleatoriamente um pequeno número de amostras de um todo numeroso é um meio eficaz de se estimar com precisão algo sobre esse todo, desde que eliminado o maior número possível de erros e desvios das amostras consideradas. Porém, apesar do sucesso das análises por amostragens, elas são somente um "atalho", ou seja, a segunda melhor alternativa, que ainda perde em termos de precisão para a possibilidade de se analisar todos os dados individualmente. Hoje, a alternativa ótima, de se analisar praticamente todos os componentes de determinado grupo, por maior que seja, se tornou possível.

As duas mudanças citadas geram uma terceira, que é uma menor busca pelo conhecimento de causas. Pesquisas através do *Big Data* são muito precisas em estabelecer correlações úteis. A análise de dados em massa permite o reconhecimento de correlações que antes não poderiam ser vistas. Assim é possível prever que algo vai acontecer, ainda que não se possa explicar exatamente por qual motivo. Correlações vão aos poucos ocupar o espaço das relações causais, que são aquelas as quais nosso pensamento racional usualmente busca estabelecer. Resumidamente, segundo Mayey-Schonberger e Cukier:

> O *Big Data* é sobre três grandes mudanças de mentalidade que são interligadas e assim reforçam uma a outra. A primeira é a habilidade de se analisar vastas quantidades de dados sobre um tópico ao invés de ser forçado a se contentar com conjuntos menores. A segunda é estar à vontade para abraçar a desorganização dos dados no mundo real ao invés de se privilegiar a exatidão. A terceira é o crescente respeito por correlações ao invés da contínua busca por uma causalidade elusiva[32].

Essa terceira mudança, porém, traz uma das principais preocupações acerca do uso cego da análise de dados em massa. Por meio do *Big Data*, padrões são descobertos que permitem, com alto grau de precisão, prever que certo evento ocorrerá. Porém, as correlações, por si só, não dizem o porquê da ocorrência de certo fenômeno.

> A causalidade não será descartada, mas está sendo retirada de seu pedestal de fonte primária de sentido. *Big Data* turbina análises não-causais,

[32] No original: "big data is about three major shifts of mindset that are interlinked and hence reinforce one another. The first is the ability to analyze vast amounts of data about a topic rather than be forced to settle for smaller sets. The second is a willingness to embrace data's real-world messiness rather than privilege exactitude. The third is a growing respect for correlations rather than a continuing quest for elusive causality". MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p.16.

> frequentemente substituindo investigações causais (...). Em um mundo do *Big Data*, por contraste, não precisaremos mais estar fixados em causalidade; ao invés nós poderemos descobrir padrões e correlações nos dados que nos oferecem *insights* novos e inestimáveis. As correlações podem não nos dizer precisamente por que algo está acontecendo, mas nos alertam que estão acontecendo. *Big Data* é sobre o quê, não sobre o porquê. Não sempre precisamos saber a causa de um fenômeno; em vez disso, podemos deixar que os dados falem por si só.[33]

Estabelecer correlações sem conhecimento de causas é especialmente problemático quando se adentra no território de análises de comportamentos humanos. Formular previsões acerca de como certa pessoa irá agir e tomar decisões que afetem essa pessoa com base nas previsões feitas, sem que se saiba o porquê de se ter obtido aquele resultado, acaba por ocasionar sérios riscos envolvendo a esfera privada dos indivíduos. Inicialmente, a análise de grandes quantidades comportamentais de certa pessoa pode revelar aspectos de sua vida que, em nenhum momento, essa pessoa teve intenção de revelar[34]. Além disso, as correlações estabelecidas podem refletir padrões históricos de discriminação de certo grupo ou classe social, em razão de certo viés presente na base de dados utilizada[35]. Esses riscos são de duas ordens: uma relativa à privacidade e outra relativa à discriminação, temática que será abordada com maior profundidades nos próximos capítulos.

---

[33] No original: "Causality won't be discarded, but it is being knocked off its pedestal as the primary fountain of meaning. Big data turbocharges non-causal analyses, often replacing causal investigations(...). In a big-data world, by contrast, we won't have to be fixated on causality; instead we can discover patterns and correlations in the data that offer us novel and invaluable insights. The correlations may not tell us precisely why something is happening, but they alert us that it is happening. Big data is about what, not why. We don't always need to know the cause of a phenomenon; rather, we can let data speak for itself." SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p.41.

[34] A empresa de lojas de varejo "Target" promoveu análise de dados a fim de identificar mulheres no segundo trimestre de gravidez, período em que, segundo as estatísticas, estão mais propensas a buscar os produtos comercializados pela rede. Cerca de um ano após a criação de um modelo que previa a gravidez de consumidores, um homem adentrou uma das lojas irritado e demandando falar com o gerente. O homem brandia cupons de desconto para roupas de bebês e outros itens relacionados à maternidade, que foram endereçados a sua filha adolescente. O homem questionou se a rede queria encorajar adolescentes a engravidar. O gerente se desculpou e não soube explicar a situação. Alguns dias depois, ao ligar novamente para pedir desculpas, o gerente foi quem ouviu desculpas do pai, que revelou ter conversado com sua filha e ela estava realmente grávida. Ele disse "Acontece que tem havido algumas atividades na minha casa que eu não conhecia completamente". DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times Magazine**, Nova Iorque, 16 fev. 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Acesso em: 19 jun. 2019.

[35] Kevin D Johnson, cidadão norte-americano negro, sofreu uma drástica restrição ao seu crédito, apesar de seu histórico de adimplemento pontual de todas as contas. A razão dada para a redução de seus limites foi o histórico de outros consumidores que costumavam utilizar cartão de crédito nos mesmos estabelecimentos que ele. A história de Kevin Johnson levantou a possibilidade problemática de consumidores serem penalizados por atividades associadas a uma raça, etnia ou classe socioeconômica em particular. Ver: HURLEY, Mikella; ADEBAYO,Julius. *Credit scoring* in the age of big data. **The Yale Journal of Law & Technology, v. 18, p.148-216,2016.** Disponível em: <https://yjolt.org/credit-scoring-era-big-data>. Acesso em: 09 nov. 2018.

A utilização *Big Data* para extração de valor por meio algoritmos que processam dados pessoais é uma prática que se tornou comum em diferentes esferas. Assim, a palavra "algoritmo", que antes era utilizada como termo técnico quase exclusivamente por profissionais especializados da ciência da computação vem sendo aplicada em diferentes contextos e tem sido alvo de diversos debates sociais relevantes. Em mais uma variação para a expressão "Sociedade da Informação", Balkin[36] afirma que hoje vivemos num momento de transição para a Sociedade dos Algoritmos, organizada em torno da tomada de decisões sociais e econômicas por algoritmos, robôs e agentes de inteligência artificial. Esses agentes não só tomam as decisões, mas também, em alguns casos, as executam. Nessa sociedade, o *Big Data* age como um combustível, que serve para que os algoritmos cumpram seu papel e se aprimorem cada vez mais. Assim, Balkin afirma que: "algoritmos sem dados são vazios e dados sem algoritmos são cegos" [37].

A ampliação da discussão que ocorre ao redor do uso de algoritmos não tem necessariamente relação com alguma inovação técnica de como o algoritmo é construído. Por exemplo, sistemas de redes neurais, que hoje atraem muita atenção, eram pensados desde à década de 60[38] . O que há de novo nesse domínio é justamente a formação do *Big Data*, com técnicas mais difundidas de recolhimento de dados, que alimentam e permitem que seja extraído maior valor desses sistemas. Assim se formam arquivos mais vastos de dados pessoais que incluem as atividades de consumo, cliques de link, movimentação geográfica rastreada pelo uso universal de dispositivos móveis. Em certas partes do mundo há basicamente uma conectividade constante dos indivíduos[39].

Grande parte dos dados hoje produzidos incluem informações pessoais. A possibilidade de se medir e quantificar diversas ações humanas propiciada inicialmente pelo uso da internet em computadores e, mais recentemente, pela integração da internet em diversos dispositivos que interagem com o mundo físico forma um fluxo contínuo do que vem sendo chamado de "escape de dados"[40]. Escape de dados se refere aos dados que são gerados como subproduto das ações e movimentos das pessoas no mundo. No

---

[36] BALKIN, Jack M. The Three Laws of Robotics in the Age of Big Data. **Ohio State Law Journal**, Columbus, v. 78, n. 592, 26 dez. 2016.
[37] BALKIN, Jack M. The Three Laws of Robotics in the Age of Big Data. **Ohio State Law Journal**, Columbus, v. 78, n. 592, 26 dez. 2016.
[38] KAPLAN, Jerry. **Artificial Intelligence: What everyone needs to know**. Oxford: Oxford University Press, 2016.
[39] BURREL, Jenna: H. How the machine 'thinks': Understanding opacity in machine learning algorithms**, Big Data & Society**, [S.l] jan-jun. p. 1–12. 2016.
[40] Tradução nossa do termo "data exhaust". HARFORD, Tim. Big data: A big mistake?. **Significance**, Londres, v. 11, n. 5, p. 14-19, 1 dez. 2014.

contexto da Internet, as interações de usuários com as páginas geram escape de dados: onde clicam, por onde o cursor do mouse se movimenta, o que é digitado etc. Hoje as empresas desenvolvem seus produtos imaginando como poderão coletar da melhor forma o escape de dados, de forma que possa ser utilizado para realimentar e melhorar seu sistema ou para desenvolver um novo produto. Toda a ação do usuário é considerada como um sinal em potencial que poderá alimentar uma análise de dados a ser reutilizada.

Portanto, apesar de todo o potencial de inovação e evolução do *Big Data*, deve-se refletir sobre os principais problemas desse novo paradigma tecnológico. Nesse sentido, Mayer-Schonberger e Cukier afirmam que as pessoas não estão preparadas para lidar com o impacto do *Big Data* em seu senso de privacidade e em seu senso de liberdade[41]. Os principais problemas levantados são relacionados à privacidade, à liberdade e ao uso cego dos números apresentados.

Sloot e Schendel fazem uma avaliação dos riscos envolvidos na rápida evolução do *Big Data*. Inicialmente, eles definem os principais âmbitos de sua aplicação, afirmando que o *Big Data* vem sendo usado primariamente em três contextos: para auxílio de tarefas típicas do governo, como tributação e definição de políticas econômicas; no setor privado para executar trabalhos específicos e auxiliar no alcance dos objetivos de empresas, com estabelecimento, por exemplo, de perfis de risco, correlações estatísticas e personalização de publicidade; pelo governo e pelo setor privado para melhorar seus serviços em benefício dos cidadãos e dos consumidores. Segundo os autores, cada um desses contextos possui características específicas de modo que requerem sua própria abordagem diferenciada para regulação[42]. Para o presente trabalho, interessa o segundo contexto, que envolve o uso do *Big Data* por atores do setor privado na busca de melhor desempenho e ganho econômico.

Quanto a esse contexto, apresentam-se duas questões importantes que devem ter tratamento adequado pelo direito. A primeira se refere ao potencial uso de dados e formação de perfis baseados em informações sensíveis como raça, condições médicas e opiniões políticas, sendo que mesmo informações aparentemente neutras podem, de fato, refletir questões sensíveis. Além disso, independentemente de haver uso de informações

---

[41] MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book*, p.83.

[42] SLOOT, Bart van der; SCHENDEL; Sacha van. Ten questions for future regulation of big data: a comparative and empirical legal study. **Journal of Intellectual Property, Information Technology and Eletronic Commerce Law,** v.7, n.2, o.110-145, 2016.

sensíveis as consequências de análises baseadas em *Big Data* no setor privado podem ser substanciais. É o caso de seu uso para desenvolvimento de perfis de riscos que bancos utilizam para definir a elegibilidade de certa pessoa para um empréstimo, ou para cobertura em planos de saúde. Nestas situações, é possível que dados que não se relacionam com a capacidade de adimplemento de certo consumidor, ou com seu estado de saúde, sejam utilizados para definir um perfil e para tomada de decisões capazes de impactar significativamente a vida destes indivíduos.

Sloot e Schendel sugerem que os fatores que devem ser levados em conta na regulação do *Big Data* no setor privado são os impactos de seu uso para os indivíduos, os tipos de dados e análise de dados utilizados e o potencial perigo de incompatibilidade entre perfis genéricos e indivíduos específicos. Os autores demonstram em sua pesquisa que o próprio termo *profiling* é comumente associado com o *Big Data* e algumas vezes até incluído em seu próprio conceito. Nesse sentido, *profiling* se refere a correlações estatísticas, normalmente de natureza preditiva, acerca de características de indivíduos ou grupos. O tipo de organização e os propósitos específicos para que se utilizam do *Big Data* também devem ser abordados com ideia de que um interesse geral seja atendido para que a prática seja considerada legalmente admissível.

Acessar adequadamente os impactos do *Big Data* na sociedade e como o Direito deve lidar com eles, tendo em vista o seu uso por atores do setor privado para estabelecimento de perfis de indivíduos ou grupos é o principal escopo do presente trabalho. Nesse sentido, observa-se que o potencial econômico do *Big Data* é enorme, de forma que muitas vezes seu uso pelas grandes empresas do setor de tecnologia ignora o reflexo de suas práticas na construção da esfera privada de cada pessoa. A busca incessante por maior quantidade de dados, seu armazenamento para usos secundários a fim de em um momento posterior se extrair valor das informações colhidas, e outras práticas da mesma natureza criam uma lógica de mercado que acaba por colocar a maioria das pessoas que se utilizam de tecnologias em conexão num constante estado de vigilância. Por muito tempo a palavra "vigilância" esteve associada ao seu uso por governos autoritários, com intuito de observar e controlar cidadãos que ousassem se posicionar contrariamente ao regime imposto. Na medida que as tecnologias da informação se difundem e passam a se revelar úteis para se extrair informações capazes de gerar ganhos econômicos, a vigilância passa a ser também um problema das relações privadas. A fim de melhor compreender a abordagem legal que deve ser dada para se

amenizar os potenciais efeitos nocivos do *profiling* se faz necessário que se entenda melhor como a vigilância do setor privado se tornou, hoje, uma constante fonte de preocupação por juristas ao redor do mundo.

1.3 Vigilância e Burocracia

Como visto, a possibilidade de se extrair valor da informação, propiciada pelo desenvolvimento de tecnologias na chamada quarta revolução industrial, permite a datificação de variados aspectos da realidade e do comportamento humano. Com a formação de grandes bases de dados que são processados de maneira mais rápida e eficiente no contexto do *Big Data*, surge uma lógica de vigilância no setor privado, uma vez que as empresas buscam cada vez mais dados pessoais a fim de se extrairem ganhos econômicos a partir da melhor compreensão de aspectos do comportamento humano.

Mais uma vez surgem variadas expressões para tentar descrever o atual estado de constante monitoramento e medição de comportamento humano praticado por empresas e pelo governo. Stefano Rodotà caracteriza o atual contexto social de Sociedade da Vigilância, em que há uma gradual erosão da zona de privacidade, uma vez que ceder informações passa a ser um preço compulsório para se usufruir das crescentes oportunidades apresentadas na sociedade da informação[43]. Na compra de produtos ou serviços a pessoa não envolve mais somente seu patrimônio material, mas se vê obrigada a expor seu próprio eu:

> A pessoa é obrigada expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito[44].

Shoshana Zuboff[45], por sua vez, faz um estudo aprofundado acerca de como a vigilância se torna uma prática econômica que domina o atual mercado, desenvolvendo o que a autora intitula um Capitalismo da Vigilância. A autora descreve detalhadamente como esse modelo se formou e como funciona atualmente. Ela descreve o Capitalismo da

---

[43] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.113.

[44] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.113

[45] ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power.** Nova Iorque: Public Affairs, 2019. E-book.

Vigilância como uma nova ordem econômica que se vale da experiência humana como matéria prima para práticas comerciais ocultas de extração, previsão e vendas[46].

A autora aponta que, no início dos desenvolvimentos de tecnologias da informação, eram imaginadas diversas formas pelas quais a análise de dados seria colocada a serviço dos interesses pessoais de seus usuários. Porém, atualmente observa-se que aprimorar a experiência do usuário de um produto se tornou um objetivo secundário. A maior parte do processo de coleta e análise de dados vem sendo utilizada para alimentar programas de aprendizagem de máquinas, a fim de se elaborar produtos "preditivos", que antecipam o que a pessoa quer ou pretende fazer atualmente, em breve ou no futuro[47]. O problema maior surge quando o processo de automação não apenas sabe do comportamento de um indivíduo, mas também tenta e consegue moldá-lo.

Zuboff demonstra que o desenvolvimento de uma lógica de vigilância por parte das grandes empresas de tecnologia foi possível graças ao espaço desregulado da Internet em que companhias como Google e Facebook surgiram. Uma vez que o modelo dessas empresas apresenta fortes resultados econômicos, suas atividades passam a servir de exemplo e se tornam aceitáveis mesmo em outros ambientes.

> Como pioneiro do capitalismo da vigilância, Google lançou uma operação de mercado sem precedentes no espaço não mapeado da internet, onde encontrou poucos impedimentos de natureza legal ou competitiva, como uma espécie invasiva em um ambiente livre de predadores naturais. Seus líderes dirigiram a coerência sistemática de seu negócio em um ritmo vertiginoso que nem instituições públicas nem indivíduos poderiam seguir (...)
> O capitalismo da vigilância não está mais confinado ao drama competitivo de grandes companhias da internet, onde mercados de comportamento futuro miravam inicialmente anúncios online. Seus mecanismos e imperativos econômicos se tornaram o modelo padrão para a maioria dos negócios baseados na internet. Eventualmente, a pressão competitiva dirigiu uma expansão ao mundo offline, onde os mesmos mecanismos fundacionais que expropriam sua navegação online, curtidas e cliques são treinados na sua corrida no parque, conversa de café da manhã, ou busca por uma vaga para estacionar. Os produtos preditivos de hoje são comercializados em mercados de comportamento futuro que se estendem além de anúncios direcionados online para muitos outros setores, incluindo seguros, varejo, finanças e uma gama cada vez maior de empresas de bens e serviços determinadas a participar desses mercados novos e lucrativos.[48]

---

[46] ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.8.

[47] ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.8.

[48] No original: "As the pioneer of surveillance capitalism, Google launched an unprecedented market operation into the unmapped spaces of the internet, where it faced few impediments from law or competitors, like an invasive species in a landscape free of natural predators. Its leaders drove the systemic coherence of their businesses at a breakneck pace that neither public institutions nor individuals could follow(...) Surveillance capitalism is no longer confined to the competitive dramas of the large internet companies, where behavioral futures markets were first aimed at online advertising. Its mechanisms and

A política dos dirigentes do Google era incialmente contrária ao uso de anúncios vinculados a pesquisa devido ao viés que isso traria para os resultados de busca. Os dados de busca gerados pelo uso da principal plataforma da empresa eram utilizados unicamente para realimentação do sistema e aprimoramento desse, de forma a otimizar a experiência dos usuários.

Porém, o estouro da "bolha da Internet" no início dos anos 2000 fez com que a companhia buscasse formas de garantir lucros para seus investidores que estavam desacreditados. Assim os desenvolvedores de sistemas do Google descobrem o potencial de se extrair um "excedente comportamental"[49] a partir da atividade de seus usuários, e a empresa passa a gradualmente se valer de uma diversidade de dados gerados por seus mecanismos de busca, e-mail e outros produtos, para extrair informações relevantes que seriam vendidas aos anunciantes da plataforma. Tecnologias de rastreamento de informação e atividade de usuários na Internet foram criadas muitos anos antes de serem integradas ao sistema de vigilância do Google[50]. Os estudiosos da área de tecnologia da informação demonstravam grandes preocupações quanto a essas tecnologias nos anos 90 e início dos anos 2000, mas até então elas nunca haviam sido utilizadas em larga escala. Enfim, pressionado pela demanda por resultados feita por seus investidores, o Google combinou toda essa tecnologia para extrair excedente comportamental de seus usuários, vender para anunciantes e assim e gerar lucros extraordinários. O desenvolvimento da publicidade direcionada online, fomentada em grande parte pela atividade do Google, pavimenta o caminho para a incubar o "Capitalismo da Vigilância".

---

economic imperatives have become the default model for most internet-based businesses. Eventually, competitive pressure drove expansion into the offline world, where the same foundational mechanisms that expropriate your online browsing, likes, and clicks are trained on your run in the park, breakfast conversation, or hunt for a parking space. Today's prediction products are traded in behavioral futures markets that extend beyond targeted online ads to many other sectors, including insurance, retail, finance, and an ever-widening range of goods and services companies determined to participate in these new and profitable markets". ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.9-10.

[49] Tradução nossa do termo "Behavioral surplus" utilizado por Zuboff. O termo se refere ao uso da atividade e dos dados pessoais gerados pelos utilizadores de um serviço para se extrair lucro com sua venda a anunciantes ou elaboração de outros produtos preditivos, ao invés de se restringir à melhora do serviço em que foram produzidos. ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.75-75.

[50] Cookies, que são pequenas linhas rastreáveis de código, baixadas pelo usuário durante a navegação na internet, já eram tratados com preocupação em relatório enviado ao Congresso americano pela Federal Trade Commission em 2000. FTC. Online profiling: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commissionreport-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 19 jun. 2019.

A atividade realizada pelas empresas que formam o "Capitalismo da Vigilância", segundo Zuboff, funciona da seguinte maneira: as empresas coletam muito mais dados comportamentais do que o necessário para promover a melhora de seus serviços para os usuários. Esse excesso de dados comportamentais é processado por algoritmos capazes de gerar previsões de comportamento dos usuários. As previsões são comercializadas como um produto para outros empresários interessados, em um mercado de comportamentos futuros, enquanto o ciclo de melhora de serviços em prol dos indivíduos que proveem os dados é relegado a um papel secundário[51].

O grande escopo da vigilância exercida nesse tipo de atividade só veio à tona e começou a ser bem entendido após os serviços oferecidos por seus grandes atores estarem profundamente integrados na vida diária das pessoas, de forma que elas achem tais práticas aceitáveis tendo em vista o serviço que utilizam. Desse modo, elas se veem forçadas a escolher entre abrir mão do controle sobre os seus dados pessoais, e consequentemente, sobre seus comportamentos e desejos atuais e futuros, em troca de serviços que consideram essenciais para a vida conectada.

Porém, é preciso que se entenda que as práticas do capitalismo de vigilância não são uma expressão inevitável das tecnologias empregadas. Segundo Zuboff, o "Capitalismo da Vigilância" foi uma invenção humana, que surge frente a pressões competitivas do mercado, mas não é um resultado inevitável do desenvolvimento das tecnologias digitais, ou do capitalismo da informação[52]. O rápido desenvolvimento do "Capitalismo de Vigilância" muito se deve ao território desgovernado da Internet em que ele encontrou espaço. As grandes companhias encontraram o território sem lei e trabalharam ativamente para manter essa desregulamentação, se utilizando do discurso de que leis somente dificultam a inovação e que nos dias de hoje é impossível que os legisladores acompanhem o desenvolvimento tecnológico. Apenas mais recentemente, quando a falta de regulamentação se reflete em insegurança para este mercado e a opinião pública se volta contra o setor a cada novo escândalo relativo ao descaso com dados pessoais, é que as empresas começam a advogar por regras mais claras para sua atuação

Porém, é possível que por meio de regulação adequada e da construção de uma arquitetura de proteção de dados, seja revertida a atual lógica que coloca a esfera privada

[51] ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.97.
[52] ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power**. Nova Iorque: Public Affairs, 2019. *E-book*, p.85.

dos indivíduos em situação de extrema fragilidade, conforme pretende-se defender no decorrer deste trabalho. Assim, as pessoas não estariam à mercê da lógica de que devem escolher entre ter privacidade e usufruir dos serviços providos pelas grandes empresas de tecnologia da informação.

A teoria construída por Zuboff é de grande utilidade para se compreender como atuam as empresas de comunicação e tecnologia. A partir dela é possível visualizar como a constante coleta de dados pessoais é utilizada para extração de valor econômico, através de, por exemplo, construção de perfis individuais e coletivos que permitem a predição do comportamento humano. Porém, o discurso da vigilância, apesar de inquietante, por muitas vezes não ataca problemas centrais da coleta e processamento massivo de informações que não são consideradas íntimas, ou tabu.

A maior parte dos dados coletados não representam, por si só, uma verdadeira intrusão à vida íntima. Endereço, estado civil, número de CPF, dentre outros, são dados que há muito tempo são compartilhados a fim de se realizar atos da vida cotidiana. Muitos não se sentem inibidos em compartilhar seus hábitos de consumo e outras características de seu estilo de vida que hoje são capturados no uso de redes sociais e outros aplicativos.

Somente apontar que grandes empresas possuem grandes quantidades de informações acerca do indivíduo e estão o tempo todo coletando mais informações desse tipo pode gerar certo desconforto, mas não explica completamente o porquê de isso ser algo negativo, ou como isso afeta diretamente a vida das pessoas. Assim, torna-se comum na população a reprodução do argumento de "não tenho nada a esconder"[53]. Esse argumento considera que se a pessoa não faz nada de errado ela não tem motivo para se preocupar com suas informações. Desse modo, não se observa o real problema de todos terem seus dados coletados livremente, afinal, servirão para melhorar a experiência no uso de produtos e serviços. Somente quem desenvolve atividades ilícitas poderá sofrer alguma consequência, o que também é algo positivo sob o ponto de vista da repressão à criminalidade.

Para Daniel Solove[54] o que deve ser o foco das discussões, para melhor se entender as ameaças à privacidade e a outros direitos no atual momento, é o que o autor chama de burocracia, presente nas instituições que tomam decisões sobre a vida dos indivíduos. Ao

[53] SOLOVE, Daniel J. Why privacy matters even if you have 'nothing to hide'. **Chronicle of Higher Education**, v. 15, 2011.
[54] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004.

compreender a burocracia dessas instituições e como isso afeta a experiência individual de cada um, fica mais claro o problema da coleta massiva de dados com fim de estabelecimento de perfis.

O que Solove considera como burocracia, tomando como referência Max Weber, é uma forma de organização de instituições, públicas ou privadas, baseada em estruturas hierárquicas e em procedimentos altamente roteirizados, que busca aumento de eficiência e padronização de decisões com alta especialização e expertise[55]. Solove observa que apesar de a burocracia trazer benefícios para a sociedade moderna, todo esse procedimento pode se tornar extremamente desumanizado pois visa eliminar qualquer elemento não quantificável, ou intangível, do processo de tomada de decisões e por isso frequentemente não é capaz de atender às necessidades especiais de um particular. Outro problema da burocracia é sua falta de transparência para o público, de forma a dificultar o escrutínio das decisões. Além disso, burocracias costumam ter pouco cuidado na maneira com que usam informações pessoais. Assim, Solove identifica problemas similares na maneira como os grandes bancos de dados são utilizados atualmente:

> O problema com as *databases* emerge com a submissão de informações pessoais ao processo burocrático com pouco controle inteligente ou limitação, o que resulta na nossa falta de participação significativa em decisões sobre a nossa informação. Processos de tomada de decisão burocráticos estão sendo exercidos cada vez mais frequentemente sobre uma esfera cada vez maior de nossas vidas, e nós temos pouco poder ou voz dentro de tal sistema, que tende a estruturar nossa participação por meios padronizados que falham em nos permitir a alcançar nossos objetivos, desejos e necessidades.[56]

Os grandes atores do setor privado que se utilizam do *Big Data* não necessariamente coagem ou punem pessoas, como a ideia tradicional de um "vigilante", mas criam um sentimento de desempoderamento e deixam-nas vulneráveis, retirando totalmente seu controle sobre as informações pessoais. Ao menos em países democráticos, o que hoje se observa não é uma autoridade centralizadora que visa exercer total controle sobre os cidadãos através de sua constante vigilância, mas vários agentes, de diferentes setores, que buscam entender o comportamento humano a fim melhorar os

---

[55] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.38

[56] No original: "The problem with databases emerges from subjecting personal information to the bureaucratic process with little intelligent control or limitation, which results in our not having meaningful participation in decisions about our information. Bureaucratic decision-making processes are being exercised ever more frequently over a greater sphere of our lives, and we have little power or say within such a system, which tends to structure our participation along standardized ways that fail to enable us to achieve our goals, wants, and needs". SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.52

resultados de suas atividades. Para Solove, o objetivo de grande parte da coleta de dados usado para marketing e desenvolvimento de produtos não visa a supressão da individualidade, mas estudá-la e explorá-la[57]. Nesse ponto, há de se fazer uma ressalva ao argumento do autor, que por vezes parece deixar de lado a possibilidade e a capacidade de grandes empresas utilizarem-se das tecnologias da informação para moldar comportamentos humanos para ganhos econômicos, questão que não deve ser ignorada.

Apesar disso, ao mudar o foco da vigilância para a burocracia, Solove consegue explicitar melhor os problemas de se viver em mundo onde terceiros estabelecem, unilateralmente, perfis pessoais que visam capturar aspectos íntimos da personalidade de uma pessoa.

Stefano Rodotà também reflete sobre uma progressiva mudança da Sociedade da Vigilância para uma Sociedade da Classificação, em que a coleta sistemática de informações não visa desencorajar comportamentos, mas explorar e promover certos hábitos de consumo. Há assim produção incessante de perfis individuais, familiares, de grupo, obtida por meio da utilização e do cruzamento das mais diversas informações. Isso passa a ser essencial para a definição das estratégias de empresas, tanto no desenvolvimento de produtos quanto na publicidade, e produz um choque entre a esfera privada e as relações de mercado. A classificação e a segmentação determinam a seleção de interesses comercialmente significativos, o que pode implicar na exclusão de qualquer outro interesse que não alcance uma determinada "massa crítica", com impactos negativos para a diversidade. Rodotà ressalta que a plenitude da esfera pública depende diretamente da liberdade com a qual pode ser construída a esfera privada[58].

A elaboração de perfis, para Solove, se equipara à construção de biografias não autorizadas, mas que são muitas vezes reducionistas:

> Nossa biografia digital é, então, do tipo não autorizada, somente parcialmente verdadeira e muito redutiva. Nós todos devemos conviver com essas biografias não autorizadas sobre nós, cujo conteúdo completo normalmente não podemos ver. Ainda que um dossiê mais extenso possa ser menos redutivo em capturar nossa personalidade, esse teria maior efeito controlador sobre a vida de um indivíduo. Não somente nossas biografias digitais são redutivas, mas elas são frequentemente inexatas. No mundo burocratizado, uma das ameaças crescente

[57] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.34.
[58] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.114-115.

> é que estaremos sujeitos a inadvertência, descuido e inconsciência da burocracia.[59]

Acrescenta-se ainda que os perfis elaborados se utilizando de grandes bases de dados podem ser também altamente enviesados[60]. Os atores do setor privado, ao transferirem toda tomada de decisão relativa aos particulares que usufruem de seu serviço a um procedimento automatizado, permitem que aspectos essenciais da experiência pessoal sejam ignorados, além de potencialmente perpetuar vieses discriminatórios presentes na base de dados utilizados na análise. Os problemas da burocracia não são problemas de inibição quanto às informações compartilhadas, mas problemas de processamento das informações[61].

Nesse sentido, observam-se os seguintes problemas que emergem da burocracia no processamento de informações para formação de perfis, e que a regulação da prática de *profiling* deve levar em conta: problemas relativos à agregação, uma vez que pequenos pedaços de dados, quando combinados formam uma informação muito mais ampla e reveladora; problemas de exclusão, que ocorrem quando as pessoas são impedidas de ter conhecimento sobre como as informações sobre elas estão sendo usadas, ou são impedidas de acessar e corrigir erros nos dados; problemas de usos secundários, quando a exploração de dados obtidos para uma finalidade é feita para um propósito não relacionado, sem o conhecimento do sujeito ou controle; problemas de distorções, que ocorrem pois, embora as informações pessoais possam revelar bastante sobre as personalidades e atividades pessoais, muitas vezes não reflete a pessoa como um todo, apenas traça um perfil distorcido, especialmente porque os registros são redutivos e geralmente capturam informações de forma padronizada em formato com muitos detalhes omitidos[62].

---

[59] No original: "Our digital biography is thus an unauthorized one, only partially true and very reductive. We must all live with these unauthorized biographies about us, the complete contents of which we often do not get to see. Although a more extensive dossier might be less reductive in capturing our personalities, it would have greater controlling effects on an individual's life. Not only are our digital biographies reductive, but they are often inaccurate. In today's bureaucratized world, one of the growing threats is that we will be subject to the inadvertence, carelessness, and mindlessness of bureaucracy." SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.46.

[60] O'NEIL, Cathy. **Weapons of math destruction: how Big Data increases inequality and threatens democracy**. Nova Iorque: Crown, 2016.

[61] SOLOVE, Daniel J. Why privacy matters even if you have 'nothing to hide'. **Chronicle of Higher Education**, v. 15, 2011.

[62] SOLOVE, Daniel J. Why privacy matters even if you have 'nothing to hide'. **Chronicle of Higher Education**, v. 15, 2011.

Algumas dessas questões são especialmente difíceis de se lidar sem que certas práticas consolidadas no mercado sejam significativamente afetadas, pois como visto no tópico anterior, são inerentes ao surgimento e uso do *Big Data*. É o caso dos usos secundários dos dados e a das distorções, uma vez que se coletam dados com a expectativa de que no futuro se tornem úteis para diversos fins e pois a informação do *Big Data* é imprecisa e desestruturada, de forma a gerar perdas no âmbito do micro e ganhos significativos no macro.

A visão desses problemas permitirá a proposição de soluções mais adequadas, sob o ponto de vista jurídico, para questão da regulação do uso de perfis pessoais pelo setor privado. No próximo capítulo, busca-se analisar aspectos técnicos do *profiling*, bem como suas principais aplicações no mercado. Assim será possível fazer uma análise mais precisa de características relevantes da prática que devem ser levadas em conta na construção do direito.

2. PROFILING

O termo "*profile*", na língua inglesa, pode ser utilizado como verbo ou como substantivo. Enquanto substantivo o termo se traduz ao português como "perfil". Como verbo, "*to profile*" é o ato de escrever uma pequena descrição sobre a vida ou trabalho de alguém, ou de prever o comportamento de um cliente ou criminoso baseado na informação que se tem sobre eles[63]. *Profiling* é a ação descrita no verbo sendo realizada continuamente, e não possui uma tradução direta para o português.

É possível encontrar nos dicionários portugueses o termo "perfilar", no sentido de "desenhar o perfil de" ou de formar uma linha "Pôr(-se) em posição vertical; aprumar(-se), endireitar(-se)."[64]. Do termo perfilar é possível se utilizar perfilação ou perfilamento para traduzir a ideia de *profiling*.

Na versão em língua inglesa do Regulamento EU 2016/679 do Parlamento Europeu, chamado de Regulamento Geral de Proteção de Dados (GDPR), o termo *profiling* aparece em diversos dispositivos. Na versão oficial em português é utilizado, no lugar de *profiling*, a expressão "definição de perfis", o que indica que expressões como perfilamento ou perfilação não se adequaram perfeitamente. No presente estudo, optou-

---

[63] CAMBRIDGE UNIVERSITY PRESS. **Cambridge Dictionary**. Cambridge, 2019. Disponível em: https://dictionary.cambridge.org/us/dictionary/english/profile. Acesso em: 31 ago. 2019.

[64] MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. São Paulo: Melhoramentos, 2019. Disponível em: https://michaelis.uol.com.br/moderno-portugues/. Acesso em: 1 set. 2019.

se pela adoção do termo em língua estrangeira, assim como vem sendo usualmente feito por outros autores brasileiros que tratam do tema[65]. No próximo tópico será explorado o conceito de *profiling* adotado na presente dissertação e algumas definições essenciais para devida compreensão dessa prática.

2.1 Conceitos e classificações do *profiling*

Ao longo do tempo, o termo *profiling* foi estudado com maior amplitude no âmbito do combate ao crime, como uma técnica utilizada para identificar serial killers com base em perfis que compilavam seus traços psicológicos[66]. No setor de marketing as discussões acerca do *profiling* também se desdobram há muitos anos, devido à necessidade do setor de conhecer os consumidores e buscar maior precisão em se atingir um público alvo[67].

Com o desenvolvimento das técnicas de coleta e tratamento de dados, a definição de perfis foi facilitada e se tornou útil em diversas áreas. Para os fins do presente estudo, buscou-se uma definição de *profiling* que sirva para tratar da extração de perfis através do processamento de dados em massa em diversos contextos.

O artigo de Roger Clarke "Profiling: a Hidden Challenge to the Regulation of Data Surveillance"[68] reflete uma primeira tentativa de se sistematizar os conceitos e métodos envolvidos nas práticas de definição de perfis e seus desafios legais e regulatórios no âmbito da governança de dados. Na definição de Clarke, perfil é uma representação esquemática dos interesses de uma pessoa usado na recuperação de informações, sendo *profiling* o processo de criação e uso desse perfil. Segundo o autor, à sua época, definições concretas eram encontradas somente no setor de marketing, como

---

[65] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014. MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação**: *Profiling* e risco de discriminação. 2018. Dissertação (Mestrado) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018.

[66] FERRARIS, Valeria; BOSCO, Francesca; CAFIERO, G.; D'ANGELO, Elena; SULOYEVA, Y., **Working paper: defining *profiling***. United Nations Interregional Crime and Justice Research Institute (UNICRI), December, 2013. Disponível em:<http://www.unicri.it/special_topics/citizen_*profiling*/*PROFILING*project_WS1_definition_0208.pdf >. Acesso em: 06 ago. 2019, p.2.

[67] ZANATTA, Rafael A. F. Perfilização, Discriminação e Direitos: Do Código de Defesa do Consumidor à Lei Geral de Proteção de dados pessoais. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/stats>. Acesso em: 31 ago. 2019.

[68] CLARKE, Roger. *Profiling*: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, Camberra, v. 4, p. 403-419, 1993.

aplicação de técnicas estatísticas para descobrir quais consumidores apresentam bons prospectos para aceitar uma oferta, e de combate ao crime, como forma de correlacionar diferentes dados a fim de determinar quão perto uma pessoa está de uma pré-determinada caracterização ou modelo de infração. Seu uso de forma explícita também era pouco documentado, aparecendo nos setores supracitados e em algumas publicações de auditorias fiscais. Para Clarke o *profiling* consiste em uma espécie de triagem que envolve múltiplos fatores.

Nos últimos anos o âmbito de aplicação do *profiling* foi ampliado significativamente. Sloot e Schendel apontam que o termo é comumente associado com o *Big Data* e algumas vezes até incluído em seu próprio conceito. Nesse sentido, *profiling* se refere a correlações estatísticas, normalmente de natureza preditiva, acerca de características de indivíduos ou grupos[69]. Mireille Hildebrandt desenvolveu estudo acerca do *profiling* inserido no contexto de desenvolvimento do *Big Data* que é referenciado nos principais artigos contemporâneos que tratam do tema[70]. A autora afirma que o termo é utilizado para se referir a um conjunto de tecnologias que compartilha uma característica comum, qual seja, o uso de algoritmos e outras técnicas de automatização para criar, descobrir ou construir conhecimento derivado de grandes bases de dados. Essas tecnologias são integradas na prática de definição de perfis, que são utilizados na tomada de decisões, muitas vezes sem intervenção humana no processo. Nesse sentido, a autora define *profiling* como o processo de construção de conhecimento, derivado da descoberta de correlação de dados em uma *database*, com a criação de perfis compostos por um conjunto de dados correlacionados que permitem a individuação e representação de um sujeito, ou sua identificação como membro de um grupo ou categoria.

Em estudo conduzido por coletivo de acadêmicos, denominado ““Protecting Citizen’s Rights Fighting Illicit Profiling” e desenvolvido no âmbito do programa “Direitos Fundamentais e Cidadania”, realizado pela União Europeia, foi estabelecido o seguinte conceito para *profiling*, tomando como base os conceitos expostos por Hildebrandt:

---

[69] SLOOT, Bart van der; SCHENDEL; Sacha van. Ten questions for future regulation of big data: a comparative and empirical legal study. **Journal of Intellectual Property, Information Technology and Eletronic Commerce Law,** v.7, n.2, p.110-145, 2016.

[70] HILDEBRANDT, Mireille. Defining *Profiling*: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 17-43.

> *Profiling* é uma técnica de processamento automático de dados pessoais e não pessoais, que visa desenvolver conhecimento preditivo a partir de dados na forma de construção de perfis que podem, subsequentemente, ser aplicados como base para tomada de decisões. Um perfil é um conjunto de dados correlacionados que representa um (humano ou não humano, indivíduo ou grupo) sujeito. Construir perfis é o processo de descobrimento de padrões inesperados entre dados em uma grande base de dados que pode ser utilizada para criar perfis. Aplicar perfis é o processo de identificar ou representar um sujeito específico ou de identificar o sujeito como membro de um grupo específico ou categoria e tomar algum tipo de decisão baseada nessa identificação e representação.[71]

Conforme visto no início deste capítulo, é possível encontrar uma definição legal para *profiling* no Regulamento Geral de Proteção de Dados do Parlamento europeu. Na sua versão em português foi utilizado o termo "definição de perfis", assim conceituado:

> Definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações[72].

Nas diretrizes do Working Party 29 sobre *profiling* e decisões automatizadas[73] é destacado que a simples classificação de indivíduos em categorias não necessariamente leva ao *profiling*, que somente ocorrerá quando a classificação for feita com intuito de fazer uma previsão ou tirar uma conclusão acerca do indivíduo, como, por exemplo, atribuir-lhe uma pontuação de crédito.

No Brasil, a Lei Geral de Proteção de Dados, (Lei n. 13.709 de 14 de agosto de 2018) não trouxe conceito expresso para o procedimento de definição de perfis. Porém, Rafael Zanatta defende que a interpretação de alguns dispositivos da lei que fazem referência à formação de perfis permite a conceituação de "perfilização enquanto

---

[71] No original: "Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation". FERRARIS, V.; BOSCO, F.; CAFIERO, G.; D'ANGELO, E.; SULOYEVA, Y., **Working paper: defining *profiling***. United Nations Interregional Crime and Justice Research Institute (UNICRI), 2013. Disponível em: <http://www.unicri.it/special_topics/citizen_*profiling*/*PROFILING*project_WS1_definition_0208.pdf>. Acesso em: 06 ago. 2019, p.32.

[72] UNIÃO EUROPEIA. Regulamento nº 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 3 de nov. 2019.

[73] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated individual decision-making and *Profiling* for the purposes of Regulation 2016/679**. Bruxelas, 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 2 jul. 2019.

processo automatizado de tratamento de dados que objetiva a análise e predição de comportamentos pessoais, profissionais, de consumo e de crédito."[74]. Uma análise aprofundada dos aspectos legais do *profiling* presentes nas legislações europeia e brasileira será desenvolvida posteriormente, no quarto capítulo do presente estudo.

Hildebrandt apresenta uma diferenciação entre *profiling* não automatizado, *profiling* automatizado e *profiling* autônomo[75].

O *profiling* não automatizado se refere a um processo racional de construção de conhecimento, conduzido sem automação. Mesmo antes da disseminação da computação, investigadores compunham perfis a fim de identificar criminosos, o setor de publicidade estudava o perfil de diferentes consumidores e especialistas em recursos humanos utilizavam perfis para entender o potencial de empregados para realizar tarefas específicas. Assim, Hildebrandt afirma que *profiling* é uma forma de generalização ou categorização que todos nós aplicamos rotineiramente no decorrer da vida.

O *profiling* automatizado, por sua vez, é resultado do processo de mineração de dados que permite o estabelecimento de previsões baseadas no comportamento passado observado. Como visto no capítulo anterior, as análises de dados no contexto do *Big Data*, como é o caso do *profiling* automatizado, são conduzidas sem o estabelecimento prévio de hipóteses, sendo, portanto, caracterizado como espécie de construção do conhecimento do tipo indutivo, pois observa uma correlação e espera que a correlação se repita no futuro. Assim, no *profiling* automatizado não são buscadas causas, mas previsões seguras para subsidiar a tomada de decisões relativa a um sujeito.

Ao contrário do que ocorre no método científico tradicional, as hipóteses não são estabelecidas a *priori* e depois testadas, mas extraídas previamente pela observação de correlações numa base de dados. Após, no momento de aplicação dos perfis, as hipóteses encontradas são testadas, de modo que o processo indutivo de geração de perfis é complementado pelo processo dedutivo de testá-los sobre uma nova base de dados. Os resultados obtidos são constantemente realimentados nos algoritmos de forma a aprimorar as previsões feitas. Nesse procedimento, são utilizadas funções automatizadas para

---

[74] ZANATTA, Rafael A. F. Perfilização, Discriminação e Direitos: Do Código de Defesa do Consumidor à Lei Geral de Proteção de dados pessoais. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/stats>. Acesso em: 31 ago. 2019.

[75] HILDEBRANDT, Mireille. Defining *Profiling*: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 23.

coletar e agregar dados. São desenvolvidas tecnologias que vão além do aconselhamento para tomada de decisões, mas que substituem a própria decisão humana. Inicialmente utilizadas para decisões de baixa complexidade, cada vez mais as tecnologias se movem para substituir decisões humanas de alta complexidade.

Ainda assim, no *profiling* automatizado a atuação humana ocorre na construção do procedimento, como, por exemplo, na seleção da base de dados a ser utilizada e dos parâmetros e critérios a serem incorporados nos algoritmos, bem como na escolha do momento de início e fim de todo o processamento de dados. Hildebrandt visualiza a chegada, no futuro, de um estágio de *profiling* autônomo. O *profiling* autônomo seria o processo pelo qual o papel humano é minimizado ao máximo e o processo de tomada de decisão é inteiramente conduzido pela máquina. O *profiling* autonômo vai além do *profiling* automatizado pois novas tecnologias conduzem o processo de tomada de decisão, proporcionando um ambiente reajustado baseado em seu perfil e sem necessidade de intervenção humana . A inteligência ambiente e a Internet das coisas são baseadas na ideia de *profiling* autônomo. As máquinas conduzem o processo de tomada de decisão, proporcionando um ambiente constantemente reajustado baseado em perfis e sem necessidade de intervenção humana.

Outra importante classificação a ser feita se refere aos sujeitos envolvidos no processo de *profiling*. Assim, o *profiling* pode ser individual ou de grupos, sendo que o *profiling* de grupos pode ser distributivo ou não distributivo.

O *profiling* individual, também chamado de personalizado, é feito com o levantamento de dados pessoais relativos a uma pessoa específica, a fim de identificá-la dentro de um grupo ou a fim de inferir algumas de suas características não explícitas na base de dados, como hábitos, comportamento, preferências, riscos e outras características econômicas e sociais. A mineração de dados que se referem a um sujeito específico permite o chamado *profiling* individual direto. Por exemplo, a coleta de dados durante a digitação permite que se forme um perfil individual que reflete a forma de digitar de certa pessoa. Assim é possível que o provedor de serviço a identifique sempre que o aquele usuário específico estiver online, pois reconhece sua assinatura de comportamento biométrico. Desse modo, o servidor é capaz de entender o comportamento de um usuário individualizado, construindo um perfil específico para fins de autenticação daquele

usuário, para oferecer bens e serviços, para que seja vendido a partes interessadas, ou reportado quando requisitado por autoridades[76].

O *profiling* de grupos[77] identifica e representa um grupo. Pode ser feito pela coleta, agregação e armazenamento de dados relevantes por um período estendido, extraindo-se correlações entre os dados a fim de formar uma categoria na qual são ligados certos atributos. A categoria é chamada de grupo e os atributos formam o perfil desse grupo. Outra espécie de *profiling* de grupos se dá pela coleta de dados direcionada a um grupo de pessoas pré-existente, que formam uma comunidade. Com a coleta e processamento de dados desse grupo, encontram-se atributos em comum entre seus membros e o perfil desse grupo. Portanto, o *profiling* de grupos pode se referir tanto à busca de características de uma certa comunidade já estabelecida, como à criação de grupos novos baseados em características comuns extraídas dos dados. Por exemplo, pode-se buscar as tendências de consumo entre praticantes de uma certa religião, ou levantar dados de consumidores a fim de encaixá-los em uma categoria artificial que represente valores buscados pela empresa.

O *profiling* de grupos pode ser distributivo ou não distributivo[78]. O *profiling* distributivo identifica um grupo no qual todos os membros compartilham as mesmas características presentes no perfil estabelecido. Assim, o perfil do grupo pode ser aplicado para qualquer de seus membros, de forma que é considerado também perfil pessoal no momento de aplicação.

No *profiling* de grupos não distributivo, os membros podem não compartilhar todos os mesmos atributos, ou mesmo não possuir todas as características ligadas ao perfil do grupo, e, ainda assim, serem agrupados conjuntamente. Por exemplo, com intuito de se diagnosticar algum distúrbio psicológico, inicialmente todas as características usualmente encontradas no grupo de pessoas acometidas pelo distúrbio é agrupado em um perfil. Após, verifica-se as características do possível membro, atribuindo certa

---

[76] NABETH, Thierry. Reply: Further Implications?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 30.

[77]FERRARIS, V.; BOSCO, F.; CAFIERO, G.; D'ANGELO, E.; SULOYEVA, Y., **Working paper: defining *profiling***. United Nations Interregional Crime and Justice Research Institute (UNICRI),2013. Disponível em: <http://www.unicri.it/special_topics/citizen_*profiling*/*PROFILING*project_WS1_definition_0208.pdf>. Acesso em: 06 ago. 2019, p.5.

[78] HILDEBRANDT, Mireille. Defining *Profiling*: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 17-43.

pontuação para cada uma das características encontradas que se encaixem no estabelecido para o perfil. Por fim, estabelece-se uma pontuação limiar para que a pessoa seja elegível como membro daquele grupo. Nem todas as pessoas diagnosticadas terão todo o conjunto de características típicas ligadas ao distúrbio estudado e pode haver diferenças significativas entre as pessoas agrupadas, razão pela qual se fala em *profiling* não distributivo.

Jaquet-Chiffelle aponta[79], ainda, que o *profiling* pode ser direto ou indireto. No *profiling* direto os dados são coletados para visando um único sujeito ou um pequeno grupo de sujeitos, e o conhecimento derivado é aplicável somente em relação aos sujeitos sobre os quais se deu a coleta de dados. Assim é possível caracterizar individualmente uma pessoa e prever seus comportamentos futuros de forma específica.

No *profiling* indireto, dados são coletados de uma grande população e grupos ou categorias de pessoas com atributos correlacionados são formados. Outros indivíduos podem, então, ser identificados como membros do grupo e como pessoas que compartilham das mesmas características usando os atributos que emergiram da coleta inicial de dados. Assim, o perfil aplicado é derivado de dados referentes a outros sujeitos. É o que ocorre, por exemplo, quando serviços de *streaming* como a Netflix, sugerem filmes ou seriados para um usuário específico baseado nas visualizações e preferências de outras pessoas que possuem certas características em comum.

A definição de perfis pode servir a diferentes objetivos. Hidelbrandt aponta que os principais usos são para individualização, avaliação de risco ou avaliação de oportunidades para o controlador dos dados utilizados[80]. O *profiling* é utilizado para individualização, por exemplo, em investigações criminais a fim de se levantar as principais características de um suspeito. Como forma de avaliação de risco é comum seu uso para tomada de decisões quanto à concessão de crédito por instituições financeiras ou para se definir o prêmio por seguradoras. Seu uso para avaliação de oportunidades tem como maior exemplo o setor de marketing, que busca, por meio do *profiling*, descobrir indivíduos e grupos com maior potencial de compra de determinados produtos.

---

[79] JAQUET-CHIFFELLE, David-Olivier. Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 34.

[80] HILDEBRANDT, Mireille. Defining *Profiling*: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 19.

Grande parte da utilização do *profiling* se refere ao chamado *profiling* comportamental, referido na literatura estrangeira como *behavioural profiling*. Esse tipo de procedimento pode ser definido como o estudo de padrões de comportamento e o agrupamento de usuário de acordo com seu comportamento exibido[81]. Isso visa coletar e armazenar registros de eventos e ações praticadas pelo sujeito em certos momentos a fim de estabelecer qual o seu comportamento típico. Identificados os padrões típicos de comportamento, busca-se encaixar o sujeito em determinada categoria que apresenta os mesmos atributos e que possui, por exemplo, tendências a consumir certo produto, inadimplir uma obrigação ou assumir determinado risco. Também é utilizado para detectar desvios desse comportamento, sendo utilizado como forma de autenticação e segurança no meio digital, para identificar que o sujeito é realmente quem afirma ser[82].

Em conclusão, ao se falar em *profiling*, no presente estudo, refere-se ao *profiling* automatizado, individual ou de grupos, direto ou indireto, como forma de construção de conhecimento preditivo. Esse procedimento envolve a construção de perfis a partir da análise automatizada de grandes quantidades dados e com objetivo de se tomar uma ação em relação ao sujeito perfilado (enviar um anúncio direcionado, aprovar ou negar a concessão de crédito, personalizar o serviço oferecido pela organização que conduz o *profiling*, dentre outras). No próximo tópico, serão apresentados os procedimentos usualmente seguidos em práticas de *profiling*, as técnicas utilizadas para coleta dos dados que alimentam a prática e como se dá a extração de conhecimento a partir da base de dados formada.

2.2 Procedimentos e técnicas

Segundo Clarke[83], o processo de *profiling* pode ser descrito nos seguintes passos: Inicialmente, faz-se uma descrição da classe de pessoas pela qual a organização que conduz o processo procura. Após, é utilizada informação pré-existente para definir o perfil dessa classe de pessoas, com as características usualmente encontradas em pessoas já identificadas como pertencentes à classe. Assim, busca-se expressar formalmente o perfil, com a definição de diferentes pesos a serem atribuídos entre as correlações

---

[81] CANHOTO, A.; BACKHOUSE, J. General Description of the Process of Behavioural *Profiling* In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 3, p. 47-63.

[82] YANNOPOULOS, A.; ANDRONIKOU, V.; VARVARIGOU, T. Behavioural Biometric Profi ling and Ambient Intelligence In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 5, p. 89-106.

[83] CLARKE, Roger. *Profiling*: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, Camberra, v. 4, p. 403-419, 1993.

buscadas e o estabelecimento de pontuações limiares para que uma pessoa seja enquadrada no perfil, por exemplo. Em seguida, é iniciado o processo de coleta de dados relativos à população relevante. Com base na coleta feita, é explorada a base de dados formada em busca dos indivíduos cujas características aderem ao perfil estabelecido, em processo altamente automatizado. Por fim, a organização que realiza o *profiling* pratica uma ação em relação aos indivíduos identificados, como enviar uma propaganda, recrutar para a empresa, ou iniciar uma investigação. Clarke entende o perfilhamento como uma espécie de triagem que envolve múltiplos fatores. Ele aponta que pode ser feito inteiramente com dados que a organização possui, mas normalmente são utilizadas múltiplas fontes.

Algumas mudanças no procedimento de *profiling* automatizado ocorrem após a descrição feita por Clarke, devido aos desenvolvimentos tecnológicos ocorridos nos anos que se seguiram. Nesse sentido, András László[84] afirma que qualquer procedimento de *profiling* envolve identificar informação, fazer previsões e por fim, inferências. Assim, o autor coloca que o procedimento pode ser dividido em três estágios. O primeiro estágio é a observação, momento no qual dados pessoais ou anonimizados são coletados (de fontes internas ou externas) e organizados. Por exemplo, um banco compila uma lista de maus pagadores e todas as demais informações disponíveis acerca de cada um deles. Após, é realizado o processo de mineração dos dados (*data minining*), em que métodos estatísticos são aplicados para estabelecer, com certa margem de erro, correlações entre variáveis observadas. Nesse estágio, o banco poderia observar, por exemplo, uma ligação estatística entre uma alteração no estado civil de certo consumidor que é seguida por um período de inadimplência. O resultado desse estágio do procedimento é a categorização dos indivíduos em grupos com base nas características observáveis, com intenção de inferir características não observáveis. O último estágio, da inferência, consiste em aplicar o mecanismo descrito a fim de inferir, com base em dados relativos a uma pessoa identificada ou identificável, novos dados que são, de fato, os da categoria a qual ela pertence.

[84] LASZLO, Andras. *Profiling*, Data Mining and Law Enforcement: Definitions**. 50 Annales U. Sci. Budapestinensis Rolando Eotvos Nominatae**, Budapeste, 2009.

Paul de Hert e Hans Lammerant[85] ressaltam que a prática de *profiling*, nos dias de hoje, é baseada no uso de "*Knowledge Discovery Databases*" (KDD), processo do qual a mineração de dados é apenas uma etapa. O objetivo das KDD é encontrar padrões úteis nos dados. Para isso, inicialmente são feitas a coleta, a seleção e a preparação dos dados. Após, é realizada a análise por meio de algoritmos programados para reconhecer padrões na base de dados, sendo essa etapa a mineração de dados em si. Conforme destacado ao longo do presente trabalho, Hert e Lammerant também ressaltam que os padrões encontrados indicam correlações entre os dados, e não causas, podendo ser considerados no máximo indicativo de causas. Uma vez estabelecidos, deve haver a devida avaliação dos padrões encontrados para determinar sua relevância. Por fim, dos padrões selecionados, pode-se derivar um perfil, não mais consistente em um grupo de dados "cru", mas em um modelo matemático do fenômeno observado.

A mineração de dados é assim definida por Calders e Custers:

> Mineração de dados é comumente definida como a automatizada ou conveniente extração de padrões representativos de conhecimento implicitamente armazenados ou capturáveis em grandes bases de dados, em armazéns de dados, na Rede, em outros repositórios de informação em massa ou em fluxo de dados. Diferentemente das estatísticas, onde o dato é coletado com o propósito particular de testar uma hipótese, ou estimar o parâmetro de um modelo, na mineração de dados usualmente inicia-se com dados históricos que não foram necessariamente coletados para análise, mas como um produto residual de um sistema operacional. Nesse contexto, a mineração de dados é referida como análise de dados secundária (...) ao invés de o usuário estabelecer uma hipótese a ser verificada sobre a base de dados, os dados em si são usados para gerar a hipótese[86].

Com a etapa de mineração de dados é possível se descobrir relações nos dados que não seriam vistas de outras maneiras, mas o processo seguido pelo algoritmo para chegar à correlação não é adequadamente acessível. Isso ocorre porque os algoritmos que formam as correlações são 'opacos', de maneira que se torna difícil, e para alguns, quase

---

[85] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. *In*: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

[86] No original: "Data mining is often defined as the automated or convenient extraction of patterns representing knowledge implicitly stored or catchable in large databases, data warehouses, the Web, other massive information repositories, or data streams. Unlike in statistics, where the data is collected specially with the purpose of testing a particular hypothesis, or estimating the parameters of a model, in data mining one usually starts with historical data that was not necessarily collected with the purpose of analysis, but rather as a by-product of an operational system. In this context, data mining is often referred to as secondary data analysis (...)instead of the user stating which hypothesis needs to be checked against the data, the data itself is used to generate the hypotheses". CALDERS, Toon; CUSTERS, Bart. What Is Data Mining and How Does It Work? In: CUSTERS, Bart et al (ed.). **Discrimination and Privacy in the Information Society**: Data Mining and *Profiling* in Large Databases. Berlim: Springer, 2013. cap. 2, p. 28.

impossível, determinar como o modelo resultante foi construído e como as correlações foram avaliadas pelo algoritmo. Esse tipo de *data mining* é chamado de descritivo, pois constrói novos olhares sobre certo domínio que permite melhor planejamento e alocação de recursos[87]. Porém, no procedimento descritivo, um objetivo não é formado previamente, razão pela qual é também chamado de não supervisionado. Outra forma de mineração de dados é a do tipo preditivo, que, para fins de *profiling*, ocorre quando a informação relativa a um sujeito é minerada para se determinar se ele se encaixa em um perfil previamente estabelecido (chamado então, de mineração de dados supervisionada).

O método preditivo comumente utilizado nesse tipo de mineração de dados é a classificação. Algoritmos classificadores buscam verificar se um novo objeto analisado pode ser encaixado numa classe previamente estabelecida. As classes possuem campos de entrada (*imput fields)* com diferentes atributos associados a ela. Quando o novo objeto contém certo número de atributos encontrados na classe, é provável que o objeto pertença à classe. Por exemplo, uma classe de "papagaios" terá um conjunto de características (bico preto, penas verdes, cauda curta, dentre outras). Quanto mais características definidas para a classe forem identificadas no novo objeto, maior a probabilidade de ele pertencer a classe. Esse procedimento é, basicamente, o que ocorre no *profiling* de grupos não distributivo, conforme conceituado anteriormente. Schermer destaca o fato de que o procedimento apresentará natureza probabilística quanto ao pertencimento do objeto à classe, sem que se possa chegar a uma certeza[88].

Ambas as técnicas de mineração de dados podem ser utilizadas em conjunto no *profiling*, mas em momentos diferentes. Ao se definir um perfil, as características que irão compor esse perfil podem ser extraídas de correlações encontradas em bases de dados por meio da mineração descritiva. Ao se definir se certa pessoa se encaixa no perfil determinado a fim de tomar uma decisão relativa a ela, utiliza-se da mineração de dados preditiva, alimentada com as informações existentes acerca desta pessoa, para se verificar se os atributos encontrados podem ser encaixados no perfil pré-estabelecido.

O procedimento de *profiling* automatizado depende da grande disponibilidade de dados. Assim, serão estudadas algumas das principais formas de coleta de dados

---

[87] SCHERMER, Bart M. The limits of privacy in automated *profiling* and data mining. **Computer Law & Security Review**, Amsterdã, v. 27, p. 45-52, 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364910001767. Acesso em: 31 ago. 2019.

[88] SCHERMER, Bart M. The limits of privacy in automated *profiling* and data mining. **Computer Law & Security Review**, Amsterdã, v. 27, p. 45-52, 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364910001767. Acesso em: 31 ago. 2019.

realizadas nos dias de hoje, principalmente através do uso da internet. A prática de *profiling* ganhou maior notoriedade e passou a gerar debates públicos com o advento da internet e o uso difundido dessas técnicas por empresas de marketing online. A ampla disseminação de anúncios direcionados aos gostos de usuários da rede levou à crescente preocupação em relação, principalmente, à privacidade dos indivíduos. Nesse sentido, nos Estados Unidos, a *Federal Trade Comission* (FTC), agência responsável pela proteção de direitos dos consumidores no país, emitiu um relatório descrevendo como é feito o rastreamento de informações no ambiente da internet.

Conforme aponta o relatório[89], para fins de direcionamento de anúncios online, dados de navegação de usuários são coletados através de *cookies* e *web bugs*. Cookies são pequenas linhas rastreáveis de código, instaladas no terminal utilizado pelo usuário para acessar páginas na internet. *Web bugs* são pequenos arquivos de imagens exibidas nas páginas de navegação, invisíveis a olho nu, capazes de enviar informações para o servidor responsável acerca do usuário que acessou a página.

Esses recursos são disponibilizados por empresas de marketing que pagam para ter anúncios de seus clientes exibidos nos sites de terceiros e são remuneradas por seus parceiros comerciais conforme o nível de interação de usuários com a propaganda exibida. Assim, ao se acessar um grande portal de notícias, por exemplo, o usuário não está interagindo somente com o provedor de conteúdo responsável por aquele site, mas com toda a rede de anunciantes com a qual aquele portal se relaciona, o que gera uma grande quantidade de "terceiros" coletando informações do usuário, de maneira oculta para a maior parte das pessoas.

Com esses mecanismos, o anunciante é capaz de coletar informações sobre *sites* e sessões dentro do *site* acessado; horário e duração das visitas; termos buscados; compras; interação com anúncios exibidos; a página da qual o usuário veio anteriormente; dentre outras. Ponto relevante ressaltado no relatório é que toda essa informação pode ser coletada mesmo se o consumidor nunca clicar em um anúncio exibido no site.

Após essa coleta, os dados do consumidor são analisados e combinados com dados de outras fontes, referentes a características demográficas, psicográficas ou outros estudos e enquetes realizados ao longo do tempo entre consumidores. Com o cruzamento de

---

[89] FTC. **Online *profiling***: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-*profiling*-federal-tradecommissionreport-congress-june-2000/online*profiling*reportjune2000.pdf>. Acesso em: 31 out. 2019.

grandes bases de dados que se referem a diversas características, os anunciantes podem fazer uma variedade de inferências sobre os interesses de cada consumidor. Assim se forma o perfil detalhado de determinado usuário que visa prever seus gostos, necessidades e hábitos de consumo. Os processos automatizados de computação e a conectividade provida pela internet permitem que esse perfil seja atualizado em tempo real, de forma que decisões instantâneas são feitas a fim de se direcionar o melhor anúncio para aquele determinado usuário, assim que ele carrega uma página na *Web*.

O relatório emitido pela FTC elucida como é conduzido o procedimento de formação de perfil feito por empresas de anúncios online. Basicamente, um *cookie* colocado pela companhia no computador do usuário pode rastrear sua atividade em qualquer site que ele acesse que possua parceria com a empresa, permitindo a coleta de dados em diversas páginas que, aparentemente, não possuem nenhuma relação. Como os *cookies* ficam instalados de maneira perene no terminal do usuário, necessitando, para sua retirada, que o consumidor ativamente os remova, a coleta é feita por um período prolongado. Assim se forma um constante fluxo de informação obtida diretamente do usuário, combinado com outros dados obtidos de fontes diversas, de maneira a formar perfis que contém centenas de campos de dados.

Tecnicamente, o que ocorre ao se conectar a uma página na internet é o seguinte: o navegador utilizado envia informações sobre o terminal do usuário ao servidor em que está hospedado o site, a fim de se comunicar com o servidor e permitir a exposição da página. A informação transmitida contém o tipo de navegador, o sistema operacional do terminal, a linguagem computacional aceita e o endereço IP do usuário. O servidor responde transmitindo o “http” (protocolo de comunicação, que define as regras para comunicação entre os dois pontos) e o “html” (linguagem mais utilizada para páginas na internet, que contém o código do site). Com essa troca de informações é possível que a página acessada seja exibida no terminal do usuário. Dentro do código “html” que o site envia, está presente um *link* para o(s) anunciante(s) parceiro(s) do servidor. O *link* é automaticamente ativado pelo navegador do usuário, enviando as mesmas informações necessárias para acesso ao servidor (sistema operacional, tipo de navegador etc.), bem como o site em que foi ativado o *link* e qualquer outra informação desse anunciante que já esteja armazenada no computador do usuário via *cookies*. Baseado nisso faz-se o cruzamento de todos os dados que o anunciante possui e decide-se qual é o anúncio mais

adequado a ser exibido para aquele usuário. Se o usuário efetivamente clica no anúncio, mais informações são enviadas e absorvidas em seu terminal.

Vale ressaltar que no início dos anos 2000, quando o relatório foi elaborado, toda essa atividade ainda era muito desconhecida pela maioria dos usuários e consumidores, uma vez que os navegadores permitiam amplamente a troca de *cookies* entre o computador pessoal e o servidor acessado sem que o usuário fosse informado. Apenas mais recentemente, em razão do esforço de diversos setores da sociedade civil e das primeiras regulações acerca da proteção de dados pessoais, se tornou comum que grandes sites da *Web* notifiquem usuários sobre sua política de *cookies*.

Ainda assim, toda a rede de anúncios online depende da coleta de dados feita por meio de técnicas de monitoramento da navegação realizada por diversos prestadores desse serviço. Conforme sintetiza Danilo Doneda:

> Estas técnicas podem se basear na navegação em determinados sites, afiliados a um dos diversos serviços de monitoramento da navegação na Internet (*tracking*). Estes serviços podem monitorar a navegação dentro de um determinado site ou grupo de sites pertencentes a uma mesma organização (por exemplo, um mecanismo que monitore a navegação em todos os sites pertencentes à empresa Google Inc.), bem como podem ser multi-site, ou seja, serviços que monitorem a navegação em diversos sites, pertencentes a organizações diversas que seriam filiadas a este serviço de monitoramento.[90]

Assim, um mesmo site pode apresentar grande número de terceiros rastreadores da atividade *online* dos usuários, fato normalmente desconhecido pelo usuário comum, que acredita estar em contato somente com o servidor que acessa. Um simples experimento, conduzido para a presente pesquisa, serve para ilustrar a situação.

A fundação "Eletronic Frontier Foundation", organização sem fins lucrativos que advoga pela defesa de liberdades civis no meio digital, desenvolveu o aplicativo Privacy Badger[91], que serve como uma extensão para navegadores. O aplicativo identifica rastreadores de terceiros presentes ao se carregar uma página qualquer da Internet. Uma vez identificados, a extensão emite um sinal de "não-rastreio". Se ignorado o sinal, a extensão bloqueia o funcionamento do rastreador. O bloqueio ocorre quando identificado o mesmo rastreador em três sites diferentes.

---

[90] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.65.

[91] Mais informações sobre a funcionalidade do aplicativo estão disponíveis em: https://www.eff.org/pt-br/node/99095. Acesso em 30 de ago. 2019.

Acessando os 5 portais dedicados a notícias que possuem maior quantidade de acessos no Brasil [92], verifica-se o seguinte quadro: o site mais acessado (globo.com) teve 10 rastreadores encontrados, sendo 7 bloqueados pelo aplicativo por não respeitarem os parâmetros definidos. Entre os 10 rastreadores, 3 são providos pela empresa Google (google-analytics.com; adservice.google.com e adservice.google.com.br) e o restante por empresas diversas, demonstrando a pluralidade de atores envolvidos na captação de dados. O segundo portal mais acessado (uol.com.br) apresentou 12 rastreadores, sendo 7 bloqueados pelo aplicativo. O terceiro site mais acessado (metropoles.com), apresentou 17 rastreadores, sendo 14 bloqueados. O quarto site mais acessado (otvfoco.com.br) foi o que apresentou maior número de rastreadores, sendo 27 identificados e 14 bloqueados. Por fim, na quinta página mais acessada (portaldoholanda.com.br) foram encontrados 17 rastreadores, sendo 8 bloqueados.

Além da coleta de dados realizada por empresas de marketing, provedores de acesso à internet também aproveitam de sua posição para coletar dados. Segundo Danilo Doneda, o provedor de acesso é capaz de analisar o fluxo bruto de informações trocada entre os usuários e o provedor de conteúdo e identificar informações relevantes dentro dos pacotes trocados entre as partes, em processo denominado DPI (*Deep Packet Inspection*)[93].

Este tópico teve como objetivo apontar, em linha gerais, como o *profiling* é feito nos dias de hoje e apresentar algumas das principais técnicas envolvidas nas diferentes fases do procedimento. Passa-se agoraao exame dos benefícios trazidos por esse tipo de análise de dados e dos riscos envolvidos na sua aplicação, focando, principalmente, em aspectos do desenvolvimento da personalidade individual.

2.3 Benefícios e riscos do *profiling*

Profiling é uma forma de analisar informações e de se utilizar de dados pessoais para avaliar aspectos da personalidade e prever o comportamento humano. Recursos de mineração de dados, potencializados pelo *Big Data* tornam essa prática mais acessível, confiável e economicamente lucrativa[94]. Assim como a maioria das tecnologias, observam-se ganhos importantes com seu uso, principalmente em termos de eficiência e

---

[92] Classificação organizada pela empresa Alexa, propriedade da Amazon. Disponível em: https://www.alexa.com/topsites/countries/BR . Acesso em 14 de ago. de 2019.
[93] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.66.
[94] SPIECKER, Indra *et al*. The Regulation of Commercial *Profiling* – A Comparative Analysis. **European Data Protection Law Review**, Berlim, p. 535-555, 2019.

eficácia de análises preditivas. Porém, o uso descuidado e sem observância de limites legais pode significar importantes efeitos prejudiciais à vida privada dos indivíduos.

Os autores anteriormente citados, como Clarke e Hildebrandt, destacam que as técnicas de *profiling* são uma importante fonte de conhecimento, cujo uso não pode ser descartado. O *profiling* feito com dados colhidos *online*, conforme exposto no tópico anterior, traz efeitos positivos para o mercado, que consegue oferecer com maior precisão seus produtos para aqueles realmente interessados. Os consumidores se beneficiam na medida em que podem encontrar mais facilmente aquilo que lhes interessa. O uso de *cookies* e outras tecnologias de rastreamento e interação com os usuários da rede possui benefícios no aprimoramento da experiência do usuário, cada vez mais personalizada. A definição de perfis para questões como a concessão de crédito pode ampliar o acesso para pessoas que não possuem alta renda, mas apresentam outras características que permitem instituições de crédito acreditar no adimplemento da dívida. Há também o argumento de que o *profiling* possibilita maior lucro aos anunciantes de forma a subsidiar conteúdos gratuitos na internet, que não seriam possíveis de se prover de outra forma, agindo, portanto, em benefício dos usuários. Seu uso contribui, ainda, no desenvolvimento e na entrada de novos produtos no mercado[95].

Os espaços chamados de "Ambientes Inteligentes"[96] vislumbram experiências continuamente centradas no usuário, adaptando-se em tempo real aos seus gostos e preferências a fim de atendê-lo da melhor forma possível. Jaquet-Chiffelle aponta que, além da melhor personalização de serviços, o *profiling* pode ser utilizado para identificar grupos vulneráveis de pessoas que recebem tratamento prejudicial do poder público ou de empresas. Assim, é possível seu uso responsável para expor e, consequentemente, reduzir desigualdades[97].

---

[95]FTC. **Online *profiling***: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-*profiling*-federal-tradecommissionreport-congress-june-2000/online*profiling*reportjune2000.pdf>. Acesso em: 31 out. 2019.

[96] Os "ambientes inteligentes" são espaços melhorados com sensores e aplicativos biométricos, conectados a uma base dados online e regidos por softwares que permitem o processo contínuo de *profiling* em tempo real. A inteligência nesses espaços não depende de um só dispositivo, mas de um conjunto de dispositivos interconectados. Assim o mundo on-line integra sua capacidade aparentemente ilimitada de coleta, agregação e armazenamento de dados comportamentais ao mundo offline, em uma mistura de realidade física e virtual. YANNOPOULOS, A.; ANDRONIKOU, V.; VARVARIGOU, T. Behavioral Biometric *Profiling* and Ambient Intelligence In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives.** Dordrecht: Springer Netherlands, 2008. cap. 5, p. 89-106.

[97] JAQUET-CHIFFELLE, David-Olivier. Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 34.

Apesar de seus benefícios, a elaboração perfis automatizados com base em dados recolhidos em massa apresenta riscos significativos de fragilização da esfera privada e de discriminação de grupos marginalizados. Em sua análise pioneira acerca do *profiling*, Clarke identificou usos negativos do *profiling* cuja relevância ainda se verifica nos dias de hoje. Esses usos negativos podem ser divididos em duas ordens[98]. Segundo o autor, existem os usos que seriam considerados inapropriados ou opressivos pela sociedade, se conhecidos e debatidos publicamente. É o caso de seu uso para fins de vigilância da população pelo setor público, visando identificar indivíduos ou grupos que representam alguma ameaça ao Estado, hipótese na qual o *profiling* não se difere de outras técnicas de vigilâncias que já eram debatidas à época, sendo problemático pois permite que cidadãos sejam oprimidos por aspectos de sua vida privada. Por outro lado, existem usos que, a princípio, são considerados aceitáveis pela sociedade, mas que podem ser realizados de maneira injusta, insensível ou discriminatória. Esses usos são difundidos principalmente no setor privado, sendo este o foco do presente trabalho. A título exemplificativo, o autor cita a seletividade de anúncios, que em certo ponto aumenta a eficiência do marketing, mas, caso extrapole certos limites, se torna plena manipulação de consumidores. Além disso, ao pré-julgar o comportamento futuro de consumidores e enviar publicidade direcionada, as empresas acabam por ignorar certos tipos de pessoas de modo a limitar seu acesso à informação acerca de produtos e serviços[99].

Nesse sentido, Stefano Rodotá aponta como o recurso a esses perfis pode ocasionar a discriminação de pessoas que não correspondem a um modelo geral, de forma a acentuar a estigmatização de comportamentos desviantes e a penalização de minorias, criando um obstáculo ao pleno desenvolvimento da personalidade individual, cerceada por perfis historicamente determinados[100]. Segundo Paul de Hert e Hans Lammerant o *profiling* é uma prática intrinsecamente intrusiva, ainda mais quando utilizado rotineiramente, nos mais variados contextos. O potencial presente nas técnicas de *profiling* encoraja a crescente coleta de dados comportamentais, a fim de se conhecer a fundo os hábitos das pessoas. Ainda que haja compartilhamento voluntário de dados por

---

[98] CLARKE, Roger. *Profiling*: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, Camberra, v. 4, p. 403-419, 1993.
[99] CLARKE, Roger. *Profiling*: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, Camberra, v. 4, p. 403-419, 1993.
[100] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.105.

partes dos indivíduos, há uma legítima expectativa de privacidade em relação ao uso de tais dados que a prática de *profiling* muitas vezes viola [101].

Hidelbrandt afirma que o uso mais comum do *profiling* no setor privado é o de *profiling* não distributivo, de forma que, como visto, os perfis são sempre probabilísticos. Os métodos de definição de perfis utilizam fatos passados para fazer uma previsão. Assim, empresas são capazes de tomar diversas decisões relativas a consumidores, como praticar discriminação de preços ou de ofertas, definir taxa de juros de um empréstimo ou estabelecer o valor do prêmio de um seguro. Essas decisões são baseadas em previsões bem informadas de comportamento futuro, fruto do procedimento de *profiling* feito com base em análise dados em massa. Hildebrandt chama esta abordagem feita em relação aos clientes de abordagem atuarial, porque se baseia em avaliações dos riscos e oportunidades envolvidos na prática comercial. O maior problema identificado pela autora nessa abordagem ocorre quando se extrapolam fatos passados consolidados na base de dados para o futuro com base em correlações cegas. Essa abordagem tende a ver o futuro como determinado por probabilidades estabelecidas, possivelmente incapacitando melhores soluções que estão no reino das baixas probabilidades. Jaquet-Chiffelle aponta que, nesse contexto, o uso do *profiling* se torna uma ferramenta que assume papel de controle social, de modo a contribuir para manutenção das pessoas em suas respectivas condições iniciais[102].

Assim, pessoas que reúnem algumas características que formam um perfil considerado de alta renda, terão bens e serviços oferecidos de forma a reforçar essa posição, o mesmo servindo para pessoas com perfil de baixa renda. De outro modo, com o *profiling* distributivo, ser membro de um grupo pode trazer problemas sociais e legais pois todos os membros são tratados como se possuíssem as mesmas características, sem maiores considerações acerca de cada indivíduo que compõe o grupo. Ainda que os perfis do grupo possuam diversas variáveis que visem capturar com exatidão todas as características de seus membros, toda a informação coletada é aplicada sem o contexto no qual foi produzida. Conforme explica Solove:

> Não obstante, a informação em bases de dados rotineiramente falha em capturar a textura de nossas vidas. Ao invés de prover um retrato sutil de nossas

[101] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. *In*: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

[102] JAQUET-CHIFFELLE, David-Olivier. Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 35.

> personalidades, compilações de dados capturam os fatos brutos do que fazemos sem as razões. Por exemplo, o registro de uma detenção sem a história ou razão por trás é enganoso. A detenção pode ter sido por causa de uma desobediência civil nos anos 1960 – mas ainda é registrada como detenção com uma denominação vaga, como 'conduta desordeira'[103].

Segundo Solove, é possível se observar um paradoxo em relação à ampla difusão do tratamento de dados pessoais. Ao mesmo tempo em que é possível se formar perfis que abrangem boa parte de nossas vidas, de forma a invadir a privacidade dos indivíduos, as limitações desses perfis também são problemáticas. Isso porque os perfis falham em capturar as pessoas em sua essência e por vezes distorcem quem elas são, mas ainda assim são usados para decidir aspectos relevantes de suas vidas.

Paul de Hert e Hans Lammerant associam três riscos às práticas de *profiling*. O primeiro diz respeito a seu impacto negativo na privacidade, o segundo se refere aos potenciais efeitos discriminatórios decorrentes da classificação social e o terceiro diz respeito à opacidade da tomada de decisões feita como resultado do procedimento de mineração de dados para formação de perfis[104].

Bart W. Schermer, por sua vez, ressalta que apesar de o *profiling* ser tratado na maioria das vezes como um problema de privacidade, seus riscos mais significantes estão associados à discriminação, "desindividualização" e assimetria de informações[105]. Quanto à desindividualização, o autor afirma que por meio do *profiling* as pessoas passam a ser julgadas com base em características de um grupo e não com base em suas próprias características e méritos. O problema da assimetria de informações ocorre, pois, o uso da mineração de dados no procedimento de *profiling*, por empresas e pelo governo, permite que as organizações conheçam a fundo certas características e comportamentos de indivíduos ou de grupos. Isso facilita, por exemplo, a tomada de decisões não desejáveis, antiéticas ou ilegais em relação a consumidores, como, por exemplo, a exclusão de oferta de bens e serviços devido a características étnicas. Além disso, as pessoas afetadas pela

---

[103] No original: "Nevertheless, the information in databases often fails to capture the texture of our lives. Rather than provide a nuanced portrait of our personalities, compilations of data capture the brute facts of what we do without the reasons. For example, a record of an arrest without the story or reason is misleading. The arrest could have been for civil disobedience in the 1960s—but it is still recorded as an arrest with some vague label, such as "disorderly conduct.". SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.49.

[104] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. *In*: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

[105] SCHERMER, Bart M. The limits of privacy in automated *profiling* and data mining. **Computer Law & Security Review**, Amsterdã, v. 27, p. 45-52, 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364910001767. Acesso em: 31 ago. 2019.

tomada de decisões resultante do *profiling* não são capazes de entender adequadamente as razões por trás da decisão tomada, nem quais características pessoais foram levadas em conta na formação de seu perfil.

Orla Linskey, em análise acerca dos potenciais danos causado pelo processamento de dados nos dias de hoje, classifica os riscos advindos do *profiling* como riscos que ocasionam danos intangíveis[106]. A autora argumenta que a fim de se beneficiar das vantagens potenciais do *profiling*, o perfil de um indivíduo deve ser preciso. Porém, é comum a ocorrência de diversas imprecisões na criação dos perfis. Por exemplo, se mais de um usuário utiliza o mesmo computador para acessar a internet, os hábitos de busca se misturam criando um perfil "misto". Os perfis inexatos podem acarretar desde pequenos inconvenientes, como constantes anúncios irrelevantes sendo exibidos para certa pessoa, até situações de constrangimento caso uma inferência errada seja feita com base no perfil.

Além disso, segundo a autora, os efeitos discriminatórios do *profiling* são um dos maiores riscos criados pelo processamento de dados. Tais efeitos podem surgir seja a definição de perfis exata ou não. A prática de *profiling* pode gerar tanto discriminação direta quanto indireta. A discriminação direta ocorre quando uma pessoa é tratada de maneira menos favorável que outra que se encontra numa mesma situação, por motivos étnicos, religiosos, de idade, de gênero ou alguma outra base que possua proteção legal. Nesse sentido, um empregador pode se utilizar de técnicas de *profiling* a fim de inferir qual a religião praticada pelos candidatos a uma vaga, eliminando os praticantes de certo culto considerado inadequado para a profissão, caso em que ocorre discriminação direta. A discriminação indireta ocorre quando uma medida, critério ou prática, conquanto aparentemente neutra, afete de maneira especialmente negativa certo grupo ou minoria protegida. Por exemplo, um algoritmo pode criar o perfil de pessoas bem-sucedidas na carreira de determinada empresa, com base em exemplos anteriores de sucesso dentro da mesma empresa, com o objetivo de determinar quais empregados atuais devem ser promovidos. Porém, se as promoções anteriores possuíam uma representatividade exacerbada de pessoas do sexo masculino, que dominaram o mercado daquela área por razões sociais e não necessariamente de mérito profissional, será reproduzido no

[106] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press. 2015, p.195.

algoritmo uma discriminação indireta contra mulheres, em razão do viés presente na base de dados utilizada[107].

Mesmo quando não se observe discriminação direta ou indireta advinda da construção de perfis, o ato de *profiling*, por sua própria natureza, promove a diferenciação entre indivíduos[108]. Ainda que a diferenciação por si só não seja imoral ou ilegal, pode trazer consequências indesejadas, principalmente quando o perfil refletir uma falsa imagem do indivíduo por ser, por exemplo, desatualizado. A diferenciação, ainda que baseada em perfis sem incorreções, pode também trazer efeitos indesejados. Orla Linskeyy usa como exemplo a facilitação de ofertas de preços diferenciados em produtos e serviços online, baseada nas informações pessoais coletadas sobre o usuário que pesquisa o produto.

Outro importante desafio identificado por Orla Linskeyy que emerge com a disseminação de práticas de *profiling* se refere aos efeitos inibitórios decorrentes da sensação de monitoramento que surge nos indivíduos quando percebem que seu perfil está sendo traçado. É comum que grandes empresas de comunicação argumentem que o *profiling* comportamental não viola a privacidade de usuários devido ao procedimento de anonimização dos dados pessoais, de forma que o perfil criado se refira a um número dentro do sistema e não a uma pessoa física individualizada. Além disso o processamento dos dados é feito por um sistema automatizado, não por seres humanos, sendo, portanto, incapaz de emitir julgamento ou opiniões sobre eventual informação íntima coletada. Ainda assim, o consumidor experimenta uma sensação de vigilância ao receber uma propaganda relacionada a algo que recentemente pesquisou, comentou em uma rede social ou a uma notícia que compartilhou.

Segundo Orla Linskey, a sensação de vigilância pode trazer os mesmos efeitos inibitórios e de controle do comportamento advindos de uma vigilância efetiva, de modo que o *profiling online* pode, ultimamente, desencorajar o exercício de liberdades civis garantidas numa sociedade democrática, como liberdade de expressão e de associação[109]. Esse risco foi também exposto pelo relatório da FTC, no qual estudiosos alertaram que o

---

[107] CALDERS, Toon; ŽLIOBAITĖ, Indrė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures. *In*: CUSTERS, Bart *et al*. **Discrimination and Privacy in the Information Society**: Data Mining and *Profiling* in Large Databases. Berlim: Springer, 2013. cap. 3.
[108] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press. 2015, p.198.
[109] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press. 2015, p.216.

profiling, quando percebido pelos usuários da internet, acaba por inibir efeitos benéficos que o relativo anonimato das redes propicia, como na busca de informações acerca de temas sensíveis, como por exemplo, relativos à sexualidade ou a questões de saúde[110].

Em conclusão, percebe-se o *profiling* apresenta benefícios relevantes de ordem econômica, de ganho de eficiência e pode ser extremamente útil no planejamento de políticas públicas. Porém, é possível se associar diversos riscos à prática. Percebe-se que o *profiling* representa uma fragilização na privacidade de indivíduos e potencializa práticas discriminatórias entre pessoas e grupos. Conforme resume Danilo Doneda:

> No *profiling*, estão em jogo não somente aspectos da privacidade do consumidor, porém da sua própria autonomia decisional e liberdade de escolha, valendo aqui um relance ao que Yves Poullet caracteriza como sendo as duas faces da privacidade moderna: de um lado, a proteção da intimidade e, de outro, a garantia da auto-determinação e da própria liberdade[111].

Com base nos riscos apresentados, identifica-se que a proteção da privacidade, de dados pessoais e a proibição da discriminação devem servir como as salvaguardas básicas para os problemas que emergem com o *profiling*. Basicamente, o que se observa é que os diferentes momentos do procedimento apresentam diferentes riscos. Ao iniciar o procedimento, toda a sistemática de coleta de dados pessoais necessária para se extrair valor, bem como as possíveis inferências e previsões obtidas ao final do procedimento são questões que afetam a privacidade dos indivíduos, que tem diversas informações expostas perante terceiros economicamente interessados em tais informações. Por sua vez, no momento de aplicação dos perfis formados, com a tomada de decisões que afetem significativamente a vida dos indivíduos, práticas discriminatórias podem emergir com o uso cego das previsões feitas. Além disso, os indivíduos não possuem o conhecimento e meios necessários para contestar ou se opor ao procedimento, conduzido de maneira burocrática, nos termos estudados no último capítulo.

A combinação dos riscos associados ao *profiling* forma, ultimamente, uma ameaça ao pleno desenvolvimento da personalidade. No próximo tópico, serão estudadas algumas realidades práticas de aplicação do *profiling* no setor privado, a fim de dar maior concretude ao tema. Cumpre destacar que o escopo da presente pesquisa se limitará ao *profiling* inserido em práticas do setor privado. O uso do *profiling* no setor público

---

[110] FTC. **Online *profiling***: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-*profiling*-federal-tradecommissionreport-congress-june-2000/online*profiling*reportjune2000.pdf>. Acesso em: 31 out. 2019.

[111] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.66.

envolve questões de interesse público que adicionam uma camada extra de complexidade ao tema, de forma que merece tratamento próprio em outras futuras pesquisas.

2.4 Aplicações

2.4.1 *Profiling* de consumidores

Uma das principais aplicações do *profiling* no setor privado é o seu uso para fins de publicidade direcionada. Coletar e agregar informações sobre consumidores, utilizando dados pessoais para enquadrá-los em determinados perfis, são os procedimentos que precedem a decisão de lhes direcionar determinado anúncio. Com a elaboração de perfis comportamentais, é possível o direcionamento de uma mensagem publicitária feita sob medida, que possui maior probabilidade de despertar o interesse do consumidor. Como o direcionamento é feito após a agregação de informações que refletem gostos e interesses do consumidor, denomina-se de publicidade comportamental a espécie de publicidade direcionada mais comum nos dias de hoje.

A publicidade de massas, voltada para venda de produtos ao grande público, remonta ao desenrolar da primeira revolução industrial. Até então, a publicidade possuía cunho informativo, de forma a expor as características essenciais de um produto. Com o crescimento dos meios de comunicação e mídia, a publicidade se torna o principal meio das grandes empresas expandirem seu mercado, sendo possível se atingir um número crescente de consumidores graças à difusão da imprensa, do rádio e, mais tarde, da televisão[112].

Na década de 1920 a ciência do *marketing* começa a se desenvolver. Com o passar do tempo, a publicidade muda seu foco dos bens comercializados para estilos de vidas desejáveis, associando ideias de liberdade, segurança, felicidade e sucesso à compra de produtos[113]. É no decorrer do século XX que se desenvolve o marketing direcionado. Os estudiosos da área constataram que a publicidade de massas consumia grande quantidade de recursos, mas somente uma fração das pessoas expostas aos anúncios era realmente impulsionada a consumir o produto em razão da publicidade vista[114]. Assim, a publicidade direcionada se desenvolveu, visando entender quais pessoas são mais

---

[112] MACHADO, Fernando Inglez de Sousa; LINDEN RUARO, Regina. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. **Conpedi Law Review**, Braga, v. 3, n. 2, p. 421-440, jul-dez. 2017.

[113] MACHADO, Fernando Inglez de Sousa; LINDEN RUARO, Regina. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. **Conpedi Law Review**, Braga, v. 3, n. 2, p. 421-440, jul-dez. 2017.

[114] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.16.

tendentes a consumir determinado produto para, então, focar os anúncios nelas, aumentado a eficácia da propaganda. Para isso, as empresas passam a identificar pessoas que consomem regularmente seus produtos e que fazem os maiores gastos. Assim, foi necessário aumentar os esforços do setor em pesquisas sobre consumidores e o desenvolvimento de maneiras efetivas de coletar, armazenar e analisar as informações disponíveis.

Uma vez identificados os consumidores mais lucrativos para empresas, que serão priorizados pelas ações de marketing, o perfil encontrado nesses consumidores é utilizado a fim encontrar outras pessoas similares. Isso envolve não somente ações para adquirir dados dos próprios consumidores daquela empresa, mas também dados demográficos relativos à população em geral.

Tem início, então, a coleta de dados em massa, possibilitada pelo desenvolvimento da computação. Para realizar a publicidade direcionada, as empresas buscaram compilar não somente informações sobre a visão dos consumidores acerca de determinado produto, mas também detalhes de seu estilo de vida e, eventualmente, passaram a elaborar perfis psicológicos completos[115]. A coleta de informações de natureza psicológica, como opiniões, atitudes, crenças e estilos de vida, para fins de se complementar a bases de dados sobre consumidores é acentuado nos Estados Unidos durante a década de 1980. Conforme expõe Solove, certas empresas elaboraram complexa taxonomia de pessoas, criando categorias de consumidores nomeados de "Sangue Nobre", "Shotguns e Pickups", "Misturas Hispânicas", dentre outras[116]. Cada grupo possuía uma descrição do tipo de pessoa que o compunha, seus gostos, rendimentos, raça, etnia, atitudes e *hobbies*.

Cada vez mais a mensagem publicitária passa a ter como destinatário um consumidor em específico, e não o público geral. A utilização de propaganda direcionada ganhou ainda mais força com o advento da internet, sendo o principal modelo de negócio utilizado por anunciantes no meio online. A efetividade da publicidade direcionada depende, principalmente, da quantidade de dados utilizada para formação de perfis mais precisos. Assim, a busca por uma coleta de dados cada vez maior se intensifica. Além disso, as empresas de publicidade não precisam praticar toda a coleta por si mesmas, podendo adquirir dados de outras fontes, de forma que as bases de dados passam a se

---

[115] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.22.
[116] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.19.

tornar verdadeiros ativos comercializados no mercado. Atividades que, por si só, permitem a coleta de enormes quantidades de dados comportamentais, como os serviços desenvolvidos pelo Facebook e pela Google, elevam essas empresas ao topo do mercado internacional.

Por meio das técnicas de rastreamento e monitoramento da atividade *online* as empresas de publicidade são capazes de individualizar o perfil de um consumidor e direcionar a ele apenas produtos compatíveis com seu gosto, por meio de mensagens adaptadas ao seu próprio estilo de comunicação, o que é chamado de *microtargeting*, ou microdirecionamento[117]. Não só o produto anunciado é compatível com os hábitos de consumo do indivíduo, mas também o meio onde o anúncio é exibido é cuidadosamente escolhido para que seja compatível com a expectativa do consumidor. Isso é a chamada publicidade contextual, que busca a inserção da mensagem publicitária em um ambiente no qual ela se harmonize com os interesses presumidos do consumidor[118].

A publicidade direcionada possui efeitos positivos para o mercado, que atinge com mais precisão seu público alvo, e para consumidores que podem encontrar mais facilmente aquilo que mais lhes interessa. Porém, a coleta de dados em massa para definição de perfis de consumidores traz diversos efeitos indesejados.

Segundo o relatório da FTC, estudiosos do tema argumentam que a publicidade direcionada pode ser considerada inerentemente injusta e enganosa. Eles afirmam ser uma prática manipuladora que foca em fraquezas dos consumidores para criar demandas de consumo que de outra forma não existiriam, de forma a minar a autonomia dos consumidores[119].

Conforme exposto por Danilo Doneda[120], a Internet possibilitou, por um lado, meios para que o consumidor adquira informações sobre produtos, serviços e fornecedores, o que proporciona uma melhora frente ao paradigma anterior no qual a

---

[117] KREISS, Daniel. Micro-targeting, the quantified persuasion. **Internet Policy Review - Journal on internet regulation**, School of Media and Journalism - University of North Carolina, United States of America, Volume 6, número 4, dezembro/2017, pp 1-2. Disponível em: < https://policyreview.info/articles/analysis/micro-targeting-quantified-persuasion >. Acesso em 31 de ago. 2019.

[118] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.60.

[119] FTC. **Online *profiling***: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-*profiling*-federal-tradecommissionreport-congress-june-2000/online*profiling*reportjune2000.pdf>. Acesso em: 31 out. 2019.

[120] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.61.

informação era restrita ao contato direto, com poucas formas de comunicação. Por outro lado, o fluxo de informações em sentido inverso, que o fornecedor consegue obter acerca do consumidor, aumentou ainda mais. Houve mudança não somente quantitativa, mas também na forma atual de obtenção de dados, que permite individualização do consumidor e de sua experiência.

Doneda aponta que os dados obtidos de consumidores, em grande parte, não são resultado da manifestação de sua expressão consentida, como ocorre quando alguém se disponibiliza a responder questionários ou a participar de um programa de fidelização de clientes. Com a internet, dados pessoais são obtidos pela mera navegação e em situações pré-contratuais, pelo mero observar de determinado produto no site do fornecedor. Segundo Doneda, a assimetria entre consumidores e fornecedores é acentuada pelo uso do *profiling* para fins de publicidade comportamental: "Estas informações comportamentais não são ponderadas e refletidas pelo consumidor - como o é a mensagem publicitária pelo fornecedor - e, mais ainda, sua disponibilização é hoje apenas precariamente controlada pelo próprio consumidor."[121]. Assim, uma imagem do consumidor é construída a partir dos seus dados pessoais, sem que esse saiba efetivamente o que essa imagem está refletindo, se informações sensíveis acerca de sua vida são inferidas, como a imagem foi construída e quais as suas consequências.

Outro problema decorrente do *profiling* para fins de publicidade surge quando, a fim de se ajustar a publicidade ao perfil comportamental do consumidor, estes podem ter seu rol de escolha e acesso a mercadorias limitados por aquilo que as empresas consideram que seja seu gosto[122]. Esse fenômeno, usualmente referido como *boxing*, pode ser assim descrito:

> A utilização de dados comportamentais como forma de influenciar a interação futura de uma pessoa - por exemplo, cuidando para que lhe seja veiculada apenas a publicidade que mais se ajuste ao seu pretenso perfil comportamental - pode limitar o rol de escolhas futuras daquela pessoa a partir de um perfil que foi inferido de seu comportamento passado. Este fenômeno já chegou a ser denominado de *boxing*, segundo a metáfora de que as possibilidades oferecidas a uma pessoa são fechadas - encaixotadas - em torno de presunções realizadas por ferramentas de análise comportamental, guiando desta forma as suas escolhas futuras.[123]

---

[121] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil, Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.62.

[122] MACHADO, Fernando Inglez de Sousa; LINDEN RUARO, Regina. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. **Conpedi Law Review** , Braga, v. 3, n. 2, p. 421-440, jul-dez. 2017.

[123] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010, p.68.

Nesse sentido, perfis de consumo extraídos de dados comportamentais podem, ainda, promover uma discriminação indireta, por se basearem em estereótipos discriminatórios historicamente determinados. Por exemplo, pesquisas relativas aos anúncios exibidos no Facebook sugerem existir uma reprodução de estereótipos de gênero e raça, principalmente na exibição de anúncios para moradia e empregos[124].

Aos poucos, vieses como os identificados na exibição de anúncios pelo Facebook, permitem uma forma de exclusão de consumidores considerados indesejados. Como alerta David Lyon em diálogo com Zygmunt Bauman, existe um processo de filtragem e seleção do perfil adequado de consumidores, que cria um paradigma de 'ban-óptico'[125] no mercado de consumo. Assim afirma:

> Se as pessoas 'não conhecem ou não se importam' com a elaboração on-line de perfis de consumidores, não é preciso ter muita imaginação para inferir que têm menos conhecimento ainda sobre o ban-óptico do consumidor, com seu "demarketing" de consumidores falhos. Para não mencionar os outros ban-ópticos à espreita no espaço urbano, como os que privam as populações proscritas de serviços essenciais com base em seus perfis pessoais, ou os que valorizam alguns distritos da cidade enquanto demonizam outros[126].

Solove traz exemplo concreto desse fenômeno, indicando que informações pessoais começam a ser usadas para identificar o que as empresas chamam de consumidores "anjos" e "demônios"[127]. Os consumidores anjos são os que trazem maior lucro, consumindo com frequência e em grandes quantidades sem trazer demandas individuais aos fornecedores. Os consumidores demônios são os que, apesar de comprarem o produto, acabam por consumir recursos da empresa de outras formas como, por exemplo, ligando para o serviço de atendimento ou solicitando trocas constantemente.

---

[124] PAUL, Katie; RANA, Akanksha. U.S. charges Facebook with racial discrimination in targeted housing ads. **Reuters**, Londres, p. 1, 19 mar. 2019. Disponível em: https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8. Acesso em: 3 set. 2019.

[125] O "ban-óptico" é uma variação, feita pelo sociólogo Zygmunt Bauman, do "pan-óptico" imaginado por Jeremy Bentham como uma estrutura de vigilância ideal, em que um único vigilante é capaz de observar todos os prisioneiros, sem que estes possam saber se estão ou não sendo vigiados. A ideia do "pan-óptico" foi desenvolvida, posteriormente, por Michael Foucault, como uma estrutura de controle social baseada na vigilância e na punição da população marginalizada. O "ban-óptico", por sua vez, é um mecanismo de categorização sistemática da população, de forma a dividi-la entre cidadãos desejados e indesejados, limitando as possibilidades de socialização destes últimos. LEOPOLDO, Rafael. Vigilância Líquida: Variações Sobre O Panoptismo. **Sapere Aude**, Belo Horizonte, v. 6, n. 12, p. 894-902, 2015. Disponível em: http://periodicos.pucminas.br/index.php/SapereAude/article/viewFile/11261/9115. Acesso em: 3 set. 2019.

[126] BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.p.114.

[127] SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: New York University Press, 2004. p.50.

Assim, especialistas recomendam que as empresas usem informações pessoais para identificar esses tipos de consumidores a fim de tratá-los de maneira diferente.

Desse modo as empresas, além de utilizar a definição de perfis para direcionar seus esforços de marketing, utilizam o *profiling* também para potencializar seus ganhos, seja pelo desenvolvimento de novos produtos que atraiam novos clientes, seja pela exploração do potencial da clientela já existente. Isso pode resultar em tratamentos diferenciados nitidamente injustos entre consumidores. O uso de dados comportamentais facilita, por exemplo, a prática de preços adaptáveis, direcionando ofertas menos vantajosas a consumidores que possuem em seu perfil características que indiquem uma inclinação a pagar maiores valores. O uso de características individuais dos consumidores para conferir a eles tratamentos diferenciados pode configurar uma prática de discriminação direta ou indireta.

2.4.2 *Profiling* para avaliação de riscos: *credit scoring* e securitização

Como visto, uma das principais utilidades do *profiling* está na avaliação de riscos, a partir da construção de previsões sobre comportamento futuro de indivíduos. Uma aplicação bastante comum no setor privado está na criação de perfis para formação do *credit scoring*. Esse é um procedimento que, a partir da consideração de dados de um indivíduo e análises estatísticas, atribui a ele um certo valor que reflete sua probabilidade de adimplemento ou inadimplemento de uma dívida a ser contraída[128]. O cálculo feito parte da consideração de certas características pessoais as quais se atribui um indicativo de solvibilidade (*input*) e assim se chega em um resultado dentro de uma escala de credibilidade (*output*). Os critérios indicativos de solvibilidade utilizados e sua importância relativa são compiladas em um modelo estatístico denominado "*scorecard*".

A pontuação de crédito individual é calculada pelo cruzamento do *scorecard* com informações específicas do possível mutuário. Com o advento do *Big Data* e de técnicas de *data mining*, esse processo passa a levar em conta dados que, a priori, não possuem relação com capacidade econômica de adimplemento de uma pessoa, com objetivo de aprimorar a efetividade da previsão feita. Além disso, é possível que se façam inferências invasivas a respeito dos hábitos daqueles que buscam crédito no mercado[129].

---

[128] ANDRADE, Daniel de Pádua. *Credit scoring* na era do big data: desafios tecnológicos no direito brasileiro. In: PARENTONI, L.; GONTIJO, B. M.; LIMA, H.C.S. **Direito, Tecnologia e Inovação**. Belo Horizonte: D'Placido, 2018. cap. 2.3, p. 246-267.

[129] O uso de informações invasivas para fins de análise de crédito era identificado nos Estados Unidos há muitos anos, quando audiências no Congresso americano na década de 70 revelaram que *bureaus* de crédito tratavam dados relativos a hábitos sexuais, opiniões políticas, vida matrimonial, dentre outros. Com o

Sob o ponto de vista técnico, *credit scoring* é, em regra, uma forma de *profiling* de grupos do tipo não-distributivo[130]. Isso significa que é identificado um grupo no qual nem todos os membros compartilham a totalidade dos atributos que compõem o perfil geral, mas há uma espécie de *checklist* (no caso de *credit scoring*, é chamada de *scorecard*) pontuada para que o perfil pessoal seja estabelecido[131].

O procedimento de *credit scoring* pode ser feito por uma empresa especializada em análise e proteção ao crédito. No Brasil, a Serasa Experian serve como o melhor exemplo ilustrativo. As instituições financeiras que irão conceder o crédito também podem desenvolver seus próprios modelos e formas de processamento. O mais comum, porém, é que os bancos e outras instituições financeiras concedentes incorporem, em seu modelo particular, a pontuação obtida em uma agência externa como um dos parâmetros para atribuir sua pontuação específica. A pontuação pode influir na decisão de concessão de crédito de variadas formas, desde a aceitação ou não do mutuário, até as condições de contratação, como limites do crédito, taxa de juros e prazos.

Uma das particularidades de sistemas de *credit scoring* é a existência de um critério "K.O" (*knock over*). Isso se refere a certo critério que, se atingido irá, invariavelmente, desqualificar o aplicante à concessão de crédito. A idade pode ter essa característica, excluindo menores do mercado e destinando certas concessões a pessoas com mais maturidade financeira. Desemprego ou prévio inadimplemento também são critérios "K.O" comumente utilizados. Além disso, usualmente para uma operação de crédito é estabelecido um "*Cut-Off-Score*", que se refere à pontuação mínima de crédito que o aplicante deve atingir para que possa ser considerado apto a adimplir a obrigação.

Critérios comuns encontrados nos sistemas de *credit scoring* são relativos aos parâmetros contratuais (número de contas junto a instituição, seus saldos e números de cartões de crédito, garantias, duração da relação entre o banco e seu cliente, dentre

---

advento da internet e do *Big Data*, informações dessa natureza estão disponíveis mais facilmente e inferências invasivas acerca de comportamentos pessoais podem ser feitas pelo tratamento de grandes quantidades de dados, ainda que não possuam relação direta com tais comportamentos. GARFINKEL, Simson. **Database nation: the death of privacy in the 21st century**. Boston: O'Reilly Media, 2010.

[130] KAMP, Meike; KORFFER, Barbara; MEINTS, Martin. *Profiling* of Customers and Consumers - Customer Loyalty Programmes and Scoring Practices. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Netherlands: Springer, 2008, p. 201-215.

[131] KAMP, Meike; KORFFER, Barbara; MEINTS, Martin. *Profiling* of Customers and Consumers - Customer Loyalty Programmes and Scoring Practices. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Netherlands: Springer, 2008, p. 201-215.

outros). São também avaliados critérios financeiros como renda, patrimônio, inadimplementos passados etc. Com o advento do *Big Data*, características demográficas são mais facilmente coletadas e passam a ter peso mais significativo. São critérios demográficos empregados comumente o endereço, idade, profissão, escolaridade e estado civil, porém outros critérios mais específicos, como a marca de carro que o aplicante possui e outros hábitos de consumo podem ser levados em conta[132].

A análise de crédito tomada com base na definição de perfis é, sem dúvidas, uma maneira extremamente útil de se garantir às instituições financeiras maior segurança na concessão de crédito, aumentando da mesma forma o potencial de acesso a crédito pela população. Porém, observa-se que a utilização de dados pessoais de forma irrestrita e desgovernada é capaz de desvirtuar a natureza da análise feita de modo a se gerar resultados discriminatórios. Esse desvirtuamento é ilustrado pelo caso ocorrido em Atlanta, onde Kevin D. Johnson, cidadão norte-americano negro, sofreu uma drástica restrição ao seu crédito, apesar de seu histórico de adimplemento pontual de todas as suas contas. A razão dada pela operadora do cartão para a redução de seu limite foi o histórico de outros consumidores que costumavam utilizar cartão de crédito nos mesmos estabelecimentos que ele. A história de Kevin Johnson levantou a possibilidade problemática de consumidores serem penalizados por atividades associadas a uma raça, etnia ou classe socioeconômica em particular[133].

Na década de 70, problemas relativos à discriminação no acesso ao crédito já eram identificados nos Estados Unidos, sendo observado uma discrepância na concessão de financiamentos imobiliários entre pessoas de diferentes raças, mas em condições econômicas semelhantes, em fenômeno descrito como *redlining.* Nos últimos anos, surgiu, ainda, o que autores chamam de *redlining* reverso, que consiste na ampliação de acesso ao crédito em condições predatória, visando principalmente populações marginalizadas e causando grande endividamento[134], tornando o problema de acesso ao crédito por minorias em uma questão de acesso ao crédito de boa qualidade[135].

---

[132] HURLEY, Mikella;ADEBAYO,Julius. *Credit scoring* in the age of big data. **The Yale Journal of Law & Technology, v. 18, p.148-216,2016.** Disponível em <https://yjolt.org/credit-scoring-era-big-data>. Acesso em: 09 nov. 2018.

[133] HURLEY, Mikella; ADEBAYO,Julius. *Credit scoring* in the age of big data. **The Yale Journal of Law & Technology, v. 18, p.148-216,2016.** Disponível em <https://yjolt.org/credit-scoring-era-big-data>. Acesso em: 09 nov. 2018.

[134] HAVARD, Cassandra Jones. On the Take: The Black Box of Credit Scoring and Mortgage Discrimination. **Boston University Public Interest Law Journal**, Boston, v. 20, n. 24, p. 241-286, 2011.

[135] HAVARD, Cassandra Jones. On the Take: The Black Box of Credit Scoring and Mortgage Discrimination. **Boston University Public Interest Law Journal**, Boston, v. 20, n. 24, p. 241-286, 2011.

A disseminação do *profiling* automatizado em instituições de crédito traz novamente à tona as preocupações quanto ao uso de critérios invasivos e a ocorrência de discriminação ao acesso ao crédito. Isso porque os modelos de pontuação de crédito levam em conta uma infinidade de dados pessoais cujo cruzamento acaba por refletir características sensíveis, como questões étnicas, que, a princípio, não podem ser levadas em conta nesse tipo de análise. Sistemas de pontuação baseados em perfis podem também representar padrões de discriminação semelhantes ao *redlining*. Além disso, a complexidade dos algoritmos utilizados impede que as razões primordiais que levam à construção da pontuação sejam devidamente acessadas, formando-se uma verdadeira caixa-preta dos modelos de *credit scoring*[136].

Além de seu uso amplamente difundido no setor de análise de crédito, o setor de seguros também se beneficia fortemente da capacidade de se extrair previsões acerca de hábitos pessoais. As mesmas preocupações que surgem com a criação de perfis para avaliação de risco na concessão ao crédito se reproduzem nesse setor. As técnicas de *profiling* podem determinar tanto a decisão de se celebrar o contrato quanto influir nos valores envolvidos na contratação. A grande quantidade de dados pessoais disponíveis para análise nos dias de hoje permite que as seguradoras, que antes encaixavam clientes dentro de categorias amplas da população para avaliar o risco envolvido na contratação, possam realizar análises individualizadas com o objetivo de obter maior precisão e margem de lucro nos contratos celebrados. Enquanto, a princípio, esse tipo de análise promete os benefícios de personalização, livrando as pessoas das generalizações presentes nas categorias amplas, O'Neil[137] alerta quea análise não é realmente individualizada, mas que os modelos colocam clientes em categorias (extraídas da base de dados), cujo comportamento se assemelha ao do indivíduo perfilado. Independentemente da qualidade da análise feita, a opacidade do procedimento, que ocorre de maneira burocrática, nos termos do exposto no capítulo anterior, apresenta diversas dificuldades para se avaliar a justiça da avaliação feita.

Além disso a coleta de dados para os fins expostos se torna cada vez mais invasiva. A área dos planos de saúde é especialmente sensível, pois muito se beneficia do tratamento da obtenção de dados que incluam características genéticas, padrões de sono,

---

[136] PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.22.
[137] O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality And Threatens Democracy. Nova York: Crown, 2016, p.97.

exercício, dieta, dentre outras[138]. Na securitização de veículos, dados de geolocalização e outros dados biométricos coletados durante a direção, por meio de smartphones começam a ser utilizados por seguradoras e locadoras de automóveis[139]. Além disso, pesquisas realizadas nos Estados Unidos sugerem que práticas de *profiling* no setor de seguros de moradia utilizam critérios raciais, ainda que indiretamente, o que vem contribuindo para uma maior segregação racial e desenvolvimento desigual do espaço urbano[140].

2.4.3 *Profiling* nas relações de emprego

O *profiling* vem ocupando papel relevante nas políticas de manutenção de pessoal em empresas do setor privado. A coleta de dados pessoais de empregados, atuais ou futuros, relativos às suas características, habilidades, competências e conhecimentos se tornou um lucrativo modelo de negócios denominado E-HRM (*Electronic Human Resources Management*)[141]. Empresas de recursos humanos desenvolvem softwares para prever quantitativos ideais de pessoal para execução de determinada tarefa e avaliar a combinação de habilidades e competências de determinada equipe. Tais ferramentas visam monitorar e avaliar os riscos associados a estratégias específicas de pessoal e promovem a coleta, análise e categorização do desempenho e da frequência de trabalho dos empregados de uma empresa, visando ganhos de eficiência. O perfilamento dos empregados que integram o quadro da empresa traz novas questões sensíveis acerca da já relativizada privacidade dos empregados frente ao poder de monitoramento dos empregadores.

Técnicas de análise de dados tornam-se extremamente úteis, ainda, na medida em que anúncios de vagas de emprego são veiculados no meio online. Isso gera, consequentemente, um enorme número de aplicantes à vaga oferecida. Empresas do setor privado utilizam-se do *profiling* automatizado a fim de selecionar de maneira mais eficiente os currículos mais adequados à vaga.

---

[138] O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality And Threatens Democracy. Nova York: Crown, 2016, p.98.

[139] CASTIGNANI, G. *et al*. Driver Behavior *Profiling* Using Smartphones: A Low-Cost Platform for Driver Monitoring. **IEEE Intelligent Transportation Systems Magazine**, Estados Unidos, v. 7, n. 1, p. 91-102, 2015. Disponível em: https://ieeexplore.ieee.org/document/7014406. Acesso em: 3 set. 2019.

[140] SQUIRES, Gregory D. Racial *Profiling*, Insurance Style: Insurance Redlining and the Uneven Development of Metropolitan Areas. **Journal of Urban Affairs**, Milwaukee, v. 24, n. 4, p. 391-410, 2003. Disponível em: https://www.tandfonline.com/doi/abs/10.1111/1467-9906.t01-1-00168. Acesso em: 3 set. 2019.

[141] BALL, Kirstie. Categorizing the workers: Electronic surveillance and social ordering in the call center. *In*: LYON, David (ed.). **Surveillance as Social Sorting**: Privacy, risk and digital discrimination. Londres: Routledge, 2003. cap. 10.

O procedimento de contratação por empresas sempre foi marcado por alto grau de subjetividade. Empresas de recursos humanos buscam, por meio de técnicas de definição de perfis, tornar o procedimento de seleção mais justo, objetivo e capaz de trazer maiores benefícios para o empregador. Porém, a triagem inicial de currículos pode possuir, muitas vezes, critérios obscuros ou de legitimidade duvidosa. Conforme aponta Pasquale, existem empresas que avaliam a atividade dos candidatos nas redes sociais para identificar características de criatividade, liderança e temperamento, excluindo do processo tanto pessoas que exibem opiniões de maneira ostensiva quanto pessoas que se abstêm do uso das plataformas de comunicação mais populares[142]. Isso gera uma verdadeira demanda de aconselhamento para pessoas que buscam emprego, de como devem se portar em redes sociais e plataformas semelhantes.

Além disso, O'Neil relata a existência de pesquisas que demonstraram a tendência de triagens automatizadas de currículos eliminarem em maior proporção candidatos com nomes associados a raça negra ou nomes estrangeiros, em comparação com candidatos de mesma qualificação, mas com nomes comuns na população branca[143]. Ainda, a título ilustrativo, a publicação inglesa Reuters publicou em 2018 matéria indicando que um algoritmo de seleção de funcionários utilizado pela Amazon foi descontinuado pela empresa, na medida em que foi identificado que o sistema estava selecionando homens em quantidade desproporcional em relação às mulheres[144]. Segundo a publicação, os algoritmos eram treinados a examinar aplicantes à vaga em busca de padrões observados em currículos submetidos à empresa nos últimos 10 anos, sendo a maior parte dos currículos de candidatos homens, que dominavam a indústria da tecnologia. Apesar de não ser uma história confirmada por representantes oficiais da empresa, a possibilidade de reprodução de preconceitos em sistemas de *profiling* alimentados por bases de dados enviesadas é uma preocupação real de especialistas da área. Conforme resume Pasquale:

> Afirma-se que sistemas automatizados avaliam todos os indivíduos da mesma forma, assim evitando a discriminação. Eles podem garantir que alguns chefes não mais baseiem suas decisões de contratar ou demitir em intuições, impressões ou preconceitos. Mas engenheiros de software constroem a base de dados minerada pelos sistemas de pontuação; eles definem os parâmetros da

[142] PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.34.
[143] O'NEIL, Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. Nova York: Crown, 2016, p.70.
[144]DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. **Reuters**, Londres, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 31 ago. 2019.

> análise por mineração de dados; eles criam os agrupamentos, conexões e árvores de decisões aplicadas, eles geram os modelos preditivos aplicados. Vieses e valores humanos são embutidos em cada passo do desenvolvimento. A computação pode simplesmente aumentar a discriminação[145].

Procedimentos de *profiling* também podem ser utilizados por empregadores após a contratação. A coleta de dados dos empregados é facilitada pela relação de subordinação que abre espaço para maior monitoramento das atividades dos funcionários de uma empresa. Nesse âmbito, o *profiling* pode ser utilizado para definir promoções e indicações para cargos de chefia. Os resultados do trabalho realizado pelo empregado não necessariamente definem sua posição na empresa, na medida em que e-mails corporativos e o monitoramento da atividade de navegação na internet durante o horário de trabalho são possíveis fontes de dados para análise, a fim de se extrair informações sobre produtividade, relação interpessoal e comportamento em geral[146].

O monitoramento da atividade dos empregados, com a definição de perfis comportamentais, é utilizado ainda para garantir a segurança das informações da empresa e possibilitar a identificação de responsáveis em possíveis casos de fraude[147]. Nesse contexto, também se verificam os riscos que comumente são associados à prática de *profiling*. Na medida em que toda informação sobre o comportamento do empregado pode ser utilizada para ganho de eficiência na empresa, cresce a tensão entre a privacidade do empregado frente ao poder de monitoramento do empregador. O uso de dados passados da empresa para tomada de decisão quanto a promoções futuras pode representar a reprodução de padrões discriminatórios, conforme indica Calders:

> Nos dias de hoje mais e mais decisões em empréstimos, recrutamento, bolsas ou aplicações para estudos vêm sendo parcialmente automatizadas baseando-se em modelos treinados sob uma base de dados histórica. Essa base de dados histórica pode ser discriminatória; por exemplo, discriminação racial ou de gênero pode ter afetado a seleção de candidatos à vaga de emprego na base de dados histórica. Nesses casos, classificadores treinados com dados discriminatórios provavelmente aprenderão a relação discriminatória e, como

---

[145] No original: "Automated systems claim to rate all individuals the same way, thus averting discrimination. They may ensure some bosses no longer base hiring and firing decisions on hunches, impressions, or prejudices.94 But software engineers construct the datasets mined by scoring systems; they define the parameters of data- mining analyses; they create the clusters, links, and decision trees applied; they generate the predictive models applied. Human biases and values are embedded into each and every step of development. Computerization may simply drive discrimination upstream." PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.35.

[146] BALL, Kirstie. Categorizing the workers: Electronic surveillance and social ordering in the call center Kirstie Ball. *In*: LYON, David (ed.). **Surveillance as Social Sorting**: Privacy, risk and digital discrimination. Londres: Routledge, 2003. cap. 10.

[147] LEOPOLD, N.; MEINTS, M. *Profiling* in Employment Situations (Fraud**)** In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 12, p. 235.

> resultado, eles farão previsões discriminatórias quando aplicado a novos dados no futuro[148].

Além disso, o uso de algoritmos de mineração de dados na construção de perfis de empregados dificulta qualquer capacidade de oposição ou controle do empregado frente as decisões tomadas com base em seu perfil construído, aumentando a assimetria entre as partes[149].

Vistos os principais conceitos, técnicas, benefícios, riscos e aplicações do *profiling* no setor privado, passa-se à análise jurídica acerca de quais devem ser os limites legais de seu uso, a fim de se amenizar os efeitos negativos que a definição automatizada de perfis pode ocasionar no desenvolvimento da esfera privada dos indivíduos. No próximo capítulo será estudado como o Direito atual lida com questões recentes relativas à privacidade, à proteção de dados pessoais e ao princípio da não discriminação, e como esses temas devem ser abordados no intuito de se criar salvaguardas legais efetivas para práticas de *profiling*.

---

[148]No original: "Nowadays more and more decisions in lending, recruitment, grant or study applications are partially being automated based on models trained on historical data. That historical data may be discriminatory1; for instance, racial or gender discrimination may have affected the selection of job candidates in the historical data. In such a case classifiers trained on this discriminatory data are likely to learn the discriminatory relation, and, as a result, they will make discriminatory predictions when applied to new data in the future." CALDERS, Toon; ŽLIOBAITĖ, Indrė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures. *In*: CUSTERS, Bart *et al*. **Discrimination and Privacy in the Information Society**: Data Mining and *Profiling* in Large Databases. Berlim: Springer, 2013. cap. 3, p. 155.

[149] BALL, Kirstie. Categorizing the workers: Electronic surveillance and social ordering in the call center Kirstie Ball. *In*: LYON, David (ed.). **Surveillance as Social Sorting**: Privacy, risk and digital discrimination. Londres: Routledge, 2003. cap. 10.

3. OS LIMITES LEGAIS DO *PROFILING*

3.1 Direito à privacidade e a proteção de dados pessoais

Conforme estudado, um dos principais problemas que emergem da prática de *profiling* é seu impacto na privacidade dos cidadãos. Nesse momento, portanto, se faz necessária a adequada compreensão do conceito de privacidade e de sua relação com a dinâmica de proteção de dados pessoais, para que possam ser estabelecidos limites legais ao *profiling* capazes de garantir a devida proteção da esfera privada dos indivíduos.

Muitos apontam que a ideia de vida privada é uma concepção que surge apenas na modernidade pós-industrial. Porém, conforme demonstra Alan Westin, certa noção de privacidade está presente mesmo em comunidades humanas primitivas, sendo uma necessidade inerente à espécie[150]. Segundo o autor, estudos biológicos apontam que quase todos os animais buscam períodos de reclusão individual ou de intimidade em pequenos grupos e apresentam verdadeira necessidade orgânica de espaço privado para sobrevivência[151]. Em sua obra, Westin também destaca como a privacidade é uma ideia dinâmica, na medida em que os indivíduos vivem num constante processo pessoal de equilíbrio entre a necessidade de espaço privado e o desejo de exposição e comunicação com seus pares.

Contudo, pode-se afirmar que o desenvolvimento conceitual do direito à privacidade remonta, realmente, ao início do século XX. O artigo publicado pelos advogados americanos Warren e Brandeis, "The Right to Privacy"[152] é apontado como principal marco do surgimento de elaboração teórica sobre esse direito. No referido texto os autores defenderam a existência de um direito à privacidade o qual conceituaram como "right to be let alone", o direito de ser deixado a só. Uma das principais contribuições do referido artigo foi atrelar a privacidade ao desenvolvimento da personalidade individual, uma vez que, anteriormente, a discussão da vida privada no meio jurídico se limitava a

---

[150] WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967, p.8.

[151] O autor faz referência a um estudo realizado com uma população de cervos isolada em uma ilha. O ambiente da ilha proporcionava aos cervos todas as condições de alimentação necessárias para sua reprodução, de modo que a população aumentou rapidamente. Em certo ponto a ilha ficou repleta pelos animais, que pararam de se reproduzir e a morrer gradualmente, apesar de haver plenitude de alimentos e água para todos e não ser encontrada nenhum tipo de infecção na população. O estudo concluiu que a morte de cerca de dois terços da população se deu devido a um estresse metabólico causado pela superpopulação presente em espaço restrito que não propiciava aos animais o devido afastamento entre uns e outros. WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967, p. 10.

[152] WARREN, Samuel D, BRANDEIS, Louis D, The Right to Privacy, **Harvard Law Review**, vol.4, p. 193-220, 1890.

aspectos de proteção da propriedade[153]. À época, os autores defenderam a existência desse direito como forma de salvaguarda dos indivíduos frente a uma tecnologia considerada intrusiva: câmeras fotográficas se tornaram portáteis, facilitando a publicação em veículos de mídia de fotos comprometedoras, o que afetava, em grande parte, a vida íntima de pessoas públicas.

No Brasil, durante muitos anos a perspectiva do direito à privacidade como direito de ser deixado a só prevaleceu na doutrina civilista[154]. Até hoje, elementos da obra de Warren e Brandeis são adotados por autores brasileiros ao tratarem do direito à privacidade dentre os direitos da personalidade tutelados pelo sistema jurídico[155].

Porém, o conceito do direito à privacidade foi intensamente debatido ao longo dos anos e se desenvolveu em diversas diferentes vertentes, se tornando, hoje, muito mais amplo do que o originalmente defendido pelos advogados americanos. Além da ideia da privacidade como o direito a ser deixado só, conforme a ideia original de Warren e Brandeis, surgem outras noções, como, por exemplo, a de privacidade como resguardo frente a interferências alheias, privacidade como sigilo, como forma de proteção ao segredo, e teorias que apontam existirem diversas camadas de vida privada que merecem diferentes graus de proteções[156]. No entanto, conforme aponta Rodotà[157], todas essas conceituações estão voltadas para a dimensão individual e negativa da privacidade, ou seja, visam determinar que tipo de informação o sujeito pode resguardar do conhecimento alheio. Isso, apesar de constituir um aspecto importante da privacidade, não mais se adequa aos constantes desafios enfrentados na proteção da esfera privada que surgem com o desenvolvimento de novas tecnologias.

Diante do cenário em que os indivíduos se veem obrigados a entregar uma grande quantidade de informações pessoais em troca de serviços fornecidos pelos grandes

---

153 CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, ed. 76, p. 213-240, ago. 2017.

154 Pontes de Miranda trata da privacidade em suas considerações quanto ao "direito a velar a intimidade", afirmando ser este o direito de manter-se em reserva, de velar a sua intimidade, de não deixar que se lhes devasse a vida privada, de fechar o seu lar à curiosidade pública, em conformidade com a concepção clássica do "right to be let alone". Porém, o autor ainda destaca uma dimensão da privacidade que coloca a liberdade como base, afirmando que só há o direito de se resguardar a esfera privada, pois há a liberdade para exteriorizá-la, conforme a vontade individual, assim se aproximando de noções contemporâneas da privacidade. MIRANDA, Pontes de. **Tratado de Direito Privado** - parte especial, tomo VII, 3a Ed. Rio de Janeiro: Borsoi,1971 p. 124-125.

155 JÚNIOR, P.J.C. **O direito de estar só: tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007.

156 LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo:Saraiva. 2011 p.52-77.

157 RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.92.

agentes públicos e privados, surge uma situação em que o indivíduo não possui mais nenhum controle sobre o que as entidades sabem sobre ele e como suas informações pessoais estão sendo utilizadas. Isso ocorre de forma sistemática desde os primeiros desenvolvimentos das tecnologias de computação, mas adquire maior relevância com o advento da Internet. Lawrence Lessig compara os problemas relativos à privacidade nos dias de hoje com o que ocorreu com os direitos autorais, demonstrando que ambos sofreram determinante perda de controle em decorrência do surgimento da rede de computadores, sendo necessário um novo balanço entre lei e tecnologia para restaurar o nível próprio de controle, de modo a balancear interesses públicos e privados:

> Em ambos os casos, a Internet produziu essa perda de controle: com o copyright, porque a tecnologia possibilita perfeitas e gratuitas cópias de conteúdo; com a privacidade (...) porque a tecnologia possibilita barato e perpétuo monitoramento de comportamento. Em ambos os casos, a questão que os responsáveis por políticas devem se fazer é qual a mistura de lei e tecnologia pode restaurar o nível adequado de controle[158].

As novas perspectivas acerca do direito à privacidade passam a ser discutidas no Brasil no início dos anos 2000. Danilo Doneda é um dos pioneiros em trazer estas perspectivas ao ressaltar que os aspectos da personalidade ligados à privacidade não mais se limitam apenas a questões de isolamento e não publicização. Autonomia, liberdade, não discriminação, igualdade e construção da personalidade passam a perpetuar a compreensão do direito à privacidade, em um caráter relacional: "que deve determinar o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior – pela qual a pessoa determina sua inserção e exposição"[159]. No mesmo sentido, Rita Blum nota que o direito ao respeito à privacidade tem cada vez menos relação com a proteção de segredos e mais proximidade com o controle da pessoa sobre os seus dados[160].

Assim, passa a ganhar força nos últimos anos a conceituação de direito à privacidade que possui em seu núcleo o direito de o indivíduo exercer controle sobre as suas próprias informações. Conforme apontam Lazaro e Metayer, a noção de controle individual sobre as informações domina as discussões acerca da privacidade, sendo a ideia de controle mencionada não só como um elemento essencial de reflexões conceituais

---

[158] No original: "In both cases, the Internet has produced this loss of control: with copyright, because the technology enables perfect and free copies of content; with privacy (…) because the technology enables perpetual and cheap monitoring of behavior. In both cases, the question policy makers should ask is what mix of law and technology might restore the proper level of control". LESSIG, Lawrence. **Code v2.0**, Nova York: Basic Books, 2006, p.200.

[159] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006.p.146.

[160] BLUM, Rita P. F. **O Direito à privacidade e à Proteção dos Dados do Consumidor**. São Paulo: Almedina, 2018. p.90-105.

acerca de privacidade, mas também como um remédio prescritivo proposto por acadêmicos frente aos desafios tecnológicos impostos nos dias de hoje. As teorias da privacidade como controle enfatizam o papel da escolha e da autodeterminação individual, sendo o controle um processo individual, dinâmico e flexível[161].

Algumas visões do direito à privacidade como direito ao controle sobre informações pessoais existem há algum tempo, mesmo antes do advento da Internet. Por exemplo, Alan Westin, em 1967, descreveu a privacidade como direito de indivíduos, grupos ou instituições determinarem por si mesmas quando, como e em que extensão informações sobre si seriam comunicadas a outros[162].

Dentre concepções mais recentes sobre a privacidade que colocam o controle sobre informações como núcleo do direito, levando em conta o contexto de tratamento de dados pessoais em massa por diversos atores públicos e privados, a conceituação de Stefano Rodotà emerge como uma das mais influentes e serve de referência para diversas obras que debatem o tema no Brasil. O jurista italiano conceitua privacidade como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" e aponta como objeto deste direito o "patrimônio informativo atual ou potencial de um sujeito"[163].

Esta conceituação leva em conta as novas estruturas de organização do poder da sociedade, em que a informação assume caráter de recurso essencial[164]. Rodotà aponta a impossibilidade existente, para o Estado e para indústria, de renunciar a uma infraestrutura informativa cada vez mais ampla e justificada, o que leva à necessidade de uma garantia efetiva e da expansão dos direitos individuais ligados à privacidade[165]. Dessa forma, o autor afirma que o cidadão não pode ser considerado somente um "fornecedor de dados" aos organismos públicos e privados como contrapartida dos benefícios que terá pelo uso dos serviços por eles disponibilizados, devendo ser efetivamente capaz de exercer controle sobre seus dados.

---

[161] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? **SCRIPTed - Journal of Law, Technology & Society.** Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.
[162] WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967, p.7.
[163] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.109.
[164] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.23.
[165] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.36.

Daniel Solove critica as tentativas de conceituação da privacidade que buscam encontrar um núcleo comum entre todas as situações que envolvem esse direito, como vem sendo feito tanto nas teorias clássicas acerca do direito à privacidade quanto nas mais recentes[166]. Nesse sentido, tratar a privacidade como o direito ao controle sobre informações pessoais seria demasiadamente restrito por não abarcar situações "físicas" de invasão de privacidade, como quando uma pessoa observa seu vizinho através de uma luneta. Do mesmo modo, Marcel Leonardi justifica a necessidade de um conceito plural de privacidade, capaz de uma tutela mais ampla desse direito[167], servindo tanto para as situações "clássicas" de invasão à privacidade, quanto às que decorrem do atual fluxo de informações corrosivo à esfera privada. Tais ideias refletem uma posição que vem sendo adotada majoritariamente no contexto norte americano, em que não ocorre uma separação clara entre o direito à privacidade e a disciplina jurídica de proteção de dados pessoais. Esta última é abarcada por considerações acerca da privacidade e por vezes referida como privacidade informacional (*informational privacy*)[168]. Como será visto mais adiante, na Europa e no Brasil, devido às teorias de proteção dos direitos da personalidade, a privacidade é complementada pelo direito à proteção de dados pessoais, visando uma abordagem plural das questões informacionais que tocam ambos os direitos.

Ao refletir sobre a atual noção de privacidade e suas novas características, Rodotà identifica quatro tendências[169]: em seu conceito, o direito a ser deixado só dá lugar ao direito de manter controle sobre as informações que me digam respeito. Além disso, da busca pela privacidade passa-se a se buscar verdadeira autodeterminação informativa. A privacidade passa a servir também como garantia de não-discriminação. Por fim, de uma busca pela proteção do sigilo, passa-se a buscar o controle de dados e informações, públicos ou não. Com isso, o autor introduz a ideia que passa a ser desenvolvida no contexto Europeu nos últimos anos e que vem sendo absorvida pela doutrina majoritária brasileira.

O que se observa nesse contexto é o descolamento entre a disciplina do direito à privacidade e a disciplina relativa a um novo direito fundamental, de proteção de dados

---

[166] SOLOVE, Daniel. **Understanding Privacy.** Cambridge: Harvard University Press, 2008. p.37-39.
[167] LEONARDI, Marcel. **Tutela e privacidade na Internet**. São Paulo:Saraiva. 2011 p.52-77.
[168] SCHWARTZ, Paul. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. **The American Journal of Comparative Law**. Berkeley: American Society of Comparative Law. v. 37, n. 04, p. 675-701, Fall. 1989.
[169] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.23.

pessoais. As novas tecnologias de coleta e tratamento de dados apresentam problemas cada vez mais complexos, de forma que todas as questões que envolvem essa temática não "cabem" mais somente dentro do conceito de privacidade, ainda que o controle sobre as informações pessoais faça parte deste conceito. Nesse sentido, passa a se discutir o direito à proteção de dados pessoais como forma autônoma de resguardo dos direitos da personalidade em ambientes fortemente afetados pelas tecnologias, de forma complementar à privacidade.

Orla Linskey expõe que existem três maneiras de se enxergar a ligação entre o direito à privacidade e o direito à proteção de dados pessoais[170]. A proteção de dados pode ser vista como uma subespécie do direito à privacidade, sendo instrumental para seu resguardo. Assim, a proteção de dados pessoais seria uma consequência do atual estágio de evolução do direito à privacidade que passa a encampar elementos de controle informacional, para além da concepção clássica do direito de ser deixado a só, conforme vem sendo aplicado nos Estados Unidos.

Outra visão possível determina que a proteção de dados e a privacidade são direitos distintos, mas complementares**,** sendo que ambos são instrumentos que atuam em conjunto para se obter uma finalidade comum, de proteção da dignidade humana. Nesse sentido, um muito referenciado precedente jurisprudencial alemão[171], que deu origem à expressão "autodeterminação informativa", fundamenta a proposição de que proteção de dados e privacidade compartilham o propósito de possibilitar o autodesenvolvimento e a autonomia dos indivíduos, componentes da dignidade humana**.**

Por fim, a proteção de dados pode ser considerada um direito autônomo que serve a múltiplas funções, inclusive, mas não limitando-se, à proteção da dignidade humana. Atualmente, esta terceira vertente é prevalente no sistema jurídico europeu. Segundo essa

---

[170] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p.90.

[171] Em 1982, a corte constitucional alemã foi instada a se manifestar quanto à constitucionalidade da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho". A lei permitia o livre cruzamento entre os dados coletados durante o censo com outros bancos de dados públicos sem limitações quanto às finalidades, bem como permitia a transferência irrestrita dos dados entre órgãos da administração. Na oportunidade a corte considerou a lei parcialmente inconstitucional pois violaria o direito à "autodeterminação informativa" dos cidadãos, garantia derivada de disposições constitucionais de proteção da dignidade humana e livre desenvolvimento da personalidade. Assim criou-se um dos grandes marcos da proteção de dados pessoais que coloca o indivíduo na posição de protagonista no processo de tratamento de seus dados. Ver: SCHWARTZ, Paul. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. **The American Journal of Comparative Law**. Berkeley: American Society of Comparative Law. v. 37, n. 04, p. 675-701, Fall. 1989.; MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

visão, mesmo conceitos amplos de privacidade não suportam provisões características das regulações de dados pessoais mais recentes, como as que tratam de fluxos transfronteiriços de dados, regras de qualidade de tratamento e de segurança da informação, de modo que os direitos passam a ter maior campo de dissociação. Observa-se que a proteção de dados pessoais no contexto europeu serve também aos interesses econômicos da região, que busca garantir a livre transação de dados entre os países do bloco de maneira responsável e com segurança jurídica, para fomentar o desenvolvimento de negócios que se baseiam no tratamento de dados. Assim, essa terceira visão apresentada se diferencia da segunda no que tange às finalidades de ambos os direitos, colocando como objetivo da proteção de dados pessoais tanto a proteção da dignidade humana quanto a garantia de desenvolvimento econômico sustentável.

Ainda assim, de acordo com as duas últimas visões apresentadas, a proteção de dados e privacidade se sobrepõe em diversos campos. Por exemplo, ambos asseguram a privacidade informacional, ou privacidade de dados. Mas ambos possuem campos essencialmente distintos. No exemplo já mencionado, de uma pessoa que observa seu vizinho com uma luneta, verifica-se uma questão afeta exclusivamente à privacidade. Por outro lado, o direito à portabilidade de dados[172] é unicamente uma questão de proteção de dados. Ainda, no campo da proteção de informações, a proteção de dados pessoais acaba por ser mais ampla que a privacidade:

> Os direitos à proteção de dados e à privacidade se sobrepõe fortemente, mas no contexto da "privacidade informacional", o direito à proteção de dados vai além do direito à privacidade por prover aos indivíduos mais direitos sobre mais dados (ou controle aumentado sobre dados pessoais)[173].

Segundo Orla Linskey, a conceituação de Rodotà aparenta se filiar à corrente que considera que a privacidade engloba a proteção de dados, por considerar que as normas de proteção aos dados pessoais são o destino de uma longa evolução no conceito de privacidade. Porém, conforme a autora, ao mesmo tempo Rodotà reconheceu que vivenciamos a reinvenção da proteção de dados, que se torna instrumento essencial e autônomo no desenvolvimento da personalidade e, portanto, evidencia-se o descolamento entre os direitos, conforme as outras visões. Assim expressou Rodotà:

---

[172] Direito previsto no art. 18, inciso V, da LGPD, que permite ao titular a portabilidade de seus dados a outro fornecedor de serviço ou produto, mediante requisição expressa.

[173] No original: "the rights to data protection and privacy overlap heavily but that in the context of 'informational privacy' the right to data protection goes beyond the right to privacy by providing individuals with more rights over more personal data (or enhanced control over personal data)." LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p. 265.

> 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.[174]

No Brasil, é possível se observar que a doutrina vem caminhando entre a primeira e a segunda concepção, que ganha força com a aprovação de uma disciplina jurídica própria de proteção de dados pessoais (LGPD). No contexto anterior à lei, autores como Danilo Doneda[175] e Laura Schertel Mendes[176] colocavam a proteção de dados pessoais como resultado do desenvolvimento histórico do conceito de privacidade, sendo a garantia do direito à proteção de dados instrumental para a garantia da privacidade. Em ambos os casos, os direitos citados são abordados como medida necessária para a adequada proteção da personalidade humana frente aos desenvolvimentos tecnológicos recentes.

Conforme explica Mendes, os fundamentos normativos desse pensamento se encontram no artigo 5º, inciso X da Constituição de 1988, que prevê a inviolabilidade da intimidade e da vida privada. Segundo a autora, esse artigo garante a proteção da esfera privada do indivíduo em todas as suas dimensões, atraindo, portanto, a proteção de dados pessoais e da autodeterminação de informações[177]. Ainda, a autora fundamenta que o *habeas data* materializa a proteção de dados ao permitir aos sujeitos direito ao conhecimento, correção e complementação de seus dados em diversos contextos. No regramento infraconstitucional, antes da aprovação da Lei Geral de Proteção de Dados, o art. 43 e os princípios do CDC eram responsáveis por estabelecer uma proteção à personalidade e à privacidade do consumidor, também na sua dimensão da proteção de dados pessoais.

Mais recentemente, Bruno Bioni demonstra que compreender a proteção de dados pessoais como um direito da personalidade autônomo é essencial para devida proteção da personalidade frente aos novos desafios impostos pelas tecnologias[178]. Além disso,

---

[174] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 17.
[175] DONEDA, Danilo**. Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006.
[176] MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.
[177] MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.
[178] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

tramita no Congresso um projeto de emenda constitucional que visa acrescentar ao rol de direitos fundamentais da Constituição menção expressa à proteção de dados[179].

Assim, depreende-se que a doutrina brasileira atual trata a privacidade e a proteção de dados pessoais como direitos distintos e autônomos, em conformidade com o desenvolvido no âmbito europeu. Observa-se, porém, que as finalidades econômicas da disciplina de proteção de dados pessoais são pouco exploradas no contexto brasileiro, estando as principais obras acerca do tema focadas no papel destes direitos para a garantia da dignidade humana, de modo que a privacidade e a proteção de dados ainda compartilham a finalidade comum no campo teórico.

Tendo em vista o descolamento que ocorre entre os direitos, algumas diferenças essenciais entre privacidade e proteção de dados pessoais devem ser esclarecidas para que se possa adentrar no tema de regulação do *profiling.* Segundo Bruno Bioni, a privacidade hoje está ligada ao controle de informações pessoais que revelem aspectos íntimos ou privados do sujeito, características que o sujeito não pretende compartilhar com o público ou com seus pares. Por sua vez, a proteção de dados pessoais não se restringe às informações privadas, uma vez que, devido aos inúmeros usos que podem ser atribuídos aos dados, mesmos dados públicos merecem certo tipo de proteção e garantias, como por exemplo, a de sua exatidão[180]. Existem ainda, informações que a pessoa conscientemente compartilha com seus pares de maneira pública, pelo uso de redes sociais por exemplo, e que, portanto, sua proteção é incompatível com a ideia de privacidade. Apesar de tais informações serem conscientemente retiradas da esfera privada do sujeito, isso não significa que as empresas possam dar destino indiscriminado a eles, devendo incidir uma disciplina de proteção de dados que evite eventuais abusos.

Assim, há uma clara diferença no escopo das informações protegidas. A proteção de dados se refere a dados pessoais, em acepção ampla, que merecem proteção ainda que não tratem de informação protegida pela privacidade. Como exemplo, a privacidade não limita o acesso, pelo empregador, dos registros de pagamentos feitos a um empregado,

---

[179] BRASIL. Senado Federal. Proposta de Emenda Constitucional nº 17, de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em 18 de nov. de 2019.

[180] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 92-101.

mas estas informações se sujeitam às regras de proteção de dados[181]. Dado pessoal, conforme vem sendo adotado em diversas legislações[182], se refere a toda informação relacionada a pessoa identificada ou identificável, e não somente a dados que a pessoa espera reter em seu âmbito de intimidade. Assim, segundo Orla Linskey:

> O direito à proteção de dados pessoais vai além de meramente modernizar e trazer o direito à privacidade para a era digital. Em vez [...], o direito a proteção de dados pessoais busca proteger direitos individuais distintos no controle e manipulação da informação pessoal: uma proteção que vai além da proteção da privacidade e é mais bem concebida como um direito proativo do indivíduo de gerenciar seus próprios dados pessoais em face das pressões tecnológicas exercidas sobre esse controle[183].

Portanto, os dados que influem na projeção da identidade pública de uma pessoa, formando parte de sua relação com o mundo exterior, constituem o escopo de proteção deste novo direito da personalidade[184]. Segundo Bioni, é necessário alocar a proteção dos dados pessoais nessa categoria jurídica para que haja coerência normativa entre uma série de faculdades jurídicas próprias desse direito, estabelecidas na Lei Geral de Proteção de Dados brasileira. Tratar a proteção de dados pessoais como um direito da personalidade autônomo facilita sua interpretação e aplicação de forma a não se confundir a compreensão de alguns de seus conceitos essenciais. Para o autor, abordar a proteção de dados como mera evolução do direito à privacidade é um equívoco cometido por parte da doutrina pois o atual estágio de transformações sociais ocasionadas pelo tratamento de dados traz problemas que em muito extrapolam o âmbito da privacidade.

Ainda conforme a exposição de Bruno Bioni[185], o fato de se verificar uma forte conexão entre privacidade e proteção de dados, presente na doutrina brasileira, ocorre,

---

[181] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p.32.

[182] Assim definiu a LGDP em seu art. 5º, inciso I: "Art. 5º Para os fins desta Lei, considera-se: IV- dado pessoal: informação relacionada a pessoa natural identificada ou identificável"; No mesmo sentido, mas de maneira mais ampla, a GDPR define em seu art. 4º, inciso I: "Dados pessoais - informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

[183] No original: "the right to data protection goes beyond merely modernizing the right to privacy and bringing it into the digital age. Instead[…], the right to data protection seeks to protect distinct individual interests in controlling the manipulation of personal information: a protection which goes beyond protecting privacy and is better conceived as a proactive right to manage one's own personal data in the face of mounting technological pressures on such control". LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press. 2015, p. 130.

[184] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.77-83.

[185] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.99.

em grande parte, por influência norte-americana, onde não se distinguem tais direitos. Isso ocorre nos EUA pois, naquele sistema jurídico, não existe a construção dogmática dos direitos da personalidade, de forma que a privacidade se alarga para defender de forma mais ampla todos os aspectos da personalidade humana. No Brasil, a doutrina consolidada dos direitos da personalidade permite a construção de uma categoria autônoma para proteção de dados pessoais.

Laura Schrtel reconhece que os dispositivos constitucionais atuais, que abordam a proteção da informação, não trataram dos problemas mais recentes relativos ao processamento de dados[186], pois a disposição constitucional atualmente em vigor protege as informações íntimas e as comunicações. Esses tipos de processamentos, dentre os quais se inclui o *profiling*, não são feitos necessariamente com a obtenção de informações de caráter íntimo ou sigiloso. Contudo, o ponto comum verificado nas técnicas de processamento modernas é a utilização de informações identificam e a caracterizam uma pessoa. Assim, trata-se de informações pessoais que merecem proteção constitucional, ainda que não sejam informações íntimas ou privadas, pois podem afetar diversos direitos fundamentais além da privacidade. Por exemplo, nessa espécie de processamento de dados, o direito à igualdade pode ser afetado devido aos possíveis efeitos discriminatórios do uso de dados pessoais para classificação da população, afetando as oportunidades de vida do indivíduo. Portanto, a disciplina da proteção de dados pessoais enfrenta diferentes questões, como os diferentes efeitos negativos à autonomia decorrentes do *profiling*, expostos no capítulo anterior.

Conforme apresenta Laura Schrtel, as garantias de sigilo e de inviolabilidade da vida privada são importantes mecanismos de proteção individual, mas se mostram insuficientes para lidar com os atuais efeitos do processamento e da utilização da informação sobre o indivíduo. Desse modo, a autora sustenta que somente o reconhecimento de um direito fundamental à proteção de dados pessoais poderia fazer frente aos atuais riscos aos quais os indivíduos estão submetidos. O reconhecimento desse direito na ordem constitucional é possível através da interpretação conjunta e extensiva das garantias de proteção da informação e do instituto do *habeas data*. Com a aprovação da Lei Geral de Proteção de Dados no Brasil, consolida-se a visão de uma disciplina

[186] MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

apartada e mais ampla que a dada anteriormente, que estava ainda muito ligada à privacidade.

Pode-se afirmar, porém, que as crescentes preocupações relativas à privacidade levaram com que maiores esforços regulatórios se desenvolvessem ao redor do mundo para tratar adequadamente do tema. Desse modo, as inquietações acerca da constante coleta de dados e vigilância praticada pelo Estado e pelo setor privado foram uma força motriz no desenvolvimento das garantias de proteção de dados pessoais, de modo que não é errado considerar tais garantias como o resultado histórico do desenvolvimento da privacidade. Porém, hoje não se pode mais afirmar que a proteção de dados pessoais seja somente uma dimensão do direito à privacidade. A proteção de dados serve, atualmente, a múltiplos fatores, como a própria privacidade, a segurança de informações, a segurança jurídica em transações de dados, dentre outros.

Nesse sentido, a proteção jurídica incidente sobre a prática de *profiling* é um ótimo exemplo na qual se verifica o gradual descolamento entre a privacidade e a proteção de dados. Frente ao *profiling*, a proteção de dados se torna instrumental para se garantir tanto a privacidade quanto a não discriminação entre indivíduos e grupos, de forma a garantir que pessoas não fiquem presas a perfis estigmatizados que limitam suas liberdades de escolhas. A proteção necessária para coibir efeitos danosos presentes no *profiling* é uma questão em que fica evidente a ideia demonstrada por Orla Linskey, de que privacidade e proteção de dados se sobrepõem em diversos aspectos, mas a proteção de dados permite uma proteção mais ampla, sobre informações mais diversas. O desenvolvimento tecnológico avançou de tal maneira que o processamento de dados em massa cria riscos que extrapolam a esfera de invasão da vida privada, como ocorre no *profiling*, que traz uma dimensão de risco de discriminação e de forte limitação em escolhas pessoais.

Assim, observa-se no *profiling* um problema relativo tanto à privacidade quanto à proteção de dados. Os riscos da definição de perfis sobre a privacidade surgem quando informações íntimas, que o indivíduo não tem intenção de publicizar, são indevidamente coletadas e utilizadas para formação de um perfil, ou quando se permite fazer inferências intrusivas de características pessoais, a partir de dados públicos legitimamente coletados. Porém, as consequências do *profiling* necessitam de um campo de proteção ainda maior, devido aos seus potenciais efeitos discriminatórios, que podem resultar da criação e da utilização de perfis, mesmo que estes não se utilizem de dados privados em sua essência ou que formem perfis sem inferências quanto a aspectos da vida íntima do sujeito. Desse

modo, a proteção de dados serve um propósito que vai além da privacidade, sendo fundamental para garantias de não discriminação pelo procedimento de classificação de pessoas por meio de perfis.

Portanto, os limites legais à prática de *profiling* devem ser dados de acordo com a definição de uma disciplina jurídica de proteção de dados, mais ampla do que a privacidade. A fim de se garantir a privacidade, normas de proteção de dados devem limitar a coleta de informações íntimas de forma indevida e evitar a utilização de dados para se extrair características da vida privada dos sujeitos na construção dos perfis. Porém, outros limites devem ser impostos, em função dos diferentes efeitos que podem surgir com tratamento de dados para *profiling*, não necessariamente ligados à privacidade e que serão explorados no próximo tópico.

Para se garantir a privacidade frente a práticas de *profiling*, o papel da proteção de dados é estabelecer mecanismos que permitam o controle dos indivíduos sobre quais dados são utilizados e quais características pessoais compõe o perfil. Observa-se que a ideia de se exercer controle sobre informações está contida tanto na proteção jurídica da privacidade quanto na proteção jurídica dos dados pessoais. O direito à privacidade garante ao indivíduo controle sobre suas informações íntimas, que revelam algo sobre sua pessoa que não se deseja compartilhar de maneira ampla. A proteção de dados pessoais, por sua vez, envolve o controle sobre todos os dados pessoais, assim entendidos como aqueles que identificam ou podem identificar uma pessoa, seja algo afeto à sua vida pública ou privada.

As teorias da privacidade e da proteção de dados que se baseiam no controle individual sobre informações, enfatizam o papel da escolha e da autodeterminação individual, sendo o controle um processo individual, dinâmico e flexível[187]. O controle sobre informações se materializa em uma série de direitos individuais, como o direito à informação sobre a coleta de dados, à ciência da disponibilização dos dados a terceiros, direito ao acesso e potencial correção ou exclusão dos dados coletados, dentre outros[188]. Desse modo, o controle sobre as informações se manifesta dentro da noção conceitual da privacidade e possui também uma noção instrumental, de manutenção da privacidade por

[187] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? **SCRIPTed - Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, jun. 2015.

[188] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? **SCRIPTed - Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, jun. 2015.

meio de mecanismos de proteção de dados pessoais[189]. A forma como esse controle deve se materializar nas legislações de proteção de dados pessoais, de forma a limitar a prática de *profiling*, será exploradas na parte final deste capítulo.

3.2 Proteção de dados pessoais e a discriminação resultante de *profiling*

Conforme estudado, a disciplina de proteção de dados pessoais é capaz de lidar com problemas de diferentes ordens, por ser mais ampla do que a privacidade e pretender conferir proteção a qualquer informação que possa identificar uma pessoa. No capítulo anterior, foi constatado que, além dos riscos à privacidade dos cidadãos, o uso de dados pessoais para constituir perfis, classificar e selecionar pessoas, pode levar a que certos indivíduos ou grupos sofram com tratamento desigual ilegítimo, devendo assim haver normas de proteção de dados pessoais capazes de limitar que estas situações ocorram.

Segundo explica Laura Schertel Mendes, os dados pessoais muitas vezes constituem a única forma de representação das pessoas perante organizações estatais e privadas, podendo vir a ser determinantes para definir seus acessos a diferentes oportunidades[190]. Assim, conforme argumenta a autora, a devida formulação de políticas de proteção de dados pessoais voltada para a tutela da personalidade, deve visar a autonomia de escolhas ao cidadão e sua proteção perante situações potencialmente discriminatórias[191]. Assim resume Stéfano Rodotà: "A difusão do recurso aos perfis pode ocasionar a discriminação das pessoas que não correspondem ao modo geral, acentuando a estigmatização dos comportamentos desviantes e a penalização das minorias. Pode-se identificar aqui um obstáculo ao pleno desenvolvimento da personalidade individual"[192].

Desse modo, uma adequada regulação da prática de *profiling* envolve a criação de mecanismos de proteção de dados pessoais para os sujeitos cujas vidas são constantemente afetadas pela tomada de decisões feita com base em perfis. Tais mecanismos devem evitar os reflexos negativos injustificáveis decorrentes do tratamento automatizado dos dados.

---

[189] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? **SCRIPTed - Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, jun. 2015.

[190] MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

[191] MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

[192] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 105-106.

No Brasil, a proibição de tratamentos discriminatórios é sustentada com base no direito à igualdade. A proteção da igualdade no ordenamento jurídico brasileiro passa por uma série de garantias constitucionais, infraconstitucionais e convencionais que se complementam. Sua principal expressão é encontrada no artigo 5º, *caput* e inciso I, da Constituição da República. Nesses dispositivos se materializam uma leitura da igualdade como imparcialidade e não discriminação, em regra dirigida aos atos do poder público[193]. Em linhas gerais, o entendimento desenvolvido no Brasil é de que a discriminação corresponde a uma violação ao direito da igualdade devido à falha em atender, cumulativa e sucessivamente, aos requisitos da racionalidade e da constitucionalidade em determinada diferenciação entre pessoas[194] Em outros termos, discriminação corresponde a uma diferenciação entre pessoas injustificável com base em um ponto de vista racional ou constitucional, devendo se verificar a razoabilidade entre o critério utilizado para diferenciação e os fins que se pretende atingir com o tratamento diferencial feito[195].

Observa-se que grande parte da discussão acerca do direito à igualdade na doutrina e jurisprudência brasileira visa definir que tipo de discriminação é ilegítima e qual tipo pode ser permitida a fim de se concretizar valores sociais diversos, constituindo-se mera diferenciação (ou discriminação legítima). Esse tipo de análise ocorre, principalmente, quando se observa uma norma jurídica que impõe tratamento diferenciado entre as pessoas e, por esse motivo, tem sua constitucionalidade contestada com base no direito à igualdade[196]. O modelo comumente adotado no Brasil que exige uma razão racional e em conformidade com a Constituição para que se configure discriminação legítima apresenta algumas limitações se aplicado em diferentes contextos, sendo duas delas especialmente relevantes para o presente estudo. Segundo Daniel Andrade[197], essa concepção se restringe à ideia de discriminação direta e, além disso, não é adequada para situações de diferenciação entre particulares, no exercício de sua autonomia privada.

---

[193] FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9ª. ed. Salvador: JusPODIVM, 2018, p. 461.
[194] MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3. ed. São Paulo: Malheiros, 2009, p. 17.
[195] ANDRADE, Daniel de Pádua. **Associação e Discriminação**: limites jurídicos para os critérios de admissão, exclusão e categorização de associado. 2018. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, Belo Horizonte, 2018, p.95-102.
[196] FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9ª. ed. Salvador: JusPODIVM, 2018, p. 465.
[197] ANDRADE, Daniel de Pádua. **Associação e Discriminação**: limites jurídicos para os critérios de admissão, exclusão e categorização de associado. 2018. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, Belo Horizonte, 2018. p. 95-105.

Conforme exposto no capítulo anterior, o *profiling* pode resultar tanto em discriminação direta quanto em discriminação indireta. Se o *profiling* for utilizado para inferências acerca da religião praticada por um candidato a certa vaga de emprego, sendo ele eliminado da seleção em virtude do resultado encontrado, verifica-se a ocorrência de discriminação direta, capaz de ser identificada pelos critérios tradicionalmente apresentados pela doutrina brasileira, uma vez que realizar esse tipo de diferenciação não se afigura razoável e fere a liberdade religiosa prevista constitucionalmente.

A discriminação indireta, porém, ocorre quando uma medida, critério ou prática, conquanto aparentemente neutra, afeta de maneira especialmente negativa certo grupo ou minoria protegida. Assim, são utilizados critérios de diferenciação entre pessoas aparentemente justificáveis e razoáveis, sendo que o resultado discriminatório do tratamento diferenciado só pode ser depreendido após análise dos resultados da prática quando reiterada ao longo do tempo. É o que ocorre no caso de *redlining* abordado anteriormente, em que instituições financeiras buscam atingir uma finalidade legítima (margem de lucro e segurança de crédito) e se utilizam de critérios de diferenciação aparentemente justificáveis para avaliação de crédito, mas que acabam refletindo negativamente em parte desprivilegiada da população, ainda que não haja elemento intencional discriminatório[198]. Nesses casos, o modelo de verificação da razoabilidade adotado no Brasil não identificaria a ocorrência de discriminação uma vez que não se verificam critérios de diferenciação ilegítimos, ainda que haja um claro prejuízo para um segmento populacional que afete significativamente a igualdade entre pessoas.

Além disso, o setor privado é responsável por grande parte das práticas de *profiling* com uso de dados pessoais e busca-se, na presente pesquisa, esclarecer quais são os limites legais ao uso dessa técnica por particulares, tendo em vista seus potenciais impactos indesejados na sociedade. Conforme destaca Daniel Andrade, a racionalidade das escolhas de particulares goza de mais ampla liberdade do que a de atos do poder público, não havendo um dever de motivação inerente às práticas de diferenciação feitas pelo indivíduo no exercício de sua autonomia privada[199]. Portanto, com base no atual entendimento que impõe uma espécie de teste para observar se as razões do tratamento

[198] BAROCAS, Solon; SELBST, Andrew D. Big Data‘s Disparate Impact. **California Law Review**, Berkeley, v. 104, p. 671-732, 2016.
[199] ANDRADE, Daniel de Pádua. **Associação e discriminação**: limites jurídicos para os critérios de admissão, exclusão e categorização de associado. 2018. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, Belo Horizonte, 2018, p. 100.

diferenciado são justificáveis ao fim pretendido, restaria impossibilitada a verificação da discriminação indireta, pela desnecessidade dos agentes privados agirem de maneira justificada a todo tempo.

Isso se torna especialmente problemático no campo de tratamento de dados por algoritmos, que apresentam um problema inerente de opacidade e são constantemente referidos como uma "caixa-preta"[200]. Isso se verifica, pois, a razão logica para certo resultado obtido na análise de dados automatizada apresenta sérias limitações de acesso mesmo para aqueles que construíram o sistema. A opacidade dos sistemas existe também por razões de direito, de proteção à propriedade intelectual dos sistemas que poderia ser inutilizada caso revelada a lógica inerente às suas decisões[201].

Observa-se, assim, que considerações jurídicas acerca da discriminação indireta e da discriminação presente em ações entre particulares ainda são pouco exploradas no contexto brasileiro. O que se torna essencial é a percepção de que o *profiling* deve ter seus limites balizados pelo princípio da igualdade, de modo a não permitir que seu uso leve ao tratamento diferenciado injustificável entre pessoas. Definir exatamente quais as situações que configuram prática discriminatória no âmbito do *profiling* praticado por empresa, e os critérios dogmáticos para sua verificação é algo que ainda demanda maior desenvolvimento no campo teórico do direito à igualdade, principalmente no que tange à discriminação indireta e à discriminação presente em atos de particulares. Certo é que o tema demandará ainda grandes evoluções, frente a alta possibilidade de que os tribunais brasileiros sejam acionados por pessoas que se sintam prejudicadas por decisões automatizadas tomadas com base em seus perfis.

Por outro lado, para os fins buscados no presente estudo, basta a constatação que há um risco concreto de que a discriminação ocorra[202] no contexto do *profiling*, ou seja, é possível que pessoas tenham as suas vidas afetadas injustamente, por decisões tomadas com base em perfis que afetam um grupo ou uma minoria de maneira desigual. Situações reais em que isso ocorre já foram identificadas, como nos citados anúncios transmitidos

---

[200] PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p.22.

[201] ALMEIDA, Virgilio; DONEDA, Danilo. What is Algorithm Governance? **IEEE-Internet Computing**, [S.l.], v. 20, p. 60-63, 2016. Disponível em: https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUyekJ2d. Acesso em: 20 nov. 2019.

[202] CALDERS, Toon; ŽLIOBAITĖ, Indrė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures. In: CUSTERS, Bart et al. **Discrimination and Privacy in the Information Society: Data Mining and *Profiling* in Large Databases.** Berlim: Springer, 2013. cap. 3.

pelo Facebook, que exibiam oportunidades de empregos e ofertas de moradia direcionados com base em estereótipos de gênero e raça[203]. Nesse sentido, Solon Barocas e Andrew D. Selbst descrevem a existência de ao menos cinco mecanismos inerentes aos procedimentos de mineração de dados para construção de perfis que possuem potencial discriminatório por permitirem que classes protegidas sejam desfavorecidas[204]. Assim esclarecem Barocas e Selbst:

> Por definição a mineração é sempre uma forma de discriminação estatística (e por isso, aparentemente racional). De fato, o próprio objetivo da mineração de dados é prover bases racionais com as quais se pode distinguir indivíduos e conferir de maneira confiável ao indivíduo características possuídas por aqueles com os quais ele é estatisticamente similar. De qualquer maneira, a mineração de dados tem o potencial de desvalorizar indevidamente membros de classes legalmente protegidas e de colocá-los em uma relativa desvantagem sistemática[205].

A fim de se conciliar a função essencial de diferenciação, característica do *profiling* feito por meio da mineração de dados pessoais, com a ideia de igualdade, é necessário que o tipo de diferenciação realizada não implique na segregação desarrazoada de pessoas com base em critérios especialmente protegidos como raça, gênero, religião ou opiniões políticas. É preciso também atentar para a tarefa mais difícil, de lidar com a discriminação indireta que resulta do uso de critérios com aparente neutralidade, mas que afetam de forma mais incisiva certos grupos de maior fragilidade.

É na disciplina jurídica de proteção de dados pessoais onde se busca potenciais soluções para os problemas apontados. Estabelecer os limites legais para o *profiling* por meio de normas de proteção de dados pessoais, a serem observadas pelos particulares que pretendem desenvolver atividades de processamento de dados, visa evitar que tais situações ocorram de forma descontrolada e sem consequências para aqueles que as propagarem.

---

[203] PAUL, Katie; RANA, Akanksha. U.S. charges Facebook with racial discrimination in targeted housing ads. **Reuters**, Londres, p. 1, 19 mar. 2019. Disponível em: https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8. Acesso em: 3 set. 2019.

[204] BAROCAS, Solon; SELBST, Andrew D. Big Data‘s Disparate Impact. **California Law Review**, Berkeley, v. 104, p. 671-732, 2016.

[205] No original: “By definition, data mining is always a form of statistical (and therefore seemingly rational) discrimination. Indeed, the very point of data mining is to provide a rational basis upon which to distinguish between individuals and to reliably confer to the individual the qualities possessed by those who seem statistically similar. Nevertheless, data mining holds the potential to unduly discount members of legally protected classes and to place them at systematic relative disadvantage.” BAROCAS, Solon; SELBST, Andrew D. Big Data’s Disparate Impact. **California Law Review**, Berkeley, v. 104, p. 671-732, 2016.

Em análise sobre o *profiling* no contexto comunitário europeu, Paul de Hert e Hans Lammerant[206] destacam que o princípio da não discriminação deve limitar o que pode ou não ser relevante na construção de perfis para determinados fins, de modo que algumas características consideradas mais sensíveis pela sociedade não devem ser utilizadas para categorizar pessoas, ao menos que plenamente justificável. Os limites impostos pela igualdade devem ser observados nos diversos estágios do processamento, da seleção da base de dados à aplicação do perfil. Segundo os autores, para se acessar eventuais casos de discriminação indireta, seria necessária a realização de testes de não discriminação aplicados sobre os resultados do *profiling*, de forma a se checar ativamente a ocorrência de tratamento diferenciado injustificado para o fim perseguido.

No mesmo sentido, Garfinkel ressalta a importância de se levar em conta a garantia da não-discriminação na criação de limites jurídicos aos tratamentos de dados pessoais[207]. Assim, o autor afirma que proteger dados pessoais nos dias de hoje é uma forma de defesa contra problemas sociais ainda não erradicados, sendo essencial para permitir o livre desenvolvimento da personalidade e da própria identidade de sujeitos que possam ter suas escolhas individuais tolhidas por estigmas sociais.

Retomando a ideia dos dossiês digitais de Solove, Bruno Bioni[208] também ressalta como a coleta de dados permite a captura da identidade do ser humano de forma a constituir sua biografia digital, sendo assim usada para classificação e segmentação da população. Com este processo, formam-se estereótipos que estigmatizam o sujeito perante seus pares e que determinam uma série de decisões acerca de sua vida. A categorização de pessoas a partir de seus dados pessoais pode repercutir nas suas oportunidades sociais dentro de uma economia movida a dados, nos termos do explorado ao longo deste estudo. Ao refletir sobre o papel da proteção de dados pessoais sobre as práticas de *profiling*, Bruno Bioni afirma:

> A tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, por tabela, ao livre desenvolvimento de sua personalidade(...) Cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio

[206] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. In: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.
[207] GARFINKEL, Simson. **Database nation**: the death of privacy in the 21st century. Boston: O'Reilly Media, 2010, p. 168.
[208] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p.89-92.

> futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade.[209]

A formação de perfis que baseiam a tomada de decisões automatizadas e impactam a vida privada dos indivíduos é um dos principais argumentos que levam o autor a destacar a ideia de que o direito à proteção de dados pessoais reclama uma normatização própria que não deve se limitar a mera evolução do direito à privacidade, mas sim ser abordada como um novo direito da personalidade. Assim, segundo Bioni, a proteção de dados pessoais se comunica com outras garantias, como liberdade de expressão, de acesso à informação e de não discriminação, que constituem a própria capacidade de autodeterminação pessoal[210].

Ante o exposto, é possível concluir que a disciplina da proteção de dados pessoais não se propõe normatizar quais situações de tratamento de dados são, de fato, discriminatórias, mas reconhece que o processamento de dados pessoais de maneira irrestrita possui forte potencial para gerar tais situações. Portanto, a proteção de dados tem como uma de suas principais pretensões evitar a ocorrência de discriminação com o processamento de dados, conferindo, por exemplo, proteção diferenciada para dados considerados sensíveis. Além disso, se torna necessária a criação de mecanismos que permitam avaliar, de maneira ampla, os reflexos sociais dos diversos tipos de tratamentos de dados, para que seja possível verificar se houve de fato alguma espécie de discriminação e coibir o processamento de dados a ela associada. Assim, a doutrina sugere a necessidade, mesmo para o setor privado, de que as legislações imponham regras de transparência e *accountabllity* para aqueles que empreguem algoritmos de processamentos de dados responsáveis pelo *profiling*[211].

É preciso atentar que, para concretizar tais ideias, é necessário, mais do que garantias legais, o desenvolvimento de soluções técnicas capazes de viabilizar as

---

[209] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 92

[210] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 92.

[211] Assim apontam os seguintes estudos: MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data:** a revolution that will transform how we live, work and think. Nova Iorque: HMH, 2013. E-book; HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. In: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173. CALDERS, Toon; CUSTERS, Bart. What Is Data Mining and How Does It Work? In: CUSTERS, Bart et al (ed.). **Discrimination and Privacy in the Information Society:** Data Mining and *Profiling* in Large Databases. Berlim: Springer, 2013. cap. 2, p. 28.

salvaguardas normativas. Cinthia Freitas[212], ao abordar os reflexos do tratamento de dados pessoais que permeiam tanto o campo jurídico quanto o das tecnologias, menciona o *profiling* e os riscos de discriminação dele advindos como como um dos principais desafios na busca pela integração das garantias legais em sistemas de alta complexidade técnica.

Hert e Lammerant[213] apontam diversos estudos desenvolvidos com o objetivo de diminuir o potencial viés discriminatório no tratamento de dados para formação de perfis, para que o processamento de dados seja feito de acordo com o ordenamento legal. Porém, os autores identificam haver certa descrença entre especialistas do tema, que acreditam que as exigências legais serão raramente aplicadas, pois o mercado não envidará esforços para tornar o *profiling* menos problemático. Isso porque a mineração de dados se tornaria muito pouco efetiva caso aplicadas muitas restrições nas variáveis utilizadas, visando reduzir uma análise enviesada.

Outros acreditam haver espaço para desenvolvimento de técnicas de auditoria de sistemas e outras soluções tecnológicas, com intuito de identificar e corrigir resultados discriminatórios em algoritmos[214]. Seria possível, inclusive, que a proibição de discriminação sob certas bases fosse programada em "*discrimination-aware algorithms*", algoritmos capazes de identificar vieses discriminatórios. Assim, afirmam ser viável que, no campo do *profiling*, as salvaguardas legais sejam suportadas por salvaguardas técnicas, padronizadas pela regulamentação de normas padronizadas[215]. Desse modo, é necessário que a imposição de limites legais ao *profiling*, por meio de normas de proteção de dados, leve em conta a efetividade da integração de garantias nas tecnologias desenvolvidas. Concluem Hert e Lammerant:

> Enquanto a proibição à discriminação é uma salvaguarda legal útil, ela deve ser levada a cabo por meio do desenvolvimento de instrumentos de auditoria e

---

[212] FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao *profiling* e à discriminação a partir das novas tecnologias**. Revista de Direito, Governança e Novas Tecnologias**, Maranhão, v. 3, n. 2, p. 18-38, jul. [dez]. Disponível em: <https://www.researchgate.net/publication/323382063_TRATAMENTO_DE_DADOS_PESSOAIS_E_A_LEGISLACAO_BRASILEIRA_FRENTE_AO_*PROFILING*_E_A_DISCRIMINACAO_A_PARTIR_DAS_NOVAS_TECNOLOGIAS>. Acesso em: 09 nov. 2018.

[213] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. In: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173

[214] CALDERS, Toon; CUSTERS, Bart. What Is Data Mining and How Does It Work? In: CUSTERS, Bart et al (ed.). **Discrimination and Privacy in the Information Society: Data Mining and *Profiling* in Large Databases**. Berlim: Springer, 2013. cap. 2, p. 28.

[215] HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. In: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

> algoritmos capazes de identificar vieses discriminatórios (...) Transparência e *accountability* podem ser projetadas nas práticas de *profiling*. Isso deve ser apoiado por salvaguardas institucionais mais fortes para permitir avaliações independentes e rápido feedback nas tomadas de decisão.[216]

Portanto, verifica-se que a disciplina legal da proteção de dados pessoais é o instrumento normativo capaz de dar o tratamento adequado ao processamento de dados que visa a definição de perfis, a fim de se atingir as finalidades de proteção à privacidade e à igualdade. Para serem efetivas, sugerimos neste trabalho a hipótese de que as normas de proteção de dados pessoais devem favorecer a criação do que vem sendo chamado de "arquitetura de controle" sobre o processamento de dados. Essa visão, cuja principal referência é a obra de Daniel Solove, visa a formação de um ambiente legislativo integrado com as novas tecnologias, de modo a favorecer o controle sobre os fluxos de dados pessoais em diversas vertentes. Os aspectos essenciais da arquitetura de controle, os limites legais que esse sistema impõe ao *profiling*, e como isso servirá para amenizar os efeitos negativos da prática de *profiling* serão discutidos no próximo tópico.

3.3 Regulação do *profiling*: criando uma arquitetura de controle sobre dados pessoais

Conforme apresentado, os limites legais da prática de *profiling* no setor privado devem ser pautados pela garantia do direito à privacidade e à igualdade dos indivíduos. Isso pode ser feito por meio de uma adequada disciplina jurídica de proteção de dados pessoais, que hoje, no sistema jurídico brasileiro, pode ser entendida como um direito da personalidade autônomo que se desdobra em diversas garantias legais previstas na Lei Geral de Proteção de Dados. O papel da proteção de dados na garantia da privacidade frente a práticas de *profiling* é criar mecanismos que limitem a coleta de informações íntimas de forma indevida e evitem a utilização de dados para se extrair características da vida privada dos sujeitos envolvidos na construção dos perfis. Por sua vez, o papel da proteção de dados na garantia da igualdade no tratamento de informações que envolva a definição de perfis é viabilizar a governança, transparência e *accountability* dos sistemas de *profiling*, a fim de identificar e coibir eventuais efeitos discriminatórios. A conjugação

---

[216] No original: "While the prohibition of discrimination is a useful legal safeguard, it must be given teeth through the development of audit tools and discrimination-aware algorithms (...) Transparency and accountability can be designed into profiling practices. This must be backed up with stronger institutional safeguards to allow for independent assessments and rapid feedback into decision-making." HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. In: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

das finalidades da proteção de dados pessoais envolve a necessidade de desenvolvimento de diversos mecanismos de controle sobre o fluxo das informações, que podem ser vistos como uma espécie de arquitetura de controle, nos termos expostos adiante.

Solucionar problemas por meio de arquitetura significa buscar a alteração de estruturas no intuito de criar um ambiente propício para realização do fim buscado. A ideia da arquitetura de controle pode ser entendida conforme a teorização construída por Daniel Solove[217]. Com intuito de apresentar soluções ao problema da burocracia verificada no processamento de dados por grandes instituições, e da formação de dossiês digitais, discutida no primeiro capítulo deste estudo, Daniel Solove propõe a formação de uma arquitetura de proteção de dados voltada para o setor privado. Argumenta o autor que as noções iniciais acerca do direito à privacidade buscavam proteger a vida privada por meio da reparação de danos em casos de violações da intimidade de um indivíduo, como, por exemplo, com a publicação de fotos de momentos privados de uma pessoa pública. Porém, conforme estudado, essa concepção estritamente negativa e reparatória da privacidade é insuficiente para lidar com os meios modernos de difusão de dados e informações, que passam a envolver desafios cada vez mais complexos.

Destaca Solove que, para se enfrentar os novos problemas do mundo digital, é preciso realizar a transição de uma posição estritamente reativa para uma posição proativa, pois os riscos emergentes da construção de perfis pela coleta em massa de dados são de natureza sistêmica[218], e não somente de episódios avulsos de ilícitos, que causam um dano isolado. No mundo atual, em que as informações pessoais estão fora do controle de seus titulares e submetidas a procedimentos burocráticos de tratamento, observa-se danos generalizados em razão de problemas sistêmicos no fluxo de informações.

Outra mudança que deve ser buscada no intuito de melhor limitar a prática de *profiling* por meio de uma arquitetura de controle, se refere a uma transição de medidas de proteção que dependem da iniciativa individual, para meios coletivos de controle de dados. As questões que envolvem o *profiling* e que potencializam efeitos nocivos advindos da prática decorrem, em grande medida, das características estruturais da sociedade da informação, de forma que não afetam somente um indivíduo específico, mas a comunidade como um todo. Daniel Solove reitera que, em casos de danos criados por

---

[217] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 93-119.
[218] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 95.

uma estrutura social, como hoje se observa na sociedade da informação, remédios individuais costumam ser pouco efetivos[219]. Vem sendo reiteradamente apontado na doutrina que estuda a proteção de dados que mecanismos de controle individual, como a obtenção de consentimento para tratamento de dados exigido pela maioria dos serviços *online*, costumam falhar em conferir qualquer tipo de garantia ao usuários pois a maioria das pessoas não detém conhecimento, recursos ou tempo hábil para compreender as questões envolvidas no tratamento de seus dados e utilizar as garantias postas à sua disposição[220].

Solove argumenta, então, que para a proteção adequada frente a danos que emergem de uma estrutura social, de natureza sistêmica, é necessária uma abordagem diferente da simples reparação individual de danos e de mecanismos individuais de controle. É por esse motivo que Solove propõe que os atuais problemas de proteção de dados sejam tratados por meio de uma arquitetura de proteção, capaz de embutir no design dos sistemas que são utilizados para processamento de dados, garantias legais que permitam a criação de um ambiente de controle individual, social e institucional sobre o processamento de dados em massa[221].

A forma como a internet e, consequentemente, a economia de dados se desenvolveram na sociedade da informação concentrou poder nas mãos de grandes empresas de tecnologia, que acabam por controlar uma infinidade de dados relativos aos indivíduos. Estes não sabem quando, como e por quem estão sendo utilizados seus dados e são, assim, colocados em situação de extrema vulnerabilidade. Por esse motivo, as pessoas ficam impotentes frente aos significantes riscos decorrentes do tratamento de dados, como os advindos do *profiling* feito por grandes empresas de tecnologia.

Problemas dessa ordem, que emanam das condições ambientais de certo sistema, como os da economia digital, necessitam, segundo Solove, de soluções de arquitetura, ou seja, maneiras de se solucionar tais problemas por meio da alteração das próprias estruturas do sistema. Assim, a proteção de dados deve fomentar reformas na arquitetura dos sistemas tecnológicos que compassam as vidas dos cidadãos, o que possibilitará uma

---

[219] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 97.
[220] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? SCRIPTed - **Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.
[221] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 112.

reestruturação nos seus relacionamentos com as empresas que coletam e detêm seus dados pessoais.

A regulação pela arquitetura é mais proativa do que reativa, e visa criar estruturas que previnam a ocorrência dos danos, ao invés de buscar a reparação quando estes ocorrem. O relacionamento burocrático entre indivíduos e as grandes organizações deve ser o principal alvo da regulação, visando a redistribuição do poder de controle sobre a informação de forma a colocar os indivíduos e as empresas em um patamar mais próximo. Assim, resume Solove:

> A menos que o relacionamento da população com as burocracias seja colocado mais em pé de igualdade, garantir às pessoas direitos de propriedade padrão sobre a informação ou outras formas de controle da informação não irá proteger a privacidade adequadamente (...). Uma proteção da privacidade viável deve consistir em mais do que um conjunto de proteções para uma série de lesões isoladas. Em vez disso, a proteção da privacidade depende de uma arquitetura que estruture o poder, um marco regulatório que governe como a informação é disseminada[222].

Portanto, uma arquitetura de proteção, nos termos propostos por Solove visa estabelecer controles sobre as redes de processamento de dados de instituições e garantir às pessoas maior participação no uso de seus dados. O autor argumenta que o primeiro passo para as regulações relativas à proteção de dados deve ser redefinir o relacionamento entre indivíduos e os grandes processadores de dados. Estes por muito tempo não prestaram contas aos cidadãos, ainda que sejam aqueles os titulares dos dados que são utilizados como base para os diversos modelos de negócios digitais[223].

Como um dos componentes dessa arquitetura, o autor sugere, por exemplo, a criação de uma espécie de relação fiduciária dos controladores de dados com os titulares dos dados, para que, assim, passem a prezar pela segurança e pelo tratamento correto e justo dos dados pessoais, no melhor interesse do titular dos dados. O dever fiduciário, no contexto americano, normalmente se verifica nas relações em que se encontra uma disparidade de conhecimento entre as partes, sendo que uma está em posição de afetar significativamente a vida da outra, como ocorre, por exemplo, na relação entre advogado

---

[222] No original: "Unless people's relationships with bureaucracies are placed on more equal footing, affording people default property rights in information or other forms of information control will not adequately protect privacy (...) Viable protection of privacy must consist of more than a set of protections for a series of isolated injuries. Rather, the protection of privacy depends upon an architecture that structures power, a regulatory framework that governs how information is disseminated." SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 100.

[223] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 102.

e cliente, médico e paciente ou de corretora e investidores. Tratar a relação entre controladores e titulares dos dados como uma relação fiduciária significaria a imposição de deveres básicos de cuidado com o tratamento de dados pessoais e diversos direitos de acesso, informação e participação dos titulares no processamento de seus dados.

Outro exemplo de iniciativa que deve ser propagada, e que em vem contribuindo para o estabelecimento de uma arquitetura de controle e proteção de dados, citado por Solove, são os princípios de boas práticas para o processamento de dados estabelecidos nas "*Fair Information Practices*". Este documento explicitou um conjunto de princípios de boas práticas para o processamento de dados[224]. Princípios da mesma natureza foram estabelecidos ainda nas: "Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", de 1980, e na "Diretiva Europeia 95/46/EC Relativa ao Processamento de Dados Pessoais", de 1995. Até hoje, estes princípios formam a base dos recentes instrumentos regulatórios relativos à proteção de dados pessoais como GDPR e a LGPD.

Citam-se como exemplos de princípios de boa prática no processamento de dados pessoais, consolidados há algumas décadas e hoje presentes na LGDP[225]: i) princípio da finalidade: estabelece que todo tratamento de dados pessoais deve ter como fim propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; ii) princípio da adequação: deve haver compatibilidade do tratamento feito com as finalidades propostas e informadas ao titular, de acordo com o contexto do tratamento; iii) princípio da necessidade: impõe a limitação da coleta e 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; iv) princípio do livre acesso: garante, aos titulares, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; v) princípio da transparência: impõe o dever aos controladores de garantir aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

---

[224] USA. Department of Justice. The Privacy Act of 1974 5 U.S.C. § 552a (2012). Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Washington, DC, 01 maio 1974. Disponível em: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>. Acesso em: 25 nov. 2019.

[225] Princípios previstos no artigo 6º da LGPD.

Os princípios de boas práticas no tratamento de dados e informações focam em duas perspectivas: participação dos sujeitos titulares de dados e responsabilidade dos controladores. Segundo Solove, a arquitetura de controle deve se basear na noção de que a coleta e o uso de informações pessoais é uma atividade que carrega deveres e responsabilidades. Isso visa balancear a estrutura da economia da informação, de modo a permitir que os indivíduos participem significativamente da coleta e do uso de seus dados pessoais e que os controladores sejam responsáveis na utilização destes dados[226]. Assim, Solove argumenta que é necessário que a lei estabeleça medidas específicas de controle sobre as entidades que mantêm sistemas de processamento de dados pessoais para realização de suas atividades. Práticas mínimas de segurança da informação devem ser legalmente exigidas, bem como a responsabilização de controladores de dados pelos resultados danosos eventualmente propagados pelo tratamento realizado por eles.

Observa-se que as primeiras regulações acerca da proteção de dados pessoais estavam centradas quase exclusivamente no objetivo de conferir controle individual sobre os dados para o cidadão[227]. Apesar de terem propiciado certo aumento no poder dos indivíduos sobre seus dados dessa maneira, ainda persistiram muitas limitações e assimetrias informacionais ao controle individual, que não foram devidamente acessadas no decorrer dos anos. Ao invés, verificou-se o crescimento de algumas fragilidades com o sistema de controle individual, uma vez que exigências como a de obtenção de consentimento para a coleta e tratamento de dados passaram a funcionar como uma carta branca para realização de processamentos cada vez mais invasivos. Conforme argumenta Orla Linskey, é ingênuo considerar que, nos dias de hoje, os indivíduos possam exercer controle efetivo sobre seus dados pessoais por si mesmos[228].

Christophe Lazaro e Daniel Métayer[229] apontam que as concepções acerca da proteção de dados baseadas no controle individual se baseiam no pressuposto de existência de agentes racionais e autônomos em suas tomadas de decisão, portanto,

---

[226] SOLOVE, Daniel. **The digital person**: technology and privacy in the information age. Nova Iorque: New York University Press, 2004, p. 104.
[227] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? SCRIPTed - **Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.
[228] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p.257.
[229] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? SCRIPTed - **Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.

capazes de deliberar adequadamente aspectos relativos à proteção de suas informações pessoais. Porém, conforme os autores expõem, existem ao menos três diferentes fatores que diminuem a capacidade dos sujeitos de definirem, por si mesmos, preferências relativas ao fluxo de seus dados. A disponibilização de informações incompletas acerca das políticas de privacidade por parte de um provedor de serviços que requer a coleta de dados, ou a sua disponibilização em formato cuja leitura é impraticável é um dos principais fatores de limitação da tomada de decisões dos sujeitos. Além disso, a própria racionalidade humana é limitada, de modo que o sujeito não é capaz de processar todas as possíveis consequências do tratamento de seus dados em certo contexto. Por fim, incentivos psicológicos, como gratificações imediatas pela disponibilização dos dados podem levar indivíduos a compartilhar muito mais do que pretendiam, sendo a coleta ainda encoberta por uma ilusão de controle conferida por um consentimento viciado. Assim apontam Lazaro e Metayer:

> Segundo um número crescente de acadêmicos, tratar controle sobre dados pessoais somente como uma questão de negociação individual e autonomia das partes em arranjos contratuais negligencia os valores sociais subjacentes à privacidade. Levar o controle a sério implica entender as dimensões coletivas e multirelacionais que existem além das preferências subjetivas e estratégias individuais de ambos, os sujeitos dos dados e os controladores.[230]

Portanto, nos últimos anos se consolidou a ideia de que os problemas decorrentes da coleta e tratamento de dados pessoais não podem ser solucionados somente através do controle individual dos dados pessoais. Tal posicionamento se torna evidente e é essencial na análise de soluções para as questões de privacidade e discriminação ligadas ao *profiling*, que demandam um conjunto de esforços para serem devidamente regulamentadas. Porém, isso não significa que a ideia do controle individual deva ser completamente abandonada, pois continua a exercer papel instrumental para propiciar maior empoderamento de indivíduos frente às instituições que fazem o tratamento em massa de dados. Ocorre que as garantias de controle individual devem ser suportadas por outras estratégias regulatórias. Nesse sentido, Orla Linskey sugere que, no intuito de propiciar uma arquitetura de controle sobre dados pessoais verdadeiramente protetiva, é

[230] No original: "According to a growing number of scholars, treating control over personal data solely as a matter of individual negotiation and party autonomy in contracting arrangements neglects the more socially oriented values underlying privacy. Taking control seriously implies understanding the collective and multirelational dimensions that exist beyond the subjective preferences and individual strategies of both data subjects and controllers." LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? SCRIPTed - **Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.

necessário conjugar as abordagens de direitos individuais com novas abordagens organizacionais de controle[231].

Orla Linskey utiliza do princípio da transparência no processamento de dados para ilustrar essa necessária conjugação. A transparência aparece como princípio de boas práticas no tratamento de dados nas citadas diretivas da década de 80 e 90, mas, apesar de ser encorajada como um dos aspectos para reforçar o controle individual, ela sozinha não se mostra realmente efetiva. Isso porque, ainda que os indivíduos tenham acesso a informações pormenorizadas acerca do tratamento de seus dados, exercer efetivamente algum tipo de controle sobre o procedimento revela-se impraticável e cria um sentimento de impotência sobre os sujeitos. Segundo a autora: "Enquanto o conhecimento acerca da maneira como nossas identidades são construídas por meio do *profiling* pode encorajar que alguns indivíduos exerçam maior controle sobre seus dados pessoais, é mais provável que essa informação aliene e agrave uma sensação de desamparo sentida por outros."[232]

Assim, Orla Linskey sugere que a transparência deve ser sempre reforçada pela ideia complementar de *accountability*, isto é, de responsabilização e prestação de contas do tratamento. A *accountability* aparece como princípio da GDPR e na LGPD, não sendo tratada por regulações anteriores que envolviam a sistemática da proteção de dados. Foi previsto no novo regulamento europeu, por exemplo, um dever para o controlador de estabelecer proativamente em seus sistemas procedimentos que facilitem o exercício de direitos individuais pelos titulares dos dados processados, conforme o artigo 25 da norma. A GDPR exige, ainda, uma obrigação contínua dos controladores de dados de comprovarem que realizam suas atividades de acordo com a lei, por meio de relatórios de proteção de dados, previstos no artigo 30.

Orla Linskey aponta que outra forma de reforçar a arquitetura de controle sobre as informações pessoais é favorecer o uso de ações coletivas e aplicar sanções administrativas mais severas pela inobservância das leis, o que requer uma entidade fiscalizadora forte[233]. Nesse sentido, ressalta o que vem ocorrendo nos Estados Unidos. Ainda que o país não possua norma jurídica própria para tratar da proteção de dados

---

[231] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p.258.

[232] No original: "While knowledge of how our identities are constructed by *profiling* may enable some individuals to exercise more control over their personal data, it is more likely to alienate and compound the sense of helplessness felt by others.". LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p.258.

[233] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p. 261.

pessoais, avanços no tema têm sido feitos de maneira até mais incisiva do que na Europa, por meio da atuação institucional da FTC[234]. A autora aponta ainda que soluções pouco ortodoxas, como o fortalecimento de regras de direito concorrencial no âmbito das grandes empresas de tecnologia, evitando grandes monopólios sobre bases de dados, também pode fomentar um ambiente de proteção de dados pessoais mais próspero para os indivíduos[235].

Ainda, para o adequado tratamento do *profiling*, um dos fatores principais na criação da arquitetura de controle é a garantia legal do que vem sendo chamado de "governança de algoritmos". Conforme estudado nos capítulos anteriores, a retirada da participação humana em certos procedimentos pode oferecer alguns riscos, de maneira que Danilo Doneda e Virgílio Almeida[236] sugerem o desenvolvimento de instrumentos de governança, a fim de se aproveitar das utilidades econômicas e sociais dos novos sistemas computacionais de maneira segura. Para tanto, os autores reforçam a necessidade de se exigir legalmente, dos atores do setor privado, maior transparência e *accountability* de seus sistemas de tratamento de dados. Almeida e Doneda argumentam que a governança de algoritmos pode variar do ponto de vista estritamente legal e regulatório ao ponto de vista estritamente técnico. As exigências legais de *accountability* e transparência só serão possíveis de se realizar com o desenvolvimento de salvaguardas técnicas, que preservem a efetividade do sistema e reduzam seus efeitos indesejados.

A transparência deve lidar com o problema da opacidade dos algoritmos de formação de perfis. Doneda e Almeida destacam que esta opacidade não é somente técnica, mas decorre também de questões de direito como a proteção à propriedade intelectual, cuja compatibilização deve, então, ser buscada nos instrumentos normativos

---

[234] Neste ano, por exemplo, a agência americana aplicou multa de 170 milhões de dólares à Google devido à coleta indevida de dados de menores e celebrou acordo no valor de 5 bilhões de dólares com o Facebook, com a intenção de mudar na totalidade a política de coleta de dados da plataforma. SINGER, Natasha; CONGER, Kate. Google Is Fined $170 Million for Violating Children's Privacy on YouTube. **The New York Times**, Nova Iorque, 4 set. 2019. Disponível em: https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html. Acesso em: 25 nov. 2019. NUÑEZ, Michael. FTC Slaps Facebook With $5 Billion Fine, Forces New Privacy Controls. **Forbes**, Nova Iorque, 24 jul. 2019. Disponível em: https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#2e499a135668. Acesso em: 25 nov. 2019.

[235] LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press. 2015, p. 262.

[236] ALMEIDA, Virgilio; DONEDA, Danilo. What is Algorithm Governance? **IEEE-Internet Computing**, [S.l.], v. 20, p. 60-63, 2016. Disponível em: https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUyekJ2d. Acesso em: 20 nov. 2019.

que venham tratar do tema. A *accountability* é uma questão que foca em noções de responsabilidade, justiça e devido processo no uso de algoritmos. Por meio dela, visa-se definir questões como quem é o responsável por um sistema de *profiling*, se o desenvolvedor do sistema deve ser responsabilizado por possíveis danos causados ou se é responsável a empresa que o utiliza, dentre outras questões.

Destacam ainda que, como as bases de dados são centrais para o funcionamento adequado dos algoritmos, servindo como seu combustível, a governança de algoritmos necessita de cuidar do uso legal e ético dos dados, cuja coleta deve ser feita por meios legítimos e a informação que contêm deve ser correta, atualizada e, na medida do possível, sem viés.

Alguns instrumentos de governança têm sido previstos nas atuais legislações de proteção de dados, que exigem medidas de transparência e justiça aplicáveis aos algoritmos de proteção de dados, conforme será exposto no próximo tópico. Estes instrumentos dependem de recursos técnicos, que possam garantir que o procedimento de mineração de dados seja feito de forma consciente quanto a eventuais preconceitos e desigualdades presentes em bases de dados históricas e quanto a possíveis resultados enviesados do procedimento de formação de perfis. Assim, técnicas de auditoria dos sistemas começam a ser desenvolvidas para se garantir que a construção de sistemas de *profiling* seja feita de acordo com padrões técnicos legalmente exigidos[237]. Almeida e Doneda reforçam também a necessidade de órgãos de supervisão capazes de estruturar e implementar a governança de algoritmos. É importante, ainda, que empresas do setor privado adotem padrões éticos na construção de sistemas de *profiling* para seu próprio benefício, na medida em que uma política de conscientização de consumidores pode levá-los a deixar de utilizar sistemas que apresentam maiores riscos. Para a abordagem do setor privado funcionar sistematicamente, a organização interna das empresas deve absorver padrões que reflitam procedimentos de supervisão, revisão e adequação com as normas de proteção de dados.

Com isso em mente, é possível estabelecer algumas conclusões sobre limites legais ao *profiling* que devem ser adotados para propiciar a formatação de uma arquitetura de controle adequada sobre a prática. Em geral, as normas que regulam a proteção de

[237] CUSTERS, Bart; SCHERMER, Bart Willem. Responsibly Innovating Data Mining and Profiling Tools: A New Approach to Discrimination Sensitive and Privacy Sensitive Attribute. *In*: HOVEN, Van den J. *et al*, (ed.). **Responsible Innovation 1**. Holanda: Springer, 2014. cap. 19, p. 335-350. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047202. Acesso em: 10 nov. 2019.

dados devem prever medidas que objetivem garantir a privacidade e a igualdade entre os cidadãos cujos dados pessoais compõem a formação dos perfis. No intuito de mitigar os efeitos do *profiling*, estas normas devem visar a criação de mecanismos para o adequado controle sobre os fluxos de informação, feito pelos indivíduos titulares dos dados, por grupos e por instituições independentes, bem como criar deveres de tratamento responsável dos dados por todos os atores envolvidos no sistema. Isso tem sido feito por meio do estabelecimento de princípios de boas práticas para o processamento de dados, pelo estabelecimento de uma série de direitos individuais para os titulares dos dados, complementados por normas de transparência e *accountability* que visam estabelecer verdadeira governança sobre os algoritmos de definição de perfis.

Assim, foram apresentados alguns aspectos essenciais que compõem a arquitetura de proteção de dados adequada para enfrentar os problemas apresentados na prática do *profiling*. No próximo tópico serão analisadas as normas brasileira e europeia de proteção de dados pessoais, com objetivo de se identificar os limites legais impostos ao *profiling* nestes ordenamentos e em que medida contribuem para a construção de uma arquitetura de controle capaz de efetivamente acessar os problemas levantados nesta prática.

3.4 Os limites legais do *profiling* na GDPR e na LGPD

A sistematização de uma proteção jurídica sobre dados pessoais teve como um dos principais marcos mundiais a edição da Diretiva Europeia sobre Proteção de Dados, de 1995, em que princípios para o tratamento de dados e direitos individuais foram consolidados no documento. A Diretiva tinha como objetivo fornecer linhas comuns para que cada país do bloco editasse sua própria legislação acerca do tema. Porém, essa abordagem se mostrou pouco efetiva e criou uma dificuldade na compatibilização das diferentes normativas no bloco, acentuada pelo caráter transfronteiriço do tema[238]. No intuito de resolver esse problema, e frente aos recentes desenvolvimentos tecnológicos que aumentaram ainda mais a exposição e difusão de dados pessoais dos indivíduos, o Parlamento Europeu editou, em 2016, o Regulamento EU 2016/679, denominado *General Data Protection Regulation* (GDPR), legislação aplicável a todos os países do bloco de maneira uniforme, com princípios e regras vinculantes. O novo regulamento Europeu entrou em vigor em 25 de maio de 2018 e, devido a sua pretensão de

[238] KUBARLIJA, Jovan. **An Introduction to Internet Governance**, 7. ed, Genebra: DiploFoundation, 2016.

aplicabilidade para além do continente, levou diversas empresas ao redor do mundo a se movimentarem recentemente para adaptar seus procedimentos às novas regras.

Enquanto uma cultura jurídica de proteção de dados é fomentada na Europa há muitas décadas, no Brasil esse movimento é ainda incipiente. A proteção de dados possuía algumas manifestações limitadas e esparsas em diversos diplomas normativos até o ano de 2018, quando foi aprovada a primeira lei geral a tratar do tema.

Anteriormente, a Lei n. 8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor) trouxe em seus artigos 43 e 44 disposições acerca dos bancos de dados e cadastro de consumidores. Nesses artigos são garantidos aos consumidores alguns direitos de acesso aos dados armazenados por fornecedores bem como princípios de transparência e exatidão sobre os dados armazenados. A Lei n. 9.472 de 16 de julho de 1997 (Lei Geral de Telecomunicações) dispôs sobre o direito dos usuários de serviços de telecomunicação à privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço (artigo 3º, inciso IX). No artigo 72 trouxe, ainda, a necessidade de anuência expressa e específica do usuário para divulgação de informações a seu respeito e previu a possibilidade de divulgação sobre o uso dos serviços para terceiros, desde que não seja possível identificar o usuário. A Lei n. 12.527 de 18 de novembro de 2011 (Lei de Acesso à Informação) apresenta algumas regras acerca do cuidado com dados pessoais tratados em bancos de dados de entidades públicas, destacando-se os artigos 31 e 32. O artigo 31 impõe que o tratamento de informações pessoais seja feito de forma transparente e com respeito a intimidade, vida privada, honra, imagem, liberdades e garantias individuais. O artigo 32 prevê a responsabilização dos agentes públicos que violem as normas de tratamento de dados pessoais previstas no artigo anterior. Ainda, no âmbito da proteção ao crédito, foram adotados princípios consolidados internacionalmente para o tratamento responsável de dados pessoais quando editada a Lei n. 12.414 de 9 de junho de 2011 (Lei do Cadastro Positivo).

A temática da proteção de dados pessoais no ambiente digital teve maior avanço com o advento da Lei n. 12.965 de 23 de abril de 2014, o Marco Civil da Internet. Na época, a aprovação do texto legal tramitou com urgência no Congresso Nacional devido à pressão por uma resposta do governo ao escândalo internacional envolvendo agências

de segurança dos Estados Unidos da América, que monitoravam diversas autoridades estrangeiras, sendo o Brasil um dos principais alvos dos norte-americanos[239].

O Marco Civil da Internet estabeleceu como fundamento do uso da internet no Brasil o desenvolvimento da personalidade, conforme previsão do artigo 2º, inciso II, o que pode ser visto como uma primeira diretriz acerca de como o *profiling* deve ser desenvolvido nesse contexto. O descolamento comentado no tópico anterior, que se observa entre as ideias de privacidade e de proteção de dados pessoais, é evidenciado em parte no Marco Civil. Assim se observa pelo tratamento dado no artigo 3º da lei, que prevê de maneira apartada a privacidade e a proteção de dados pessoais como princípios do uso da internet no Brasil, nos incisos II e III, respectivamente. O artigo 7º, que dispõe sobre os direitos dos usuários da Internet, determina diversas garantias a respeito da privacidade e da proteção dos dados pessoais, consagrando alguns dos princípios estabelecidos internacionalmente sobre o tema. São garantidos: a inviolabilidade da intimidade e da vida privada (inciso I); o direito dos usuários a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades determinadas (inciso VIII); e a exigência de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (inciso IX). No artigo 8º ficou estabelecido que a garantia do direito à privacidade é uma condição para o pleno exercício do direito de acesso à internet, sendo nula cláusula contratual que a viole. Por fim, nos artigos 10 a 12 o legislador especificou certas proteções acerca da coleta e do tratamento de dados pessoais, estabelecendo possíveis sanções para seu descumprimento. Observa-se, no entanto, que em vários desses dispositivos, consta a expressão que os direitos e garantias relativos à proteção de dados pessoais serão exercidos "na forma da lei". Com isso, fica expresso no Marco Civil da Internet que aquele diploma não exaure o tema da proteção de dados pessoais, sendo necessária a edição de uma lei geral de proteção de dados que trouxesse a adequada regulação do tema.

Apesar de conterem algumas previsões aplicáveis ao *profiling*, por exigirem o tratamento responsável e transparente de dados pessoais, nenhuma das normativas anteriores tratava do tema de maneira manifesta. Em 2018, um conjunto de fatores

[239] LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. IN:LEMOS, Ronaldo; LEITE, Salomão George (Coord.). **O Marco civil da Internet**. São Paulo: Atlas. 2014. p. 4-11.

contribuiu para que o Brasil aprovasse, finalmente, sua Lei Geral de Proteção de Dados, alterando o paradigma normativo vigente. A entrada em vigor da GDPR no continente europeu trouxe a exigência de que países que desejem transacionar dados com a região possuam nível adequado de proteção de dados (previsão do artigo 45[240]). Além disso, qualquer empresa, ainda que situada fora do continente, mas que trate dados pessoais de usuários europeus, deve respeitar os padrões impostos pelo regulamento (artigo 3, item 2[241]). Ainda, o escândalo de vazamento de dados envolvendo o Facebook, promovido pela empresa Cambridge Analytica[242], voltou a colocar em foco no Brasil a necessidade de uma adequada proteção de dados pessoais nas redes. Por fim, a intenção de se alterar a Lei do Cadastro Positivo, para possibilitar a inclusão no sistema de qualquer consumidor, sem a necessidade que este promova seu próprio cadastro previamente, ampliou a necessidade de uma legislação que conferisse uma proteção de dados pessoais mais robusta aos consumidores antes de se efetivarem tais mudanças[243]. Assim, em 10 de julho de 2018, ocorreu a aprovação do PLC 53/2018 pelo Senado, após prévia aprovação pela Câmara no mês de maio. Em 14 de agosto, houve a sanção presidencial que deu origem à Lei n. 13.709 de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD). A lei previu prazo de vacância de 18 meses, restando sua vigência postergada para o ano de 2020.

É neste diploma normativo em que serão encontrados, hoje, limites legais incisivos aplicáveis ao processamento de dados por meio de *profiling*. A lei brasileira foi fortemente influenciada pelo novo regulamento Europeu, de modo que muitos de seus dispositivos se equivalem, observando-se algumas diferenças sutis. Isso se deu, em grande parte, devido à citada imposição, prevista na GDPR, de que países que pretendam

---

[240] Artigo 45 da GDPR: "Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado."

[241] Artigo 3, item 2, da GDPR: "O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União."

[242] BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**.** **BBC News**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml Acesso em: 10 nov. 2019.

[243] MARCHETTI, Bruno. Porque você deve se preocupar com a nova lei do Cadastro Positivo. **Vice**. Disponível em: https://www.vice.com/pt_br/article/qvxn95/dados-lei-cadastro-positivo . Acesso em: 09 nov. 2018.

estabelecer fluxo de dados com o continente estabelecessem um sistema jurídico de proteção de dados adequado aos padrões europeus. Desse modo, o estudo conjunto desses regulamentos se mostra importante, pois permite buscar as ideias que originaram a lei brasileira e melhor compreender as peculiaridades presentes no ordenamento pátrio.

De maneira geral, é notado que um dos principais avanços da GDPR em relação à Diretiva que a antecede é a criação de regras que buscam efetivar uma arquitetura de controle em diferentes níveis. Enquanto anteriormente se observava na diretiva uma tentativa de se criar uma espécie de "caixa de ferramentas de direitos individuais"[244], o novo regulamento europeu transfere com mais vigor o ônus dos efeitos negativos do tratamento de dados pessoais para os próprios responsáveis pelo tratamento e visa fortalecer mecanismos de controle para além do exercício de direitos individuais. Conforme visto no último tópico, esse tipo de abordagem é capaz de criar uma arquitetura de controle sobre dados pessoais que será mais efetiva na amenização dos efeitos negativos que decorrem do *profiling*. A LGPD tenta reproduzir essa mesma abordagem, de modo que ambas as regulações criam, ao menos em tese, um ambiente mais favorável para o uso responsável das técnicas de *profiling*.

Feito um breve histórico da regulação incidente sobre dados pessoais, cabe agora analisar os dispositivos vigentes que criam limites legais ao *profiling*. Inicialmente, retoma-se o conceito de *profiling* previsto no artigo 4º, item 4, do regulamento europeu, que não possui equivalente na lei brasileira:

> Definição de perfis: qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Com base nesse conceito fica explícito que práticas como a de *credit scoring* se encaixam como forma de *profiling*, pois envolvem o tratamento de dados pessoais para avaliar certo aspecto pessoal de uma pessoa singular, visando, nesse caso, prever um aspecto relacionado com sua situação econômica e de fiabilidade. Nas diretrizes do Grupo de Trabalho 29 sobre *profiling* e decisões automatizadas[245] foi destacado que a simples

---

[244] LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? SCRIPTed - **Journal of Law, Technology & Society**. Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015

[245] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated individual decision-making and *Profiling* for the purposes of Regulation 2016/679**. Bruxelas, 6 fev. 2018.

classificação de indivíduos em categorias não necessariamente leva ao *profiling*, que somente ocorrerá quando a classificação for feita com intuito de fazer uma previsão ou tirar uma conclusão acerca do indivíduo, como é o caso da sua pontuação de crédito, de avaliações para fins de seguros, decisões de recrutamento, dentre outras comentadas ao longo do presente trabalho. No considerando 72 do regulamento europeu explicitou-se que o *profiling* se submete às regras de governança sobre o processamento de dados estabelecidas, como as de observância aos princípios de tratamento e das bases legais necessárias para se iniciar o tratamento de dados. Ainda, foi previsto no artigo 70, item 1, alínea 'f'[246], que diretrizes especificas e detalhadas sobre a prática de *profiling* devem ser editadas pela autoridade de proteção de dados europeia após a entrada em vigor do regulamento.

Apesar de não constar expressamente do texto da LGPD, Rafael Zanatta afirma que a interpretação dos dispositivos presentes na lei brasileira que fazem referência à formação de perfis permitem a conceituação de perfilização: "enquanto processo automatizado de tratamento de dados que objetiva a análise e predição de comportamentos pessoais, profissionais, de consumo e de crédito"[247], ou seja, um conceito muito próximo do presente na GDPR. O termo "perfil" é citado nos artigos 12, parágrafo 2º e 20 da LGDP. No primeiro dispositivo, há a previsão de que dados anonimizados, que em tese não são dados pessoais por não identificarem um sujeito, serão considerados dados pessoais "quando utilizados para formação do perfil comportamental de determinada pessoa natural". Isso permite que o sujeito exerça todos os direitos previstos na lei ainda que seu perfil seja constituído por dados anonimizados.

Por sua vez, o artigo 20 confere ao titular dos dados direito a "revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional,

---

Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 2 jul. 2019.

[246] Artigo 70, item 1, da GDPR: "O Comité assegura a aplicação coerente do presente regulamento. Para o efeito, o Comité exerce, por iniciativa própria ou, nos casos pertinentes, a pedido da Comissão, as seguintes atividades: (...) (f) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número, para definir mais concretamente os critérios e condições aplicáveis às decisões baseadas na definição de perfis, nos termos do artigo 22.o, n.o 2."

[247] ZANATTA, Rafael A. F. Perfilização, Discriminação e Direitos: Do Código de Defesa do Consumidor à Lei Geral de Proteção de dados pessoais. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/stats>. Acesso em: 31 ago. 2019.

de consumo e de crédito ou os aspectos de sua personalidade". Portanto, não se observa qualquer prejuízo na lei brasileira decorrente da ausência de um conceito para o *profiling*, uma vez que as situações de aplicação dos princípios, regras e direitos de proteção sobre dados pessoais serão, basicamente, as mesmas previstas na GDPR: quando houver tratamento automatizado de dados que identifiquem um sujeito, formando um perfil para tomada de decisão que afete seus interesses.

Quanto aos princípios que devem ser observados para o processamento de dados que incorra em *profiling*, destacam-se o da transparência do processamento (artigo 6º, inciso VI da LGPD e 5º, item 1, alínea 'a', da GDPR) que garante aos titulares dos dados pessoais informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; o da não discriminação (artigo 6º, inciso IX da LGPD) que visa impossibilitar a realização de tratamentos para fins discriminatórios ilícitos ou abusivos; e o da responsabilização e prestação de contas (artigo 6º, inciso X da LGPD e 5º, item 2 da GDPR).

O princípio da transparência no âmbito da GDPR é ampliado no contexto do *profiling*, sendo estabelecida obrigação para o controlador de dados de informar ao titular, de maneira destacada, quando o tratamento de dados envolver a definição de perfis e as consequências que poderão advir desse tratamento, conforme disposto no artigo 13, item 2, alínea 'f'. Quanto ao princípio da não discriminação, explícito na lei brasileira, não foi tratado expressamente no texto da GDPR. Porém, o regulamento europeu prevê que o tratamento de dados deve ser legítimo e justo, conforme artigo 5º, item 1, alínea 'a'. Segundo as diretrizes do Grupo de Trabalho 29, é essa previsão que garante a vedação ao tratamento discriminatório por meio do *profiling*. O Grupo utiliza como exemplo de tratamento injusto certas formas discriminatórias de análise de crédito[248]. Assim, analisaram caso real em que houve a oferta de crédito em condições excessivamente onerosas para pessoas em situação de vulnerabilidade financeira, com a sua classificação em grupos com denominações pejorativas como "Rurais que mal-mal sobrevivem"[249].

---

[248] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated individual decision-making and *Profiling* for the purposes of Regulation 2016/679**. Bruxelas, 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 2 jul. 2019.

[249] O exemplo dado, no original: "A data broker sells consumer profiles to financial companies without consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Tough Start: Young Single Parents,") or "score" them, focusing on consumers' financial vulnerability. The financial companies offer these consumers payday loans and other "non-traditional" financial services (high-cost loans and other financially risky products)". ARTICLE 29 DATA PROTECTION WORKING

Entre os artigos 17 e 22 da LGPD são estabelecidos os direitos individuais dos titulares dos dados pessoais. Nesses artigos se encontram os principais mecanismos para que a pessoa natural possa exercer o controle sobre suas informações, de forma a dirigir a construção de sua esfera privada. Nesse sentido, o artigo 18 garante os chamados "direitos de acesso" que permitem que o titular dos dados obtenha do controlador todo tipo de informação a seu respeito que seja objeto de coleta, armazenamento e tratamento. Esse artigo garante também a possibilidade de eliminação e correção dos dados pelo seu titular, bem como o direito de revogação, a qualquer tempo, do consentimento manifestado para a coleta. Aqui, é preciso destacar que o consentimento não é a única base legítima para processamento de dados pessoais. Atualmente, na LGPD, o artigo 7º lista 10 hipóteses em que dados pessoais podem ser legalmente coletados e tratados. Por exemplo, é possível o tratamento de dados pessoais, mesmo que sem consentimento, para finalidades de proteção ao crédito, conforme previsto no inciso X do artigo citado.

O artigo 19 da LGPD garante a transparência e legibilidade das informações prestadas pelo controlador acerca do procedimento de tratamento de dados do titular. No âmbito do *profiling*, esses direitos são essenciais para que, por exemplo, o indivíduo possa promover a fidedignidade das informações detidas por instituições financeiras com a sua real situação econômica, de forma que a pontuação de crédito a ele atribuída seja justa.

De modo geral, os direitos de acesso se assemelham na lei brasileira e no regulamento europeu. Uma especificidade das regras de proteção de dados aplicadas ao *profiling*, presente na GDPR, está na possibilidade de objeção imediata a esse tipo de tratamento de dados quando feito para fins de publicidade direcionada. Nesse sentido, o artigo 21, item 2, do regulamento, estabelece que quando os dados pessoais forem utilizados para marketing direto, o titular poderá fazer cessar o tratamento dos dados que vise a constituição do seu perfil nesse contexto. Esse direito, conforme previsão do artigo 21, item 4, deve ser explicitamente levado à atenção do titular dos dados e ser apresentado de modo claro e distinguido de quaisquer outras informações na primeira comunicação entre o controlador dos dados e seu titular. Tal previsão não possui equivalente na LGPD, mas se mostra como uma maneira simples de facilitar o exercício da autonomia individual no controle de fluxos de dados, com possibilidade de diminuir os excessos advindos do

---

PARTY. **Guidelines on Automated individual decision-making and *Profiling* for the purposes of Regulation 2016/679**. Bruxelas, 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 2 jul. 2019.

profiling no contexto de anúncios online. Na lei brasileira, o direito de oposição ao tratamento só poderá ser exercido pelo titular dos dados quando tiver sido iniciado sem o seu consentimento e em descumprimento de outras bases legais legítimas, conforme disposição do artigo 18, parágrafo 2º.

Discute-se, ainda, dois direitos individuais relacionados ao *profiling* que possuem, estreita relação. Trata-se do "direito a não ser submetido a decisões totalmente automatizadas"[250] e do "direito à explicação"[251].

O primeiro direito constitui uma regra geral de proibição ao *profiling*, quando feito de maneira totalmente automatizada, constante da GDPR em seu artigo 22, item 1, que assim prevê: "O titular dos dados tem 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". A proibição não se aplica em três casos: quando o *profiling* for necessário para celebração ou execução de um contrato entre o controlador e o titular dos dados; quando feito com consentimento explícito do titular; ou para casos que a União Europeia ou o Estado Membro autorize, desde que haja previsão de medidas que resguardem outros direitos do titular (artigo 22, item 2.).

Nos casos em que o *profiling* é autorizado, a GDPR prevê, no item 3 do mesmo artigo, que haja a possibilidade de revisão da decisão que dele resulte. Assim, exige-se que o responsável pelo tratamento aplique medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados, devendo possibilitar, no mínimo, o direito de o titular obter intervenção humana por parte do responsável, de manifestar o seu ponto de vista e de contestar a decisão. Trata-se da consagração, no direito comunitário europeu, do paradigma chamado de "*human in the loop*", pelo qual se entende a necessidade de sempre haver um humano responsável pela tomada de decisões obtidas com auxílio de meios automatizados[252].

---

[250] LOPES, G.F.P. O direito à explicação de decisões automatizadas no âmbito do regulamento geral de proteção de dados da união europeia. *In*: SOARES, F. M.; DE OLIVEIRA, T.B.G.; DA MATA, P. C. O. A. (org.). **Ciência, Tecnologia e Inovação**: Políticas & Leis. Florianopolis: Tribo Ilha, 2019. p. 235-259. Disponível em: https://www.observalei.net.br/ambito-do-observatorio/ciencia-tecnologia-e-inovacao-politicas-leis. Acesso em: 11 dez. 2019.

[251] GOODMAN, Bryce, FLAXMAN, Seth. EU Regulations on Algorithmic Decision-Making and a "right to Explanation", **AI Magazine**, Oxford, vol 38, n. 3, 2017.

[252] DINIZ, T. D. M.; DE OLIVEIRA, T. B. G. Decisões automatizadas por máquinas e o humano no loop: cenários discriminatórios, vieses cognitivos e regulação normativa. *In*: SOARES, F. M.; DE OLIVEIRA, T.B.G.; DA MATA, P. C. O. A. (org.). **Ciência, Tecnologia e Inovação**: Políticas & Leis. Florianopolis:

O tratamento de dados considerados sensíveis[253] é, em regra, proibido no âmbito da GDPR, salvo 10 hipóteses previstas no artigo 9º, item 2 do regulamento. Porém, o uso de dados sensíveis para tomada de decisões com base em *profiling* é ainda mais limitado, de modo que só pode ser feito em duas hipóteses: com consentimento explícito do titular e somente para uma finalidade específica, podendo a União ou Estado Membro prever hipóteses em que nem o consentimento poderá afastar a proibição; ou quando o tratamento for necessário por motivos de interesse público importante exigido pelo direito da União ou do Estado Membro. É o que se depreende do artigo 22, item 4 do regulamento.

Não se optou, na LGPD, por se criar uma regra geral de proibição ao *profiling*, consubstanciada em um "direito a não ser submetido a decisões totalmente automatizadas" nos moldes da GDPR. A proibição expressa ao *profiling* se deu somente em um caso específico, de tratamento de dado sensível[254] na área da saúde. O artigo 11, parágrafo 5º, incluído pela Lei n. 13.853 de 8 de julho de 2019, proíbe que o *profiling* seja realizado por operadoras de planos privados de assistência à saúde, nos seguintes termos: "É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários".

Para os demais casos, em que não há restrição de se iniciar o *profiling*, foi prevista a possibilidade de revisão das decisões que dele decorrem, nos termos do artigo 20 da LGPD, em consonância com o previsto na GDPR. Nesse artigo foi garantido que, quando houver tratamento automatizado de dados pessoais, que afete o interesse do titular dos dados, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, o titular poderá solicitar a revisão da decisão. Originalmente houve previsão de que a revisão deveria ser feita por uma pessoa natural, adotando-se a mesma ideia característica da GDPR, que consagrou o

---

Tribo Ilha, 2019. p. 191-214. Disponível em: https://www.observalei.net.br/ambito-do-observatorio/ciencia-tecnologia-e-inovacao-politicas-leis. Acesso em: 11 dez. 2019.

[253] São dados sensíveis na GDPR, conforme artigo 9º, item 1, os que: "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.".

[254] A lei brasileira também limita as hipóteses em que é legítimo o tratamento de dados considerados sensíveis. São considerados dados sensíveis, segundo o artigo 5º, inciso II: 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.

"*human in the loop*". Porém, tal exigência foi vetada, por ter sido considerada restritiva ao desenvolvimento de modelos de negócio atuais[255], sendo nova redação conferida ao artigo 20 da lei.

Para que os titulares dos dados possam efetivamente contestar uma decisão tomada com base em seu perfil, é necessário que ele entenda as razões por detrás daquela decisão. Assim, vem sendo discutido o chamado "direito à explicação", que se refere à possibilidade de o titular dos dados demandar informações pertinentes acerca das decisões automatizadas feitas com base em seus dados, quando lhe afetem um interesse de forma significativa[256]. Conforme visto, o artigo 22, item 3, do regulamento europeu, estabelece que, havendo uma decisão baseada unicamente no processamento automatizado dos dados de um sujeito, o responsável pelo tratamento dos dados deve implementar medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados.

Goodman e Flaxman apontam que uma das medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do titular dos dados seria fornecer a ele uma explicação sobre as razões que levaram à decisão tomada. Isso seria uma garantia proveniente dos direitos de acesso, que exigem que o controlador dos dados informe ao titular sobre a existência de decisões automatizadas, com informações úteis relativas à lógica subjacente a ela, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados, previsão contida no artigo 13, item 1, alínea 'f' da GDPR[257]. As informações úteis sobre a lógica subjacente das decisões automatizadas constituiriam o que os autores consideram uma explicação acerca da decisão automatizada.

---

[255] Razões do veto: "A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.". Disponpível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm . Acesso em 11 de nov. de 2019.

[256] GOODMAN, Bryce, FLAXMAN, Seth. EU Regulations on Algorithmic Decision-Making and a "right to Explanation", **AI Magazine**, Oxford, vol 38, n. 3, 2017.

[257] GOODMAN, Bryce, FLAXMAN, Seth. EU Regulations on Algorithmic Decision-Making and a "right to Explanation", **AI Magazine**, Oxford, vol 38, n. 3, 2017.

Porém, a existência de tal direito é contestada no âmbito do regulamento europeu[258], de forma que alguns autores argumentam que as informações úteis garantidas pelos direitos de acesso não constituem uma verdadeira explicação de todo o modelo que envolve o sistema de tratamento de dados que gera a decisão, mas de informações básicas que podem ser propriamente limitadas, visando, principalmente a garantia de segredos industriais. Certo é que o termo "explicação" só é expressamente mencionado no considerando 71 do regulamento. Ainda que se considerasse existente esse direito na norma europeia, ele possuiria sérias limitações[259]. Isso porque o regulamento prevê sua aplicação em decisão tomada "exclusivamente com base no tratamento automatizado de dados" o que permitiria que uma atuação humana, ainda que meramente nominativa, excluísse a possibilidade de se exigir uma explicação da decisão. Ainda que se interpretasse que não é qualquer atuação humana que descaracteriza uma decisão de ser "exclusivamente automatizada", seria necessário estabelecer o que é uma atuação humana significativa para afastar esse direito.

Além disso, conforme o artigo 22, o usuário só teria direito a salvaguardas contra decisões que produzam efeitos legais sobre ele ou que lhe afetem significativamente. Assim a norma demandaria grande esforço interpretativo para saber que efeitos seriam esses que fazem nascer o direito a explicação. O considerando 71 do regulamento fornece um caminho para interpretação, ao usar como exemplos de decisões com efeitos significativos a recusa automática de um pedido de crédito por via eletrônica. Nesse contexto, a pronta recusa do crédito é exemplo ilustrativo claro de decisão automatizada. Porém, caso seja feito o procedimento de *credit scoring* como subsídio para que um agente humano tome a decisão quanto à concessão do crédito, o titular dos dados não possuiria, em tese, mecanismo legal para buscar entender ou contestar a forma pela qual sua pontuação foi calculada.

No âmbito da legislação brasileira, Renato Leite Monteiro afirma que o direito à explicação já existia, justamente no setor de análise de crédito, garantida por uma aplicação conjunta de dispositivos do Código de Defesa do Consumidor (artigo 43,

---

[258] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017.

[259] EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. **Duke L. & Tech. Rev.**, v. 16, p. 18, 2017.

parágrafo 6º[260]) e da Lei do Cadastro Positivo (artigo 5º, inciso IV[261]). Segundo o autor, a LGPD amplia o escopo desse direito para outros setores que se utilizam de técnicas de *profiling* e de decisões automatizadas. O artigo 20, parágrafo 1º da LGPD dispõe que "O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial".

Observa-se, porém, que há também na LGPD a limitação quanto à restrição do direito, por ser aplicável somente a decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, o que abre espaço para que intervenções humanas meramente formais afastem essa previsão. Por outro lado, a LGDP avança ao colocar importante contrapartida na limitação da explicação ao segredo comercial e industrial, prevendo no parágrafo 2º do artigo 20 que " Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais".

Até o momento, os dispositivos analisados visam limitar a prática de *profiling* por meio de direitos individuais que o responsável pelo tratamento dos dados deve garantir ao titular. Lilian Edwards e Michael Veale criticam o foco que tem sido dado a estes direitos nas discussões acerca dos mecanismos previstos na GDPR para mitigação dos efeitos indesejados de decisões automatizadas, como as tomadas com base em *profiling*[262]. Nos termos argumentados no tópico anterior, tão importante quanto os direitos individuais, são as mudanças estruturais que envolvem formas coletivas de controle, fiscalização por instituições e o desenvolvimento de novas tecnologias capazes de lidar com as garantias legais. Conforme Bart van der Sloot e Sascha can Schendel demonstram, no contexto do *Big Data*, muitas vezes o foco está além do indivíduo, se voltando para as informações agregadas, com padrões gerais e perfis grupais[263]. A categorização de dados sensíveis, da qual se espera que informações potencialmente

---

[260] Artigo 43, parágrafo 6º, do CDC: Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[261] Artigo 5º da Lei do Cadastro Positivo: São direitos do cadastrado: IV- conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial.

[262] EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. **Duke L. & Tech. Rev.**, v. 16, p. 18, 2017.

[263] SLOOT, Bart van der; SCHENDEL; Sacha van. Ten questions for future regulation of big data: a comparative and empirical legal study. **Journal of Intellectual Property, Information Technology and Eletronic Commerce Law,** v.7, n.2, o.110-145, 2016.

discriminatórias sejam retiradas das análises de dados, também tem a funcionalidade prejudicada pela facilidade de extração de inferências sensíveis com o cruzamento de grandes bases de dados[264]. Os direitos à revisão de decisão automatizada e à explicação, muito celebrados como forma de empoderar os titulares de dados a exercerem maior controle sobre o processamento e a tomada de decisões que lhe afetem, encontram sérias limitações para serem viáveis, sendo tanto limitações inerentes à iniciativa individual quanto às ordem técnica afetas aos sistemas de *profiling*[265].

É notória a existência de uma assimetria entre consumidores e as instituições responsáveis pelo processamento de dados em massa. Essa assimetria se manifesta em diversas ordens: informacional, financeira e até política. Assim, controles individuais tendem a ser muito pouco efetivos, conforme se argumentou no tópico anterior. Nesse sentido, é possível identificar que a GDPR teve como intuito buscar meios técnicos e organizacionais de se amenizar o potencial lesivo da automatização da tomada de decisões com base no *profiling*. Isso se constata com o seguinte trecho do considerando 71 do regulamento:

> A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

Disposições presentes nas leis de proteção de dados que não tratam de direitos individuais, mas tentam fornecer uma estrutura para o desenvolvimento de melhores práticas de proteção de dados e *design* de sistemas menos invasivos por natureza, são essenciais para se criar uma verdadeira arquitetura de controle capaz de solucionar o problema da burocracia no processamento de dados, nos termos definidos por Daniel Solove. Nesse sentido, citam-se as disposições da GDPR que impõe a elaboração de

---

[264] ANDRADE, D. P. *Credit scoring* na era do big data: desafios tecnológicos no direito brasileiro. In: PARENTONI, L.; GONTIJO, B. M.; LIMA, H. C.Z. **Direito, Tecnologia e Inovação**. Belo Horizonte: D'Placido, 2018. cap. 2.3, p. 246-267. v. I.

[265] EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. **Duke L. & Tech. Rev.**, v. 16, p. 18, 2017.

Avaliações de Impacto de Proteção de Dados (DPIAs) e o sistema de certificações e códigos de conduta relativas à proteção de dados[266].

O artigo 35 da GDPR cria uma sistemática de produção de relatórios, por parte dos responsáveis por tratamentos de dados, que avaliem o impacto do uso de certas tecnologias sobre a proteção de dados pessoais, quando oferecerem elevados riscos a direitos e liberdades de indivíduos. Segundo o item 3, alínea 'a' do mesmo artigo, esse relatório será obrigatório para aqueles que pretendam se utilizar da definição de perfis no âmbito de suas atividades[267]. Na LGPD, por outro lado, não foram previamente delimitados casos em que relatório semelhante será exigível, ficando a cargo da autoridade nacional de proteção de dados solicitar esse instrumento quando entender necessário, conforme se depreende do artigo 38 da lei[268]. Por meio deste mecanismo, seria possível, na elaboração e análise dos relatórios, identificar potenciais riscos para a privacidade e igualdade dos indivíduos submetidos ao *profiling*, de modo a facilitar e direcionar a busca de soluções técnicas que mitiguem esse tipo de impacto.

A GDPR fomenta, entre os artigos 41 e 43, a elaboração de códigos de conduta de boas práticas em proteção de dados e a construção de procedimentos de certificação em proteção de dados, que servirão para efeito de comprovação de conformidade com a lei das operações de um responsável pelo tratamento de dados. Para obter a certificação, os responsáveis pelo tratamento devem assumir compromissos vinculativos, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, que imponham a aplicação das garantias adequadas ao tratamento de dados, como as relativas

---

[266] EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. **Duke L. & Tech. Rev.**, v. 16, p. 18, 2017.

[267] Artigo 35, item 1 e item 3, alínea 'a', da GDPR: "1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. (...) 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.o 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar".

[268] Artigo 38 da LGPD: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único: Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

aos direitos dos titulares. Para obter essa certificação, o controlador dará todo acesso às suas atividades de tratamento para uma entidade certificadora e o certificado deverá ser renovado periodicamente. Trata-se de uma maneira de incentivar que os próprios atores do mercado busquem aderência às normas de proteção de dados e assim formar um ambiente que preze pela segurança e pela responsabilidade dos tratamentos. Estas disposições devem contribuir na construção de sistemas de *profiling* menos intrusivos, mais auditáveis, e que permitam a identificação tempestiva de eventuais casos de invasão à privacidade ou de discriminação indireta.

Na Lei brasileira, destaca-se como iniciativa da mesma natureza o previsto no artigo 50 que abre a possibilidade para que controladores estabeleçam regras de boas práticas e governança no tratamento de dados pessoais. Essas regras deverão conter, por exemplo, normas de segurança, padrões técnicos, ações educativas e mecanismos internos de supervisão e de mitigação de riscos por parte dos responsáveis. A possibilidade de a autoridade nacional de proteção de dados determinar a realização de auditorias para identificação de práticas discriminatórias em sistemas de *profiling*, conforme definido no artigo 20, parágrafo segundo, contribui, ainda, para a criação de uma arquitetura protetiva. Por fim, ressalta-se o fortalecimento de controles coletivos na medida em que o artigo 22 garante que a defesa dos direitos e interesses dos cidadãos previstos na lei poderão ser defendidos em juízo por meio instrumentos de tutela coletiva.

Em conclusão, observa-se que ambas regulações acerca da proteção de dados pessoais apresentam um amplo espectro de previsões que devem ser observadas pelo setor privado no caso de tratamentos de dados que envolva o *profiling*. Foram previstos princípios que devem reger a atividade, limites referentes ao tratamento de dados sensíveis, direitos individuais que garantam ao titular dos dados maior controle sobre suas informações e previsões complementares que visam criar um ambiente de tratamento de dados mais responsável e menos intrusivo. A GDPR, no geral, atentou-se ao *profiling* de maneira mais específica e restritiva, definindo seu conceito legal e prevendo uma regra geral de proibição a esse tipo de tratamento, além de diretrizes interpretativas diversas em seus considerandos. A LGPD faz poucas menções diretas à definição de perfis, optando por deixar a prática submetida, em regra, ao mesmo sistema de proteção de dados aplicável a outras formas de tratamento. De qualquer forma, ambas as legislações vão além da concessão de direitos individuais e visam criar, efetivamente, uma estrutura de controle sobre práticas invasivas de tratamento de dados, como as decorrentes de

profiling. Assim, espera-se que caso se verifique, de fato, a observância pelos agentes do setor privado das normas legais que limitam o *profiling*, será possível a garantia do direito à privacidade e à igualdade no atual contexto de burocracia, uma vez que se estabeleceu uma arquitetura de controle de diversos níveis capaz de alterar as estruturas dos fluxos de informação.

CONCLUSÃO

O desenvolvimento e a difusão das tecnologias digitais nos últimos anos resultam em uma das maiores mudanças nas relações econômicas e sociais observadas na história recente. O termo “Sociedade da Informação” vem sendo utilizado para referir a tais mudanças, refletindo uma era em que a informação flui em altíssima velocidade e assume valores sociais e econômicos fundamentais. Esse novo paradigma se baseia em um insumo chave, de disponibilidade universal, que gera uma série de inovações técnicas e organizacionais inter-relacionadas. Na “Sociedade da Informação”, os dados assumem esse papel de insumo chave, sendo a matéria prima que move as principais tecnologias modernas.

Hoje, praticamente toda a atividade dos usuários na internet gera uma espécie de “rastro”, que pode ser convertido e armazenado como mais informação por uma série de agentes. É a partir da coleta massificada de dados de usuários das novas tecnologias da informação, no contexto de uma “Sociedade da Informação”, que o *profiling*, se desenvolve e se difunde, principalmente no setor privado.

Somos hoje confrontados com o surgimento de verdadeiros dossiês digitais, que formam uma coleção detalhada de dados acerca de um indivíduo. O desenvolvimento da quarta revolução industrial permite que ocorra datificação em campos que antes não podiam ser explorados, de modo que muitos aspectos da vida cotidiana passam a ser mensurados para fins comerciais. Assim, os dossiês pessoais se tornam muito extensos e são usados de maneira que afeta profundamente a vida das pessoas, sem que essas tenham poder para exercer alguma influência no rumo de suas informações.

A análise de dados em massa permite o reconhecimento de correlações que antes não poderiam ser vistas. Por meio do *Big Data*, padrões são descobertos que permitem, com alto grau de precisão, prever que certo evento ocorrerá. Porém, as correlações, por si só, não dizem o porquê da ocorrência de certo fenômeno. Estabelecer correlações sem conhecimento de causas é especialmente problemático quando se adentra no território de análises de comportamentos humanos. Formular previsões acerca de como certa pessoa irá agir e tomar decisões que afetem essa pessoa com base nas previsões feitas, sem que se saiba o porquê de se ter obtido aquele resultado, acaba por ocasionar sérios riscos envolvendo a esfera privada dos indivíduos. Inicialmente, a análise de grandes quantidades comportamentais de certa pessoa pode revelar aspectos de sua vida que, em

nenhum momento, essa pessoa teve intenção de revelar. Além disso, as correlações estabelecidas podem refletir padrões históricos de discriminação de certo grupo ou classe social, em razão de certo viés presente na base de dados utilizada.

A busca incessante por maior quantidade de dados cria uma lógica de mercado que acaba por colocar a maioria das pessoas que se utilizam de tecnologias digitais num constante estado de vigilância em suas relações privadas. A própria experiência humana se torna objeto para práticas comerciais de extração, previsão e vendas. O grande escopo de vigilância exercida nas atividades do meio digital só começa a ser bem compreendido após os serviços oferecidos por grandes atores estarem profundamente integrados na vida diária das pessoas, de forma que elas achem tais práticas aceitáveis tendo em vista o serviço que utilizam. Desse modo, elas se veem forçadas a escolher entre abrir mão do controle sobre os seus dados pessoais, e consequentemente, sobre seus comportamentos e desejos atuais e futuros, em troca de serviços que consideram essenciais para a vida conectada.

O discurso da vigilância, apesar de inquietante, por muitas vezes não ataca problemas centrais da coleta e processamento massivo de informações que não são consideradas íntimas, ou cuja revelação não traz constrangimento. A maior parte dos dados coletados não representam, por si só, uma verdadeira intrusão à vida íntima. Muitos não se sentem inibidos em compartilhar seus hábitos de consumo e outras características de seu estilo de vida que hoje são capturados no uso de redes sociais e outros aplicativos. Somente apontar que grandes empresas possuem grandes quantidades de informações acerca do indivíduo e estão o tempo todo coletando mais informações desse tipo pode gerar desconforto, mas não explica como isso afeta diretamente a vida das pessoas.

Conforme demonstrado a partir das ideias de Daniel Solove, o foco das discussões deve ser a burocracia presente nas instituições que tomam decisões sobre a vida dos indivíduos como base em seus dados pessoais. Por ser esse procedimento burocrático, ele se torna extremamente desumanizado pois visa eliminar qualquer elemento não quantificável, ou intangível, do processo de tomada de decisões e, por isso, frequentemente não é capaz de atender às necessidades especiais de um particular. Outro problema da burocracia é sua falta de transparência para o público, de forma a dificultar o escrutínio das decisões. Além disso, burocracias costumam ter pouco cuidado na maneira com que usam informações pessoais. Os grandes atores do setor privado que se utilizam da análise de dados não necessariamente coagem ou punem pessoas, mas criam

um sentimento de desempoderamento e deixam-nas vulneráveis, retirando totalmente seu controle sobre as informações pessoais e sobre aspectos definidores de suas vidas. Assim é possível compreender melhor os problemas de se viver em mundo onde terceiros estabelecem, unilateralmente, perfis pessoais que visam capturar aspectos íntimos da personalidade de uma pessoa.

A prática de *profiling* é um dos principais exemplos de análise de dados burocráticas com a qual o direito deve lidar nos dias de hoje. Antes limitada a investigações policiais e a pesquisas de marketing, com o desenvolvimento das técnicas de coleta e tratamento de dados, a definição de perfis foi facilitada e se tornou útil em diversas áreas.

O *profiling* se refere à formação de correlações estatísticas, normalmente de natureza preditiva, acerca de características de indivíduos ou grupos. O *profiling* automatizado é resultado do processo de mineração de dados que permite o estabelecimento de previsões baseadas no comportamento passado observado. Seus principais usos são para individualização, avaliação de risco e avaliação de oportunidades. Grande parte da utilização do *profiling* se refere ao chamado *profiling* comportamental. Esse tipo de procedimento pode ser definido como o estudo de padrões de comportamento e o agrupamento de usuário de acordo com o comportamento exibido. Assim, o profiling é feito partir da análise automatizada de grandes quantidades dados e com objetivo de se tomar uma ação em relação ao sujeito perfilado (enviar um anúncio direcionado, aprovar ou negar a concessão de crédito, personalizar o serviço oferecido pela organização que conduz o *profiling*, dentre outras).

Recursos de mineração de dados, potencializados pelo *Big Data* tornam essa prática mais acessível, confiável e economicamente lucrativa. Observam-se ganhos importantes com seu uso, principalmente em termos de eficiência e eficácia de análises preditivas. Porém, o uso descuidado e sem observância de limites legais pode significar importantes efeitos prejudiciais à vida privada dos indivíduos.

Muitos dos usos do *profiling*, a princípio, aparentam ser aceitáveis, mas podem ser realizados de maneira injusta, insensível ou discriminatória. O *profiling* é uma prática intrinsecamente intrusiva, ainda mais quando utilizado rotineiramente, nos mais variados contextos. O potencial presente nas técnicas de *profiling* encoraja a crescente coleta de dados comportamentais, a fim de se conhecer a fundo os hábitos das pessoas, mesmo que essas não desejem tamanha exposição. Ainda que haja compartilhamento voluntário de

dados por partes dos indivíduos, há uma legítima expectativa sobre os usos que poderão ser feitos dos dados, o que a prática de *profiling* muitas vezes extrapola.

Ao mesmo tempo em que é possível se formar perfis que abrangem boa parte de nossas vidas, de forma a invadir a privacidade dos indivíduos, as limitações desses perfis também são problemáticas. Isso porque os perfis falham em capturar as pessoas em sua essência e por vezes distorcem quem elas são, mas ainda assim são usados para decidir aspectos relevantes de suas vidas.

Além disso, ao pré-julgar o comportamento futuro de consumidores, as empresas acabam por ignorar certos tipos de pessoas de modo a limitar seu acesso à informação acerca de produtos e serviços. O recurso aos perfis pode ocasionar a discriminação de pessoas que não correspondem a um modelo geral, de forma a acentuar a estigmatização de comportamentos desviantes e a penalização de minorias, criando um obstáculo ao pleno desenvolvimento da personalidade individual, cerceada por perfis historicamente determinados.

Os métodos de definição de perfis utilizam fatos passados para fazer uma previsão. Assim, empresas são capazes de tomar diversas decisões relativas a consumidores, como praticar discriminação de preços ou de ofertas, definir taxa de juros de um empréstimo ou estabelecer o valor do prêmio de um seguro. Essa abordagem tende a ver o futuro como determinado por probabilidades estabelecidas, possivelmente incapacitando melhores soluções que estão no reino das baixas probabilidades. Além disso, as pessoas afetadas pela tomada de decisões resultante do *profiling* não são capazes de entender adequadamente as razões por trás da decisão tomada, nem quais características pessoais foram levadas em conta na formação de seu perfil.

A prática de *profiling* pode gerar tanto discriminação direta quanto indireta. A discriminação direta ocorre quando uma pessoa é tratada de maneira menos favorável que outra que se encontra numa mesma situação, por motivos étnicos, religiosos, de idade, de gênero ou alguma outra base que possua proteção legal. A discriminação indireta ocorre quando uma medida, critério ou prática, conquanto aparentemente neutra, afete de maneira especialmente negativa certo grupo ou minoria protegida.

Percebe-se, então, que o *profiling* apresenta benefícios relevantes de ordem econômica, de ganho de eficiência e de planejamento de ações. Porém, é possível se associar diversos riscos à prática. Conclui-se que o *profiling* potencializa uma fragilização na privacidade de indivíduos e permite práticas discriminatórias entre pessoas e grupos

Com base nos riscos apresentados, identifica-se que a proteção da privacidade e a proibição da discriminação devem servir como as salvaguardas fundamentais para os problemas que emergem com o *profiling*. Basicamente, o que se observa é que os diferentes momentos do procedimento apresentam diferentes riscos. Ao iniciar o procedimento, toda a sistemática de coleta de dados pessoais necessária para se extrair valor, bem como as possíveis inferências e previsões obtidas ao final do procedimento são questões que afetam a privacidade dos indivíduos, que tem diversas informações expostas perante terceiros economicamente interessados em tais informações. Por sua vez, no momento de aplicação dos perfis formados, com a tomada de decisões que afetem significativamente a vida dos indivíduos, práticas discriminatórias podem emergir com o uso cego das previsões feitas. Além disso, os indivíduos não possuem o conhecimento e meios necessários para contestar ou se opor ao procedimento, conduzido de maneira burocrática. A combinação dos riscos associados ao *profiling* forma, ultimamente, uma ameaça ao pleno desenvolvimento da personalidade.

Quanto à proteção da privacidade frente às práticas de *profiling*, percebe-se que o conceito de privacidade foi intensamente debatido ao longo dos anos e se desenvolveu em diversas vertentes, se tornando, hoje, muito mais amplo do que o direito a ser deixado só. Diante do cenário em que os indivíduos se veem obrigados a entregar uma grande quantidade de informações pessoais em troca de serviços fornecidos pelos grandes agentes públicos e privados, surge uma situação em que o indivíduo não possui mais nenhum controle sobre o que as entidades sabem sobre ele e como suas informações pessoais estão sendo utilizadas. Assim, ganha força nos últimos anos a conceituação de direito à privacidade que possui em seu núcleo o direito de o indivíduo exercer controle sobre as suas próprias informações. As teorias da privacidade como controle enfatizam o papel da escolha e da autodeterminação individual, sendo o controle um processo individual, dinâmico e flexível.

Nesse contexto se observa um gradual descolamento entre a disciplina do direito à privacidade e a disciplina relativa a um novo direito fundamental, de proteção de dados pessoais. As novas tecnologias de coleta e tratamento de dados apresentam problemas cada vez mais complexos, de forma que todas as questões que envolvem essa temática não “cabem” mais somente dentro do conceito de privacidade, ainda que o controle sobre as informações pessoais faça parte deste conceito. Nesse sentido passa a se discutir o direito à proteção de dados pessoais como forma autônoma de resguardo dos direitos da

personalidade em ambientes fortemente afetados pelas tecnologias, de forma adicional à privacidade. São direitos distintos, mas complementares**,** sendo que ambos são instrumentos que atuam em conjunto para se obter uma finalidade comum, de proteção da dignidade humana.

A proteção de dados e a privacidade se sobrepõe em diversos campos. Porém, no campo da proteção de informações, a proteção de dados pessoais acaba por ser mais ampla. A privacidade está ligada ao controle de informações pessoais que revelem aspectos íntimos ou privados do sujeito, características que o sujeito não pretende compartilhar com o público ou com seus pares. Por sua vez, a proteção de dados pessoais não se restringe às informações privadas. Mesmo dados públicos merecem certo tipo de proteção e garantias. Existem, ainda, informações que a pessoa conscientemente compartilha com seus pares de maneira pública e que, portanto, sua proteção é incompatível com a ideia de privacidade. Apesar de tais informações serem conscientemente retiradas da esfera privada do sujeito, isso não significa que as empresas possam dar destino indiscriminado a elas, devendo incidir uma disciplina de proteção de dados que evite eventuais abusos. A proteção de dados se refere a dados pessoais, que são aqueles que identificam ou podem identificar uma pessoa, e, portanto, merecem proteção ainda que não tratem de informação protegida pela privacidade. Esses dados que influem na projeção da identidade de uma pessoa, formando parte de sua relação com o mundo exterior, constituem o escopo de proteção deste novo direito da personalidade.

O *profiling* não é feito necessariamente com a obtenção de informações de caráter íntimo ou sigiloso. Ainda que não se utilize dados íntimas ou privados, o *profiling* pode afetar direitos fundamentais além da privacidade. O direito à igualdade pode ser afetado devido aos possíveis efeitos discriminatórios do uso de dados pessoais para classificação da população, afetando as oportunidades de vida do indivíduo. Portanto, a disciplina da proteção de dados pessoais enfrenta diferentes questões, como os diferentes efeitos negativos à autonomia decorrentes do *profiling.*

Assim, a proteção jurídica que deve incidir sobre a prática de *profiling* ilustra o gradual descolamento entre a privacidade e a proteção de dados. Diante do *profiling*, a proteção de dados se torna instrumental para se garantir tanto a privacidade quanto a não discriminação entre indivíduos e grupos, de forma a garantir que pessoas não fiquem presas a perfis estigmatizados que limitam suas liberdades de escolhas.

Assim, observa-se no *profiling* um problema relativo tanto à privacidade quanto à proteção de dados. Os riscos da definição de perfis sobre a privacidade surgem quando informações íntimas, que o indivíduo não tem intenção de publicizar, são indevidamente coletadas e utilizadas para formação de um perfil, ou quando se permite fazer inferências intrusivas de características pessoais, a partir de dados públicos legitimamente coletados. A fim de se garantir a privacidade, normas de proteção de dados devem limitar a coleta de informações íntimas de forma indevida e evitar a utilização de dados para se extrair características da vida privada dos sujeitos na construção dos perfis.

Para além disso, o uso de dados pessoais para constituir perfis, classificar e selecionar pessoas, pode levar a que certos indivíduos ou grupos sofram com tratamento desigual ilegítimo, devendo, assim, haver normas de proteção de dados pessoais capazes de limitar que estas situações ocorram. Considerações jurídicas acerca da discriminação indireta e da discriminação presente em ações entre particulares ainda são pouco exploradas no contexto brasileiro. Apesar disso, existe a percepção de que o *profiling* deve ter seus limites balizados pelo princípio da igualdade, de modo a não permitir que seu uso leve ao tratamento diferenciado injustificável entre pessoas. Há um risco concreto de que a discriminação ocorra no contexto do *profiling*. A fim de se conciliar a função essencial de diferenciação, característica do *profiling* feito por meio da mineração de dados pessoais, com a ideia de igualdade, é necessário que o tipo de diferenciação realizada não implique na segregação desarrazoada de pessoas com base em critérios especialmente protegidos como raça, gênero, religião ou opiniões políticas. É preciso também atentar para a discriminação indireta que resulta do uso de critérios com aparente neutralidade, mas que afetam de forma mais incisiva certos grupos de maior fragilidade.

Estabelecer os limites legais para o *profiling* por meio de normas de proteção de dados pessoais, a serem observadas pelos particulares que pretendem desenvolver atividades de processamento de dados, visa evitar que tais situações ocorram. O princípio da não discriminação deve limitar o que pode ou não ser relevante na construção de perfis para determinados fins, de modo que algumas características consideradas mais sensíveis pela sociedade não devem ser utilizadas para categorizar pessoas, ao menos que plenamente justificável. Os limites impostos pela igualdade devem ser observados nos diversos estágios do processamento, da seleção da base de dados à aplicação do perfil. Para se acessar eventuais casos de discriminação indireta, seria necessário se checar ativamente a ocorrência de tratamento diferenciado injustificado para o fim perseguido

nas práticas de *profiling*. Para tanto, verifica-se a necessidade, mesmo para o setor privado, que as legislações imponham regras de transparência e *accountabllity* para aqueles que empreguem algoritmos de processamentos de dados responsáveis pelo *profiling.* Para concretizar tais ideias, é necessário, mais do que garantias legais, o desenvolvimento de soluções técnicas capazes de viabilizar as salvaguardas normativas.

Portanto, verifica-se que a disciplina legal da proteção de dados pessoais é o instrumento normativo capaz de dar o tratamento adequado ao processamento de dados que visa a definição de perfis, a fim de se atingir as finalidades de proteção à privacidade e à igualdade. Para serem efetivas, as normas de proteção de dados pessoais devem favorecer a criação de uma "arquitetura de controle" sobre o processamento de dados. Isso visa a formação de um ambiente legislativo integrado com as novas tecnologias, de modo a favorecer o controle sobre os fluxos de dados pessoais em diversas vertentes.

Solucionar problemas por meio de arquitetura significa buscar a alteração de estruturas no intuito de criar um ambiente propício para realização do fim buscado. Para se enfrentar os novos problemas do mundo digital, é preciso realizar a transição de uma posição estritamente reativa para uma posição proativa, pois os riscos emergentes da construção de perfis pela coleta em massa de dados são de natureza sistêmica. No mundo atual, em que as informações pessoais estão fora do controle de seus titulares e submetidas a procedimentos burocráticos de tratamento, observa-se danos generalizados em razão de problemas sistêmicos no fluxo de informações.

Para melhor limitar a prática de *profiling* por meio de uma arquitetura de controle, é essencial a transição de medidas de proteção que dependem da iniciativa individual, para meios coletivos e organizacionais de controle de dados. As questões que envolvem o *profiling* e que potencializam efeitos nocivos advindos da prática decorrem, em grande medida, das características estruturais da "Sociedade da Informação". Mecanismos de controle individual costumam falhar em conferir qualquer tipo de garantia ao particular pois a maioria das pessoas não detém conhecimento, recursos ou tempo hábil para compreender as questões envolvidas no tratamento de seus dados e utilizar as garantias postas à sua disposição.

Por esse motivo, é necessária uma arquitetura de proteção, capaz de embutir no design dos sistemas que são utilizados para processamento de dados, garantias legais que permitam a criação de um ambiente de controle individual, social e institucional sobre o processamento de dados em massa. O relacionamento burocrático entre indivíduos e as

grandes organizações deve ser o principal alvo da regulação, visando a redistribuição do poder de controle sobre a informação, de forma a colocar os indivíduos e as empresas em um patamar mais próximo.

Portanto, nos últimos anos se consolidou a ideia de que os problemas decorrentes da coleta e tratamento de dados pessoais não podem ser solucionados somente através do controle individual dos dados pessoais. Tal posicionamento se torna evidente e é essencial na análise de soluções para as questões de privacidade e discriminação ligadas ao *profiling*, que demandam um conjunto de esforços para serem devidamente regulamentadas. Porém, isso não significa que a ideia do controle individual deva ser completamente abandonada, pois continua a exercer um papel instrumental para propiciar maior empoderamento de indivíduos frente às instituições que fazem o tratamento em massa de dados. Ocorre que, as garantias de controle individual devem ser suportadas por outras estratégias regulatórias, que conjuguem as abordagens de direitos individuais com novas abordagens organizacionais de controle.

Em geral, as normas que regulam a proteção de dados devem prever medidas que objetivem garantir a privacidade e a igualdade entre os cidadãos cujos dados pessoais compõe a formação dos perfis. No intuito de mitigar os efeitos do *profiling*, estas normas devem visar a criação de mecanismos para o adequado controle sobre os fluxos de informação, feito pelos indivíduos titulares dos dados, por grupos e por instituições independentes, bem como criar deveres de tratamento responsável dos dados por todos os atores envolvidos no sistema. Isso tem sido feito por meio do estabelecimento de princípios de boas práticas para o processamento de dados, pelo estabelecimento de uma série de direitos individuais para os titulares dos dados, complementados por normas de transparência e *accountability* que visam estabelecer verdadeira governança sobre os algoritmos de definição de perfis.

Limites legais incisivos aplicáveis ao processamento de dados por meio de *profiling* são definidos, no panorama europeu, pela *General Data Protecion Regulation* (GDPR) e, no Brasil, na Lei Geral de Proteção de Dados (LGPD). As novas regulamentações transferem com mais vigor o ônus que antes era suportado pelos indivíduos pelo tratamento de dados pessoais para os próprios responsáveis pelo tratamento e visam fortalecer mecanismos de controle para além do exercício de direitos individuais. Esse tipo de abordagem é capaz de criar uma arquitetura de controle sobre

dados pessoais que será mais efetiva na amenização dos efeitos negativos que decorrem do *profiling*.

Observa-se que ambas regulações acerca da proteção de dados pessoais apresentam um amplo espectro de previsões que devem ser observadas pelo setor privado no caso de tratamentos de dados que envolva o *profiling*. Foram previstos princípios que devem reger a atividade, limites referentes ao tratamento de dados sensíveis, direitos individuais que garantem ao titular dos dados maior controle sobre suas informações e previsões complementares que visam criar um ambiente de tratamento de dados mais responsável e menos intrusivo. A GDPR, no geral, atentou-se ao *profiling* de maneira mais específica e restritiva, definindo seu conceito legal e prevendo uma regra geral de proibição a esse tipo de tratamento, que só poderá ser feito em contextos específicos. Além disso, diretrizes interpretativas diversas são desenvolvidas em seus considerandos. A LGPD faz poucas menções diretas à definição de perfis, optando por deixar a prática submetida, em regra, ao mesmo sistema de proteção de dados aplicável a outras formas de tratamento. De qualquer forma, ambas as legislações vão além da concessão de direitos individuais e visam criar, efetivamente, uma estrutura de controle sobre práticas invasivas de tratamento de dados, como as decorrentes de *profiling*. Assim, espera-se que, caso se verifique, de fato, a observância pelos agentes do setor privado das normas legais que limitam o *profiling*, seja possível a garantia do direito à privacidade e à igualdade no atual contexto de burocracia, uma vez que se estabeleceu uma arquitetura de controle de diversos níveis capaz de alterar as estruturas dos fluxos de informação.

REFERÊNCIAS

ALMEIDA, Virgilio; DONEDA, Danilo. What is Algorithm Governance? **IEEE-Internet Computing**, [S.l.], v. 20, p. 60-63, 2016. Disponível em: https://www.computer.org/csdl/magazine/ic/2016/04/mic2016040060/13rRUyekJ2d. Acesso em: 20 nov. 2019.

ANDRADE, Daniel de Pádua. **Associação e Discriminação**: limites jurídicos para os critérios de admissão, exclusão e categorização de associado. 2018. Dissertação (Mestrado em Direito) - Programa de Pós-Graduação em Direito da Universidade Federal de Minas Gerais, Belo Horizonte, 2018.

ANDRADE, Daniel de Pádua. *Credit scoring* na era do big data: desafios tecnológicos no direito brasileiro. In: PARENTONI, L.; GONTIJO, B. M.; LIMA, H.C.S. **Direito, Tecnologia e Inovação**. Belo Horizonte: D'Placido, 2018. cap. 2.3, p. 246-267.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Automated individual decision-making and *Profiling* for the purposes of Regulation 2016/679**. Bruxelas, 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 2 jul. 2019.

BALKIN, Jack M. The Three Laws of Robotics in the Age of Big Data. **Ohio State Law Journal**, Columbus, v. 78, n. 592, 26 dez. 2016.

BALL, Kirstie. Categorizing the workers: Electronic surveillance and social ordering in the call center Kirstie Ball. *In*: LYON, David (ed.). **Surveillance as Social Sorting**: Privacy, risk and digital discrimination. Londres: Routledge, 2003. cap. 10.

BAROCAS, Solon; SELBST, Andrew D. Big Data‘s Disparate Impact. **California Law Review**, Berkeley, v. 104, p. 671-732, 2016.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.p.114.

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. BBC News**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml Acesso em: 10 nov. 2019.

BELL, Daniel. **The coming of post-industrial society**. New York: Basic Books, 1999.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLUM, Rita P. F. **O Direito à privacidade e à Proteção dos Dados do Consumidor**. São Paulo: Almedina, 2018.

CALDERS, Toon; CUSTERS, Bart. What Is Data Mining and How Does It Work? In: CUSTERS, Bart et al (ed.). **Discrimination and Privacy in the Information Society: Data Mining and *Profiling* in Large Databases**. Berlim: Springer, 2013. cap. 2, p. 28.

CALDERS, Toon; ŽLIOBAITĖ, Indrė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures. *In*: CUSTERS, Bart *et al*. **Discrimination and Privacy in the Information Society**: Data Mining and *Profiling* in Large Databases. Berlim: Springer, 2013. cap. 3.

CAMBRIDGE UNIVERSITY PRESS. **Cambridge Dictionary**. Cambridge, 2019. Disponível em: https://dictionary.cambridge.org/us/dictionary/english/profile. Acesso em: 31 ago. 2019.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, ed. 76, p. 213-240, ago. 2017.

CANHOTO, A.; BACKHOUSE, J. General Description of the Process of Behavioural *Profiling* In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 3, p. 47-63.

CASEMIRO, Luciana. Hering terá que explicar o que faz com dados de reconhecimento facial de clientes. **O Globo**, Rio de Janeiro, 26 fev. 2019. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23482114. Acesso em: 19 jun. 2019

CASTELLS, Manuel. **A galáxia internet. Reflexões sobre internet, negócios e sociedade**. Tradução Rita Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

CASTIGNANI, G. *et al*. Driver Behavior *Profiling* Using Smartphones: A Low-Cost Platform for Driver Monitoring. **IEEE Intelligent Transportation Systems Magazine**, Estados Unidos, v. 7, n. 1, p. 91-102, 2015. Disponível em: https://ieeexplore.ieee.org/document/7014406. Acesso em: 3 set. 2019.

CETIC.br, **Pesquisa TIC Domicílios**. Disponível em: http://cetic.br/pesquisa/domicilios/. Acesso em 01 de jul. 2018.

CLARKE, Roger. *Profiling*: A hidden challenge to the regulation of data surveillance. **Journal of Law & Information Science**, Camberra, v. 4, p. 403-419, 1993.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. **Reuters**, Londres, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 31 ago. 2019.

DINIZ, T. D. M.; DE OLIVEIRA, T. B. G. Decisões automatizadas por máquinas e o humano no loop: cenários discriminatórios, vieses cognitivos e regulação normativa. *In*:

SOARES, F. M.; DE OLIVEIRA, T.B.G.; DA MATA, P. C. O. A. (org.). **Ciência, Tecnologia e Inovação**: Políticas & Leis. Florianopolis: Tribo Ilha, 2019. p. 191-214. Disponível em: https://www.observalei.net.br/ambito-do-observatorio/ciencia-tecnologia-e-inovacao-politicas-leis. Acesso em: 11 dez. 2019.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasil/Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar. 2006.

DUHIGG, Charles. How Companies Learn Your Secrets. **The New York Times Magazine**, Nova Iorque, 16 fev. 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Acesso em: 19 jun. 2019.

EDITORIA: ESTATÍSTICAS SOCIAIS. PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país. **Agência IBGE Notícias**, Rio de Janeiro, 20 dez. 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais. Acesso em: 18 jun. 2019.

EDWARDS, Lilian; VEALE, Michael. Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. **Duke L. & Tech. Rev.**, v. 16, p. 18, 2017.

FARIAS, Adriana. Justiça proíbe uso de câmeras de reconhecimento facial no Metrô. **Veja São Paulo**, São Paulo, 15 set. 2018. Disponível em: https://vejasp.abril.com.br/cidades/justica-proibe-uso-de-cameras-de-reconhecimento-facial-no-metro/. Acesso em: 19 jun. 2019.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional**. 9ª. ed. Salvador: JusPODIVM, 2018.

FERRARIS, Valeria; BOSCO, Francesca; CAFIERO, G.; D'ANGELO, Elena; SULOYEVA, Y. **Working paper: defining *profiling***. United Nations Interregional Crime and Justice Research Institute (UNICRI), December, 2013. Disponível em:<http://www.unicri.it/special_topics/citizen_*profiling*/*PROFILING*project_WS1_definition_0208.pdf >. Acesso em: 06 ago. 2019.

FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao *profiling* e à discriminação a partir das novas tecnologias**. Revista de Direito, Governança e Novas Tecnologias**, Maranhão, v. 3, n. 2, p. 18-38, jul. [dez]. Disponível em: <https://www.researchgate.net/publication/323382063_TRATAMENTO_DE_DADOS_PESSOAIS_E_A_LEGISLACAO_BRASILEIRA_FRENTE_AO_*PROFILING*_E_A_DISCRIMINACAO_A_PARTIR_DAS_NOVAS_TECNOLOGIAS>. Acesso em: 09 nov. 2018.

FTC. Online profiling: a report to congress. 2000. Disponível em: <https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commissionreport-congress-june-2000/onlineprofilingreportjune2000.pdf>. Acesso em: 19 jun. 2019.

GANTZ, John; REINSEL, David. The digital universe in 2020: big data, bigger digital shadows, and biggest growth in the far east. IDC iView - Analyze the Future, 2012. Disponível em: https://www.emc.com/leadership/digital-universe/2012iview/index.htm. Acesso em: 5 jul. 2019.

GARFINKEL, Simson. **Database nation: the death of privacy in the 21st century**. Boston: O'Reilly Media, 2010.

GOODMAN, Bryce, FLAXMAN, Seth. EU Regulations on Algorithmic Decision-Making and a "right to Explanation", **AI Magazine**, Oxford, vol 38, n. 3, 2017.

HAVARD, Cassandra Jones. On the Take: The Black Box of Credit Scoring and Mortgage Discrimination. **Boston University Public Interest Law Journal**, Boston, v. 20, n. 24, p. 241-286, 2011.

HARFORD, Tim. Big data: A big mistake?. **Significance**, Londres, v. 11, n. 5, p. 14-19, 1 dez. 2014.

HERT, Paul De; LAMMERANT, Hans. Predictive *profiling* and its legal limits: Effectiveness gone forever. *In*: VAN DER SLOOT, Bart; BROEDERS, B.; SCHRIJVERS, E. **Exploring the boundaries of big data**. Amsterdã: Amsterdam University Press, 2016. p. 145-173.

HILDEBRANDT, Mireille. Defining *Profiling*: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 17-43.

HURLEY, Mikella; ADEBAYO,Julius. *Credit scoring* in the age of big data. **The Yale Journal of Law & Technology, v. 18, p.148-216,2016.** Disponível em <https://yjolt.org/credit-scoring-era-big-data>. Acesso em: 09 nov. 2018.

JAQUET-CHIFFELLE, David-Olivier. Reply: Direct and Indirect *Profiling* in the Light of Virtual Persons In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 34.

JÚNIOR, P.J.C. **O direito de estar só: tutela penal da intimidade**. São Paulo: Revista dos Tribunais, 2007.

KAMP, Meike; KORFFER, Barbara; MEINTS, Martin. *Profiling* of Customers and Consumers - Customer Loyalty Programmes and Scoring Practices. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Netherlands: Springer, 2008, p. 201-215.

KAPLAN, Jerry. **Artificial Intelligence: What everyone needs to know**. Oxford: Oxford University Press, 2016.

KREISS, Daniel. Micro-targeting, the quantified persuasion. **Internet Policy Review - Journal on internet regulation**, School of Media and Journalism - University of North Carolina, United States of America, Volume 6, número 4, dezembro/2017, pp 1-2. Disponível em: < https://policyreview.info/articles/analysis/micro-targeting-quantified-persuasion >. Acesso em 31 de ago. 2019.

KUBARLIJA, Jovan. **An Introduction to Internet Governance**, 7. ed, Genebra: DiploFoundation, 2016.

LASZLO, Andras. *Profiling*, Data Mining and Law Enforcement: Definitions**. 50 Annales U. Sci. Budapestinensis Rolando Eotvos Nominatae**, Budapeste, 2009.

LAZARO, Christophe; MÉTAYER, Daniel Le. Control Over Personal Data: True Remedy or Fairy Tale? **SCRIPTed - Journal of Law, Technology & Society.** Edinburgh: University of Edinburgh School of Law. v. 12, n. 01, p. 03-34, June. 2015.

LEMOS, Ronaldo. O Marco Civil como símbolo do desejo por inovação no Brasil. IN:LEMOS, Ronaldo; LEITE, Salomão George (Coord.). **O Marco civil da Internet**. São Paulo: Atlas. 2014. p. 4-11.

LEOPOLD, N.; MEINTS, M. *Profiling* in Employment Situations (Fraud**)** In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 12.

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

LEOPOLDO, Rafael. Vigilância Líquida: Variações Sobre O Panoptismo. **Sapere Aude**, Belo Horizonte, v. 6, n. 12, p. 894-902, 2015. Disponível em: http://periodicos.pucminas.br/index.php/SapereAude/article/viewFile/11261/9115. Acesso em: 3 set. 2019.

LESSIG, Lawrence. **Code v2.0**, Nova York: Basic Books, 2006.

LOPES, G.F.P. O direito à explicação de decisões automatizadas no âmbito do regulamento geral de proteção de dados da união europeia. *In*: SOARES, F. M.; DE OLIVEIRA, T.B.G.; DA MATA, P. C. O. A. (org.). **Ciência, Tecnologia e Inovação**: Políticas & Leis. Florianopolis: Tribo Ilha, 2019. p. 235-259. Disponível em: https://www.observalei.net.br/ambito-do-observatorio/ciencia-tecnologia-e-inovacao-politicas-leis. Acesso em: 11 dez. 2019.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press. 2015

MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação**: *Profiling* e risco de discriminação. 2018. Dissertação (Mestrado) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018.

MACHADO, Fernando Inglez de Sousa; LINDEN RUARO, Regina. Publicidade Comportamental, Proteção de Dados Pessoais e o Direito do Consumidor. **Conpedi Law Review**, Braga, v. 3, n. 2, p. 421-440, jul-dez. 2017

MARCHETTI, Bruno. Porque você deve se preocupar com a nova lei do Cadastro Positivo. **Vice**. Disponível em: https://www.vice.com/pt_br/article/qvxn95/dados-lei-cadastro-positivo . Acesso em: 09 nov. 2018

MAYER-SCHONBERGER, Viktor; KENNETH, Cukier. **Big Data: a revolution that will transform how we live, work and think**. Nova Iorque: HMH, 2013. *E-book.*

MEIRELLES, Fernando. **Pesquisa anual do uso de TI.** Disponível em: https://eaesp.fgv.br/ensinoeconhecimento/centros/cia/pesquisa . Acesso em: 18 de jun. 2019.

MELLO, Celso Antônio Bandeira de. **O conteúdo jurídico do princípio da igualdade**. 3. ed. São Paulo: Malheiros, 2009,

MENDES, L.S. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1. ed. São Paulo: Saraiva, 2014.

MICHAELIS. **Dicionário Brasileiro da Língua Portuguesa**. São Paulo: Melhoramentos, 2019. Disponível em: https://michaelis.uol.com.br/moderno-portugues/. Acesso em: 1 set. 2019.

MIRANDA, Pontes de. **Tratado de Direito Privado** - parte especial, tomo VII, 3a Ed. Rio de Janeiro: Borsoi,1971.

NABETH, Thierry. Reply: Further Implications?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling* the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 2, p. 30.

NUÑEZ, Michael. FTC Slaps Facebook With $5 Billion Fine, Forces New Privacy Controls. **Forbes**, Nova Iorque, 24 jul. 2019. Disponível em: https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#2e499a135668. Acesso em: 25 nov. 2019.

O'NEIL, Cathy. **Weapons of math destruction: how Big Data increases inequality and threatens democracy**. Nova Iorque: Crown, 2016.

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

PAUL, Katie; RANA, Akanksha. U.S. charges Facebook with racial discrimination in targeted housing ads. **Reuters**, Londres, p. 1, 19 mar. 2019. Disponível em: https://www.reuters.com/article/us-facebook-advertisers/hud-charges-facebook-with-housing-discrimination-in-targeted-ads-on-its-platform-idUSKCN1R91E8. Acesso em: 3 set. 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHERMER, Bart M. The limits of privacy in automated *profiling* and data mining. **Computer Law & Security Review**, Amsterdã, v. 27, p. 45-52, 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364910001767. Acesso em: 31 ago. 2019.

SCHWAB, Klaus**. A quarta revolução industrial.** Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SCHWARTZ, Paul. The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination. **The American Journal of Comparative Law**. Berkeley: American Society of Comparative Law. v. 37, n. 04, p. 675-701, Fall. 1989.

SIMÃO FILHO, A.; SCHWARTZ, G. A. D. Big Data em tempos de internet das coisas. In: PARENTONI, L.; GONTIJO, B.M.; LIMA, H.C.S. **Direito, Tecnologia e Inovação**. Belo Horizonte: D'Placido, cap. 2.2, p. 217-246. v. I. 2018.

SINGER, Natasha; CONGER, Kate. Google Is Fined $170 Million for Violating Children's Privacy on YouTube. **The New York Times**, Nova Iorque, 4 set. 2019. Disponível em: https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html. Acesso em: 25 nov. 2019.

SLOOT, Bart van der; SCHENDEL; Sacha van. Ten questions for future regulation of big data: a comparative and empirical legal study. **Journal of Intellectual Property, Information Technology and Eletronic Commerce Law,**v7,n.2, o.110-145, 2016.

SOLOVE, Daniel J. Why privacy matters even if you have 'nothing to hide'. **Chronicle of Higher Education**, v. 15, 2011.

SOLOVE, Daniel. **The digital person: technology and privacy in the information age**. Nova Iorque: NEW YORK UNIVERSITY PRESS, 2004.

SPIECKER, Indra *et al*. The Regulation of Commercial *Profiling* – A Comparative Analysis. **European Data Protection Law Review**, Berlim, p. 535-555, 2019.

SQUIRES, Gregory D. Racial *Profiling*, Insurance Style: Insurance Redlining and the Uneven Development of Metropolitan Areas. **Journal of Urban Affairs**, Milwaukee, v. 24, n. 4, p. 391-410, 2003. Disponível em: https://www.tandfonline.com/doi/abs/10.1111/1467-9906.t01-1-00168. Acesso em: 3 set. 2019.

TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000.

UNIÃO EUROPEIA. Regulamento nº 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 3 de nov. 2019.

USA. Department of Justice. The Privacy Act of 1974 5 U.S.C. § 552a (2012). Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Washington, DC, 01 maio 1974. Disponível em: <https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition>. Acesso em: 25 nov. 2019.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017.

WARREN, Samuel D, BRANDEIS, Louis D, The Right to Privacy, **Harvard Law Review**, vol.4, p. 193-220, 1890.

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.

YANNOPOULOS, A.; ANDRONIKOU, V.; VARVARIGOU, T. Behavioural Biometric Profi ling and Ambient Intelligence In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. ***Profiling*** **the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. cap. 5, p. 89-106

ZANATTA, Rafael A. F. Perfilização, Discriminação e Direitos: Do Código de Defesa do Consumidor à Lei Geral de Proteção de dados pessoais. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais/stats>. Acesso em: 31 ago. 2019.

ZUBOFF, Shoshana. **The age of Surveillance Capitalism: the fight for a human future at the new frontier of power.** Nova Iorque: Public Affairs, 2019. E-book.