ARTIGO

Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados

David Salim Santos Hosni
davidsshosni@gmail.com

Mestre e doutorando em Direito pela UFMG. Professor de Direito no Curso Superior de Administração Pública da Fundação João Pinheiro.

Pedro Bastos Lobo Martins
pedroblmartins@gmail.com

Mestrando em Direito pela UFMG. Pesquisador do grupo de pesquisa Persona e Coordenador Acadêmico do Data Privacy Brasil.

Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados

Palavras-chave
Proteção de Dados
Tomada de decisão automatizada
Profiling
Lei Geral de Proteção de Dados
GDPR

Resumo
Este texto explora as alternativas adotadas pela Lei Geral de Proteção de Dados (Lei 13.709/18) em relação à regulamentação da tomada de decisões automatizada e seu potencial de proteção dos direitos dos titulares de dados. Introduziremos brevemente, a partir de metodologia jurídico-exploratória e da utilização de dados secundários e de uma combinação de bibliografia nacional e estrangeira, os riscos de atividades de *profiling* e tratamento automatizado de dados e a sua intersecção com a regulação da proteção de dados. Partimos da hipótese de que uma abordagem individualista focada apenas em empoderar titulares a partir de direitos individuais encontra deficiências. Para esse estudo, foram analisados tanto questões conceituais de *profiling* e tomada de decisões automatizadas, quanto os mecanismos normativo-regulatórios trazidos pela LGPD e GDPR. Na parte final é feita uma análise do panorama regulatório trazido pela lei brasileira sobre o tema, no qual argumentamos que existe um promissor potencial para um arranjo institucional e de supervisão que tenha enfoque na construção de um sistema de proteção coletivo, a partir de um ferramental trazido pela lei que possibilita ações coletivas em caráter preventivo para garantir os direitos e princípios estabelecidos pela LGPD.

Automated Decision-Making and Data Protection Regulation: Collective Alternatives Presented by the Brazilian General Data Protection Law

Keywords
Data Protection
Automated Decision-making
Profiling
Brazilian General Data Protection Law
GDPR

Abstract
This paper explores the alternatives adopted by the Brazilian General Data Protection Law (Law 13.709/18) – also known as LGPD – in relation to the regulation of automated decision-making and its potential to protect the rights of data subjects. We will briefly introduce, based on legal-exploratory methodology and the use of secondary data and a combination of national and foreign bibliography, the risks of profiling and automated data processing activities and their intersection with data protection regulation. We start from the hypothesis that an individualistic approach focused only on empowering subjects based on individual rights finds deficiencies. For this study, conceptual issues of profiling and automated decision making were analyzed, as well as the normative-regulatory mechanisms brought by both LGPD and GDPR. In the final part, an analysis of the regulatory panorama brought by Brazilian law on the subject is made, in which we argue that there is a promising potential for an institutional and supervisory arrangement that focuses on the construction of a collective protection system, based on a toolbox brought by the law that allows preventive collective actions to guarantee the rights and principles established by the LGPD.

1. Introdução

A criação e expansão de legislações de proteção de dados pessoais foi impulsionada a partir da regulação europeia sobre proteção de dados, a *General Data Protection Regulation* – GDPR – e, hoje, mais de 120 países possuem alguma lei de proteção de dados (Banisar, 2019). No Brasil, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) – LGPD – trouxe importantes inovações ao ordenamento jurídico brasileiro. A lei teve influência direta da GDPR, prevendo, de forma geral, um regime jurídico com diversas semelhanças.

No entanto, enquanto a GDPR surge como uma evolução de algumas regulamentações que já existiam no cenário europeu de proteção de dados, notadamente a Diretiva 95/46/EC, no caso brasileiro não havia nenhuma lei que disciplinasse de forma abrangente a matéria de proteção de dados antes da LGPD. Havia apenas leis setoriais e institutos jurídicos que se aplicavam indiretamente ao tema, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, aplicável ao setor de crédito, além da Lei de Acesso a Informação e o *Habeas Data*, estes últimos sendo instrumentos normativos voltados para a fiscalização do poder público (Bioni, 2019).

Desta forma, a LGPD deve ser entendida como uma lei que inaugura e unifica um novo sistema de proteção de dados no Brasil. Como consequência disso, regras mais abrangentes e um foco em princípios gerais podem ser observados, especialmente quando comparada à GDPR. Se isso pode ser considerado como algo que leve a um regime de proteção de dados mais fraco, é algo a ser observado nos próximos anos, uma vez que a referida lei entrou em vigor no dia 18 de setembro de 2020.[1] Por outro lado, tambem é de se notar que a lei brasileira, embora tenha se inspirado na GDPR, trouxe algumas inovações para o campo de proteção de dados, advindos de outras áreas do direito brasileiro, como o processo coletivo (Zanatta, 2020).

Conforme buscaremos demonstrar ao longo do texto, essas inovações podem ser importantes para fomentar um caráter coletivo para a proteção de dados (Mantelero, 2016; Taylor, Floridi e Van der Sloot, 2017; Mittelstadt, 2019). Em outras palavras, acreditamos ser possível argumentar que a LGPD deixa de entender os direitos previstos por ela como direitos unicamente individuais, uma vez que prevê de forma expressa o exercício de ações coletivas para sua tutela. Além disso, argumentamos que a lei brasileira dispõe de instrumentos promissores para o combate às discriminações geradas por atividades de tratamento de dados.

A partir dessas ideias centrais, no restante do texto vamos desenvolvê-las tendo como recorte a regulação que recai sobre decisões automatizadas e o direito à explicação. Existe uma grande discussão acerca da existência ou não desse direito na GDPR (Goodman e Flaxman, 2017; Selbst e Powles, 2017; Wachter, Mittelstadt e Floridi, 2017), conforme iremos abordar, e vislumbra-se que o mesmo debate ocorrerá no Brasil.

Para além da discussão da existência ou não desse direito, há uma discussão mais ampla, a respeito das salvaguardas legais que recaem sobre decisões automatizadas, notadamente o art. 22 da GDPR e o art. 20 da LGDP e a efetividade destes dispositivos.

Partimos da hipótese de que os direitos dos titulares, aplicados em uma escala individual, podem não ser os melhores instrumentos de proteção em face de decisões que muitas vezes são tomadas (ou ao menos causam efeitos) em âmbito coletivo (Mantelero, 2016; Rouvroy, 2016; Edwards e Veale, 2017).

Na primeira parte do texto serão abordados alguns dos problemas e violações à direitos que decisões totalmente automatizadas podem causar, esperando demonstrar que o alcance dessas

atividades ultrapassa o limite do individual, de forma que nem sua regulamentação e nem os exercícios de direitos de titulares podem ficar restritos a essa esfera.

Na segunda parte, forneceremos uma visão geral das salvaguardas na tomada de decisões automatizada, focada no artigo 22 da GDPR, e traçaremos paralelos com o que a lei brasileira traz como alternativas, apontando diferenças e semelhanças. Argumentamos que, embora a LGPD forneça uma regulamentação possivelmente mais fraca que a GDPR, algumas de suas disposições, notadamente a possibilidade de exercer os direitos dos titulares de dados em escala coletiva, o princípio de não discriminação e transparência e a possibilidade de reversão do ônus da prova, aparecem como instrumentos promissores na regulação e controle da tomada de decisões automatizada.

A presente pesquisa qualitativa justifica-se em razão da busca de um adequado tratamento jurídico para a garantia de eficácia dos direitos e deveres estipulados na legislação sobre proteção de dados, em especial nas atividades de *profiling* e tomada de decisão automatizada, construída a partir dos instrumentos processuais e materiais vigentes no Brasil. Valemo-nos, no atual estado da arte e considerando ainda a incipiente vigência da LGPD e das práticas institucionais do setor (inclusive considerada a inexistência da Autoridade Nacional de Proteção de Dados), de metodologia jurídico-exploratória. Partimos da análise de dados secundários, de leitura crítica de bibliografia internacional e nacional e de raciocínios indutivos, bem como de uma exposição de justificações jurídico-axiológicas, para buscar uma avaliação preliminar dos instrumentos disponíveis no campo e identificar a possibilidade de novas hipóteses, pesquisas e atuações na área, fundadas na legislação nacional e como autores brasileiros a vem interpretando, e na incorporação crítica da experiência europeia.

2. Tratamento de Dados, Tomada de Decisão Automatizada suas Ameaças

Nesta seção iremos analisar os principais elementos conceituais do *profiling* e sistemas tomadas de decisão automatizada, buscando compreendê-los como fenômenos supra-individuais. Ou seja, como fenômenos que não só causam efeitos em uma escala coletiva, mas só podem ser adequadamente compreendidos e avaliados se examinados nesta dimensão.

Em seguida, os riscos apresentados por essas atividades de tratamento de dados serão também introduzidos, identificando os pontos críticos a partir de uma perspectiva da proteção de direitos fundamentais.

2.1. Análises de Big Data e *Profiling* como Fenômenos Supra-Individuais

A Lei Geral de Proteção de Dados não traz em seu texto uma definição de *profiling*, no entanto, em seus artigos 12, § 2º, e 20, caput, essa atividade é mencionada indiretamente, na definição de dados pessoais e dos tipos de decisões automatizada em que são garantidos direitos de revisão ao titular dos dados. Assim, o foco regulatório da LGPD, no que tange às atividades de *profiling*, recai sobre a predição do comportamento do titular (Zanatta, 2019) e sobre a sua utilização para tomada de decisões que possam ter consequências para os interesses e exercício de direitos do titular (Bioni, 2019).

Na literatura científica, uma proeminente definição de *profiling* é proposta por Hildrebradnt (2008):

> O processo de 'descoberta' de correlações entre dados em bancos de dados que podem ser usados para identificar e representar um sujeito humano ou não humano (indivíduo ou grupo) e / ou a aplicação de perfis (conjuntos de dados correlacionados) para individuar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria (p.19).[2]

Já a GDPR define *profiling* em seu artigo 4º, item 4, com ênfase em seus usos para previsão comportamental e outras características socialmente relevantes do sujeito:

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

Outro ponto importante a ser observado na definição trazida pela GDPR está no fato de que, para ser caracterizado como criação de perfil, algum processamento automatizado deve ocorrer, o qual, no entanto, não precisa ser totalmente automatizado. Em outras palavras, a participação humana no processo não descaracteriza o fenômeno (Article 29 Working Party, 2018).

Apesar dessa tentativa de destacar os elementos éticos e juridicamente relevantes, a referida legislação deixa de lado alguns dos aspectos mais preocupantes. Antoinette Rouvroy (2016) ressalta que analisar a atividade de *profiling* como unicamente um tratamento de dados pessoais que tem como objetivo gerar informações sobre uma pessoa específica encontra suas limitações. Conforme afirma a autora:

> Os modelos preditivos ou perfis supra-individuais atribuídos a indivíduos são baseados em dados infra-individuais decorrentes de um grande número de indivíduos. Nesse processo, os dados de qualquer indivíduo são tão válidos quanto os de qualquer outro - seus dados são tão bons quanto os de seu vizinho (p. 33).[3]

Além disso, a criação de perfil pode ser feita com dados anonimizados (Mantelero, 2016) e pode ser direcionada para um determinado grupo e não para uma pessoa específica (Hildebrandt, 2008), ao contrário do que a definição da GDPR pressupõe, ao conceituar que a utilização desses dados servirá "para avaliar certos aspectos pessoais de uma pessoa singular".

Outro ponto legalmente relevante do uso de criação de perfis deixado de fora pela legislação apresentada é o fenômeno do *group profiling*[4] e do clustering. Isso se refere ao uso de big data e técnicas de profiling para criar grupos que ainda não são conhecidos ou que não podem ser conhecidos fora da lógica de processamento do aprendizado de máquina.[5]

Antoinette Rouvroy (2016) traça uma diferenciação entre a classificação de indivíduos a partir de uma lógica tradicional de categorização e a formação de *clusters* a partir do tratamento de dados. Segundo a autora, em uma categorização por meio de uma lógica tradicional, características comuns a um grupo são identificadas, seja pelo próprio indivíduo ou por terceiros, e com isso subsumidas em categorias pré-existentes. Em outras palavras, as categorias já existem como um fenômeno social dotado de significado (e.g. grupo étnico, grupo religioso etc.) e, ao serem colocados (ou se colocarem) nessa categoria, os indivíduos se veem como pertencentes ao grupo, podendo

criar relações de interdependência e solidariedade. Diferentemente, no clustering ou group profiling:

> O objetivo dos processos de group profiling ou clustering, por outro lado, é de realçar categorias anteriormente desconhecidas, social e visualmente imperceptíveis, com base na análise de dados sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias. Em processos de clustering, os indivíduos são colocados [...] em 'categorias' socialmente e existencialmente sem significado, que são imperceptíveis (porque emergem apenas enquanto o processo se desenrola) e, na maioria das vezes, sem possibilidade de estar ciente do que está acontecendo ou de se reconhecer (ROUVROY, 2016, p. 28).[6]

Temos, então, que, nos grupos formados por meio de *clustering*, não há relações sociais pré-existentes, como naqueles formados por uma categorização tradicional, o que dificulta o exercício de direitos, principalmente se criarem novos grupos vulneráveis à discriminação e que eram, até então, imperceptíveis. Assim, o sujeito pode ser colocado em grupos que sequer poderia imaginar que fizesse parte, junto a pessoas que nunca imaginou ter algum tipo de relação, alterando sua percepção de pertença social.

Mittelstadt (2017) identifica esses grupos constituídos por meio de *clustering* como "grupos *ad hoc*", uma vez que são formados através de um agrupamento volátil, com um processamento e finalidade específicos. Desta maneira, o próprio titular terá dificuldade para saber da existência desse grupo de que é parte e que pode estar sendo afetado por isso. Mesmo em uma perspectiva de tutela coletiva, existe uma grande dúvida a respeito de como se daria a representação dos interesses desses grupos *ad hoc*.

Assim, o perfil construído não é uma representação exata dessa pessoa, mas uma tentativa de prever seu comportamento para um objetivo específico, feito a partir de uma massiva agregação de dados. Sandra Watcher (2019) alega que "o que importa é se o usuário se comporta de maneira semelhante o suficiente ao grupo suposto para ser tratado como um membro do grupo (p. 13)".[7]

Hildebrandt (2008) cita um exemplo de uma hipotética comunidade de mulheres de olhos azuis que possua uma correlação específica de maior probabilidade de desenvolver câncer de mama, podendo emergir como um "sujeito" em uma base de dados, composto como um grupo, se diferenciando do conceito de *titular*, adotado nas legislações brasileria e europeia, como pessoa natural identificada ou identificável. Isso explicita que, mesmo sem nunca ter consentido com a coleta de dados pessoais ou seu processamento, a classificação de risco com base em atributos comuns pode afetar indiretamente pessoas que, individualmente, não detém a possibilidade de se opor.

Portanto, como não são usados apenas dados pessoais de uma só pessoa para construir um modelo, cria-se um limbo entre a possibilidade de exercício de direitos individuais para controle de um perfil e os dados agregados provenientes de diversos indivíduos usados para a formação desse perfil.

2.2. Outras Características Relevantes dos Processos de Tomada de Decisão Automatizada

No tópico anterior, identificamos as limitações existentes na associação dos processos

de *profiling* tão somente à identificação ou avaliação de uma pessoa natural específica, esperando demonstrar que essa técnica causa consequências em escala supra-individual. Agora, mostraremos outras ameaças colocadas pelos processos de tratamento de dados, tendo como foco seus efeitos discriminatórios.

Inicialmente, é importante observar que as correlações estabelecidas pelas técnicas de aprendizado de máquina não podem ser antecipadas com segurança e não têm a capacidade de identificar nenhuma relação de causalidade por trás dessas correlações. Não conseguem nem mesmo atribuir uma racionalidade para essas descobertas. Como aponta Mireille Hildebrandt (2008), as relações indicadas por processos de perfilação não estabelecem causas ou razões para o surgimento ou perpetuação dessas relações. Os algoritmos operam indicando como as relações entre as variáveis analisadas tem se estabelecido até aquele momento e, se for usado para um processo de tomada de decisão, qual o melhor curso de ação considerando a probabilidade das relações se manterem iguais.

Pode-se, a partir disso, questionar a legitimidade do "conhecimento" produzido por meio de algoritmos de aprendizado de máquina, considerando que podem causar consequências diretas na vida de pessoas (por exemplo, ao negar um pedido de crédito).

Ademais, essa natureza classificatória das tecnologias de perfilação abre margem para que levantemos um problema a elas associado: a perfilação possui enorme potencial de aprofundar os padrões discriminatórios já existentes (como àqueles ligados à etnia, gênero, orientação sexual, orientação política ou religiosa), ou mesmo de criar novos focos discriminatórios. (Hildebrandt, 2008; Schermer, 2013; Mann & Matzner, 2019; Wachter, 2019). O caso COMPAS, em que réus negros foram sistematicamente prejudicados por um algoritmo de previsão de reincidência criminal é um clássico exemplo desse aprofundamento discriminatório (Larson, Mattu, Kircher & Angwin, 2016).

Um raciocínio apressado a respeito desse problema traz a solução simples de que tais dados sejam excluídos dos processos de tratamento, como fez o item 4 do artigo 22 da GDPR, proibindo que decisões automatizadas se baseiem em dados sensíveis. Entretanto, essa solução apresenta uma série de problemas. O primeiro deles são as flexibilizações feitas pela GDPR nesse próprio artigo, permitindo o uso desses dados em dois casos: consentimento do titular e substancial interesse público (arts. 9 (2) (a) e (g)). A inadequação do requisito do consentimento como uma proteção ao titular nesse contexto, trabalhada adiante no tópico 3.1, se mostra como uma forte limitação dessa norma legal.

Outra inadequação dessa proteção, baseada na utilização de dados sensíveis, é decorrente de sua própria definição[8], que inclui, por exemplo, dados que revelem origem étnica ou racial, opiniões políticas e religiosas, dados biométricos, dados de saúde, orientação sexual, entre outros. No entanto, outros dados que identificam grupos vulneráveis não estão incluídos, como gênero, renda, local de moradia e emprego (Martins, 2020).[9]

Schermer (2011) ainda argumenta que remover dados sensíveis das bases de processamento automatizado pode representar a exclusão de meios para verificar, após o processamento, se um algoritmo tomou uma decisão discriminatória.

Ainda, outro comprometimento desse modelo se relaciona com as técnicas de *group profiling* e *clustering*, comentadas no item anterior. Sandra Wachter (2019) indica que, nesses casos, há a possibilidade de utilização pelo controlador dos chamados "*proxy data*". Esses seriam dados que não ligam diretamente um titular a uma categoria sensível (como etnia, por exemplo) mas apenas identificam uma "afinidade" do titular com determinado grupo. Isso pode ser feito, por exemplo, ao usar os dados

de curtidas ou visitas a páginas de promoção da igualdade racial para inferir uma afinidade com um grupo étnico. A autora alerta que essa situação permitiria, em tese, ao controlador não se submeter a obrigações legais, uma vez que poderia alegar não estar identificando uma informação sensível. Essa manobra foi identificada nas configurações de direcionamento de propaganda permitidas pelo Facebook, em que anunciantes podiam excluir determinados grupos com "afinidades étnicas" de receberem seus anúncios (Angwin e Parris Jr, 2016).

Esse efeito discriminatório pode advir em diversos estágios de implementação da técnica, como no desenho do algoritmo, na escolha dos dados de treinamento do algoritmo de *profiling* ou do uso corrente do algoritmo em meios sociais onde práticas discriminatórias são corriqueiras, gerando uma retroalimentação inadequada (Kuner e outros, 2017).

A real existência, no entanto, de uma discriminação injusta e que viola a ordem jurídica na execução de *profiling* e tomadas de decisão automatizada não é fácil de se verificar. Além das dificuldades técnicas, muitas vezes é difícil também de se determinar o que seria um resultado justo.[10]

Além dos riscos inerentes à própria técnica de profiling destacados até então, o fato de os titulares não terem acesso ao conhecimento utilizado para classificá-los em perfis faz com que fiquem em posição de extrema desvantagem em relação ao controlador de dados (Hildebrandt, 2008). Schermer (2011) vai identificar esse risco como assimetria informacional entre titular e controlador, reforçada pela proteção proprietária do controlador dos algoritmos usados no processo e de seus resultados. Essa assimetria pode gerar sérios problemas nos mercados de consumo, onde não só a oferta, mas o próprio preço dos produtos pode ser definido com base em características pessoais, e nas relações de liberdades democráticas entre governos e cidadãos.

Todas essas características das tecnologias de perfilação e seus usos são importantes para que possamos, novamente, olhar para a abordagem proposta pela GDPR e LGPD de regulação das decisões automatizadas com base nessas técnicas.

3. Salvaguardas na Tomada de Decisão Automatizada na GDPR e LGDP

A Lei Geral de Proteção de Dados menciona a tomada de decisão automatizada somente em seu artigo 20, *caput*, estabelecendo o direito à revisão de decisões "tomadas unicamente com base em tratamento automatizado de dados pessoais". Já no art. 20, §1º, é previsto o direito de solicitar informações "a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada". Portanto, de acordo com a legislação brasileira, para que o direito de revisão seja aplicável, é necessário que a decisão tenha sido tomada sem a participação humana, mesmo que ela empregue ou utilize o resultado de técnicas de criação de perfil. Por outro lado, o direito à informação, trazido pelo art. 20, §1º, não exige, pelo menos a princípio, que a decisão tenha sido tomada apenas através de processamento automatizado.

Já a GDPR, por sua vez, aborda a tomada de decisões automatizadas diversas vezes ao longo de seu texto,[11] regulando-as mais detalhadamente em seu art. 22. A princípio, esse artigo garante um direito geral aos titulares de não serem submetidos a decisões tomadas unicamente com base em um tratamento automatizado. Sobre esse dispositivo, por ora, cabe ressaltar que a proibição geral também se aplica às atividades de *profiling*, mesmo que para sua caracterização não se exija um processamento

totalmente automatizado, como mencionado acima (Tópico 2.1).

Sob essa perspectiva, a lei brasileira é mais rigorosa com a noção de decisão automatizada, de forma que a participação humana no processo de tomada de decisão torna inaplicável o direito à revisão. Por outro lado, a GDPR permite uma maior flexibilidade para o conceito, exigindo a completa automação (com a exceção do *profiling)* apenas para a aplicação de seu art. 22.

Outro ponto a ser observado é que a GDPR e a LGPD contam com a supervisão e as ações das autoridades de proteção de dados, reforçando a supervisão da lei, sem que todo o peso de fiscalização recaia sobre o exercício de direitos dos titulares (Doneda, 2006). Além disso, elas agem não apenas como uma entidade de aplicação da lei, mas também têm o papel de estabelecer guias de conformidade e boas práticas. Entretanto, lamentavelmente, no cenário brasileiro, a Autoridade Nacional de Proteção de Dados, prevista pela LGPD, teve sua estrutura criada pelo Decreto nº 10.474, porém ainda não há a nomeação de nenhum de seus membros.

Além disso, no que diz respeito à tomada de decisões automatizada, ainda não está totalmente claro como a regulamentação será aplicada, se reforçando os direitos individuais fornecidos aos titulares dos dados ou exigindo avaliações e certificações de impacto prévios para os controladores de dados.

Kaminski e Malgieri (2019) propõem uma abordagem promissora sobre a segunda hipótese, indicando como a GDPR exige uma "avaliação de impacto algorítmico" [*algorithmic impact assessment]* e uma abordagem de explicação em várias camadas. Edwards e Veale (2018) também argumentam a favor de uma abordagem sistêmica em detrimento de uma focada na ação individual.

A eficácia dessa abordagem de escopo individual é questionável e, no mínimo, restritiva. A garantia do direito individual como forma de combater a discriminação gerada de maneira sistêmica por técnicas de *profiling* e tomada de decisão automatizada é possivelmente ineficaz devido a esse falso empoderamento. Exploraremos essa premissa a partir de uma avaliação do Artigo 22 da GDPR e o direito de não se submeter à tomada de decisão totalmente automatizada.

3.1. O Direito de Não de se Submeter a Decisões Totalmente Automatizadas e as Limitações do Artigo 22 da GDPR

O artigo 22 da GDPR vem sendo visto como uma importante proteção contra os riscos individuais e coletivos advindos da perfilação e da mineração de dados. Nesse sentido, o *Article 29 Working Party* (2018) considerou o artigo 22 como uma proibição geral de ser submetido a decisões automatizadas, excluindo a possível interpretação de que se trate de um direito de *opt-out*. Essa opinião é seguida por Mendoza e Bygrave (2017) quando afirmam que uma interpretação contrária, onde os direitos ali garantidos exigiriam ações do titular dos dados, resultaria em um claro enfraquecimento da regulamentação, tanto do ponto de vista da privacidade quanto da proteção de dados.

Acreditamos que, tanto em sua elaboração quanto em sua abordagem do problema, a solução proposta pelo artigo 22 possa frustrar as expectativas do legislador europeu. Veale e Edwards (2018) afirmam que o referido artigo é repleto de complicações e exceções. Explicamos, a começar por estas últimas.

Após ser colocado tão preemptivamente no

caput do artigo 22, o direito de não ser submetido a decisões baseadas apenas em processamento automatizado pode ser afastado em três casos: para viabilizar a celebração de um contrato entre sujeito e controlador de dados – item 2(a), autorização pela legislação da União ou do Estado Membro, com as medidas adequadas para salvaguardar os direitos do titular dos dados – item 2(b), e em razão do consentimento livre e informado do titular dos dados – item 2(c). Apesar de reduzidas em número, a última exceção é ampla e baseada em um critério problemático, especialmente no contexto analisado.

Diversos autores vêm questionando a efetividade de se proteger o titular por meio de seu consentimento informado como elemento suficiente para servir de exceção ao direito de não ser submetido a decisões automatizadas. Kuner e outros (2017, p. 1) questionam "como é possível obter o consentimento informado em relação a um processo que pode ser inerentemente não transparente (uma "caixa preta"[black box])?".[12] Os autores também se perguntam se, ainda que seja possível explicar um processo algorítmico, seria possível fazê-lo em termos inteligíveis para o titular dos dados e se seria, nessa lógica, necessário um consentimento específico para cada situação em que um algoritmo de tomada de decisão for aplicado, como no caso de contextos financeiros, empregatícios ou médicos (Kuner e outros, 2017).

Mais contundente, ainda sobre o consentimento, é a crítica de Schermer. O autor não apenas afirma que há a possibilidade clara de que os sujeitos de dados não consigam avaliar adequadamente os riscos advindos de seu consentimento à submissão a processos automatizados de decisão, como deve ser considerado o fato de que tal consentimento, muitas vezes, gera benefícios concretos aos consumidores, como serviços gratuitos, enquanto os riscos envolvidos são menos tangíveis, levantando dúvidas sobre a própria possibilidade do titular consentir livremente e de maneira informada (Schermer, 2011). Portanto, pode ser argumentado que, nesse contexto, confiar no consentimento do titular, na verdade, diminui a sua proteção legal.

Além desse problema referente às exceções previstas pelo art. 22 (2), há impasses quanto à própria construção e delimitação do direito geral a não ser submetido a decisões automatizadas e *profiling*. Em especial, a definição das expressões a seguir destacadas: "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*". Tais expressões, como se pode perceber, contém substancial ambiguidade, permitindo interpretações tão diversas que podem representar a diferença entre a efetividade da norma ou seu simbolismo simplório. O mesmo problema está presente na lei brasileira, uma vez que o caput do art. 20 condiciona o direito de revisão a "decisões tomadas unicamente com base em tratamento automatizado".

Sobre o tema o Article 29 Working Party (2018) se posicionou no sentido de que a participação humana no processo de tomada de decisão precisa ser significativa, com autoridade e competência para influir no resultado, para que ela não seja considerada totalmente automatizada. O "*human in the loop*" não pode apenas referendar o resultado apresentado pelo algoritmo.

Por outro lado, restringir o alcance da proteção para aquelas baseadas apenas em processamento automatizado pode acabar por inutilizar a proteção. Veale e Edwards (2018) destacam que a definição do alcance da expressão é fundamental, uma vez que, dentre os sistemas de decisão automatizada utilizados atualmente, "poucos o fazem sem o que é frequentemente descrito como um "humano no circuito" [human in the loop] - em outras palavras, agem

como sistemas de apoio à decisão, em vez de tomar decisões autonomamente (p. 400)."[13]

Ainda, Rouvroy (2016) questiona se, mesmo em sistemas de recomendação, em que a decisão final cabe a um humano competente para se opor ou seguir recomendação, não haveria uma inescapável autoridade na recomendação do sistema algorítmico ante o posicionamento humano. A autora argumenta que, mesmo quando uma decisão automatizada serve como recomendação para a decisão final, ela poderá ser o elemento decisivo, transformando a própria noção do que entendemos como processo de tomada de decisão. Isso porque, para desconsiderar uma recomendação o operador humano terá que usar argumentos que seriam aferíveis quantitativamente tanto quanto as previsões algorítmicas. Nesse caso, todo espaço para alguma concepção pessoal de justiça ou mesmo de incerteza é eliminado em favor de uma mensuração preditiva avessa a riscos.

Por fim, como reafirmaremos adiante, o peso dado às análises algorítmicas é, em geral, determinante:

> Há alguma evidência de que, mesmo quando os sistemas se destinam explicitamente apenas a apoiar um tomador de decisão humano, por razões de confiança na lógica automatizada, falta de tempo, conveniência ou o que seja, o sistema tende a operar, de fato, como totalmente automatizado (Veale e Edwards, 2018, p.400).[14]

Dessa forma, um texto legal que desconsidera os impactos que mesmo um sistema algorítmico de recomendação pode ter, tanto para o titular quanto para uma lógica de governamentalidade algortímica[15] que impacta toda sociedade, se esquiva de realmente enfrentar o problema.

Já a respeito do outro problema de construção do artigo 22 da GDPR, que diz respeito ao requisito de que a decisão tenha efeitos legais ou "significativamente similares". O A29WP (2018) argumenta que estariam inclusas quaisquer decisões que "influenciam significativamente as circunstâncias, o comportamento ou as escolhas dos indivíduos envolvidos" ou que gere "exclusão ou discriminação (p. 10)"[16]. É importante, nesse ponto, estar atento ao fato de que a palavra utilizada é "influencia" e não "causa", sendo indicado por Veale e Edwards (2018) que tal incluiria até situações onde o comportamento do titular dos dados não é diretamente causado pela decisão, mas meramente influenciado por esta, como na possibilidade da perfilação alterar a forma como são dispostas as opções de escolha do titular ou gerando preços diferenciados, influenciando sua decisão.

Um terceiro ponto de incerteza quanto ao alcance do direito previsto no artigo 22 da GDPR diz respeito à definição dos sujeitos a quem os efeitos significativos se relacionam. Esses efeitos devem atingir diretamenta e especificamente o indivíduo que reivindica o direito ou, como já destacamos anteriormente com a possibilidade de efeitos coletivos do processo *profiling*, podem esses serem efeitos que afetam uma comunidade a que o sujeito pertença? Nesse caso, um exemplo pode ser esclarecedor:

> Por exemplo, um anúncio direcionado àqueles com nomes associados à etnia negra [black-sounding first names], sugerindo que a ajuda de um advogado de defesa criminal pode ser necessária, faz pouco para prejudicar a reputação da pessoa negra em questão, Latanya Sweeney, professora de segurança de Harvard que investigava o fenômeno quando ocorreu a ela, mas pode criar uma penumbra de preconceito racial e expectativas de comportamento ilegal em todo o grupo de negros, alguns dos quais serão mais vulneráveis do que a professora. (...) Não há razão para que essas decisões

> não se enquadrem no art. 22 - é a decisão que diz respeito ao titular dos dados que o aciona, mesmo que os dados utilizados para tomar a decisão venham parcial ou totalmente de outro lugar. De fato, esses fatores "relacionados aos pares" são a norma e não a exceção no aprendizado de máquina (Veale e Edwards, 2018, p. 402).[17]

Em casos desse tipo, Schermer (2011) indica que a análise tão somente de problemas individuais pode ser inútil, visto que, com uma quantidade virtualmente infinita de dados, sempre é possível encontrar uma explicação a respeito de determinada decisão que encubra ou ao menos levante dúvidas a respeito de alguma discriminação em relação a um indivíduo. Os problemas que põem em xeque a confiança no consentimento também podem ser aplicados aqui, uma vez que a ação individual para contestar decisões automatizadas que tomam larga escala criam um fardo excessivo para o indivíduo.

Mantelero (2016), em linha similar, reforça a importância das autoridades de proteção de dados para lidar com problemas gerados em escala coletiva, sugerindo uma abordagem com a participação de todos *stakeholders* para análise de riscos, supervisionado pelas autoridades de proteção de dados. Essa análise de risco, segundo o autor, deveria seria feita por controladores que pretendam trabalhar com análise de *big data* antes mesmo de se engajarem na atividade de tratamento de dados.

Desse modo, restringir a eficácia do artigo 22 da GDPR apenas a casos isolados de problemas individuais pode, como no caso dos demais problemas comentados, eliminar a efetividade do dispositivo.

Dada as questões levantadas sobre a abordagem tomada pela GDPR, avaliaremos quais novidades a Lei Geral de Proteção de Dados trouxe em relação à regulamentação europeia que acreditamos merecer alguma atenção em pesquisas e estudos adicionais sobre regulamentação de atividades de tratamento de dados e tomada de decisão automatizada.

4. Perspectivas e Alternativas Oferecidas pela Lei Geral de Proteção de Dados

Agora, na parte final do texto, considerando as avaliações iniciais a respeito das proteções jurídicas contra decisões automatizadas na GDPR e a inadequação de um sistema voltado para a proteção individual, iremos entrar em mais detalhes sobre como a Lei Geral de Proteção de Dados brasileira pode apresentar avanços na direção de um sistema protetivo de caráter coletivo no âmbito de decisões automatizadas. A LGPD, como ressaltado na introdução, possui um caráter mais principiológico e menos minucioso do que a GDPR. Assim, será preciso analisar como suas disposições serão interpretadas nos próximos anos. Aqui faremos alguns apontamentos iniciais sobre o texto final da lei e como autores brasileiros vem interpretando esse direito. O argumento a ser feito não é de que a LGPD apresenta um sistema protetivo mais robusto do que a GDPR, mas sim que, por influências e particularidades de outras áreas do direito brasileiro, a lei brasileira de proteção de dados traz algumas soluções que merecem atenção.

É importante ressaltar que não há, como no art. 22 da GDPR, um direito geral de não ser submetido a decisões totalmente automatizadas, incluindo o *profiling*, o que, mesmo com os problemas apontados no tópico anterior, dá a GDPR um caráter protetivo mais forte. Contudo, a LGPD traz ao longo de seu art. 20 direitos de titulares que recaem especificamente sobre tratamentos automatizados:

> Art. 20. O titular dos dados tem direito a solicitar 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, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º 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.
>
> § 2º 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.

Em primeiro lugar, apesar de não haver o direito a não ser submetido a decisões automatizadas, há expressamente, no *caput* deste artigo, um direito à revisão de decisões totalmente automatizadas que afetem o interesse do titular. Essas decisões incluem, mas não se limitam àquelas ligadas a formação de perfis comportamentais. Destaca-se que o termo "interesse" dá maior abrangência a essa norma, não sendo necessária a verificação de uma violação de um direito específico para que o art. 20 possa ser invocado. O simples fato de uma decisão totalmente automatizada afetar interesses do titular (o que também inclui ameaças a direitos) já é o suficiente para sua aplicação.

Portanto, ao se diferenciar da GDPR, que restringe a incidência de seu art. 22 para decisões automatizadas que produzam efeitos legais ou, de maneira similar, significativamente afete o titular, a LGPD torna possível uma tutela preventiva por parte do titular, antes mesmo de se caracterizar um dano efetivo. Ainda que a GDPR fale que é necessário que a decisão automatizada tenha efeitos legais ou "significativamente similares", a LGPD evita a vagueza dessas expressões da norma europeia pela menção expressa a interesses e, como veremos no final deste tópico, pela principiologia adotada na lei, que inclui, por exemplo, expressamente o princípio da não-discriminação entre aqueles que devem ser observados pelo controlador de dados.

Assim, havendo suspeita de que decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade possam vir a lhe causar qualquer dano, o sujeito de dados poderá se antecipar para, antes de ocorrido esse dano, solicitar a revisão do *profiling*. Esse direito, no texto original da LGPD, era previsto de maneira ainda mais robusta, como um direito à revisão humana, até que a Lei 13.853/19 alterou algumas disposições originais da LGPD e, por meio do veto presidencial, a revisão não mais requer o envolvimento de um humano. Não se sabe, ainda, até que ponto essa alteração retira a eficácia do dispositivo ou se, do contrário, é possível dar efetividade, ainda assim, ao direito de revisão.

Ademais, o art. 20, §1º, estabelece direito a informação para o titular de dados, segundo o qual o controlador deve "fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial". Esse direito, assim estabelecido, pode ser compreendido como um direito à explicação? Para tomarmos uma posição a respeito, é preciso abrir breve parênteses para, em síntese, buscar compreender quais os argumentos que se sobressaem no debate internacional.

Goodman e Flaxman (2017) defendem

fortemente a existência de um direito à explicação na GDPR. Este seria decorrente de seus artigos 13, 14 e 15, como salvaguarda estabelecida pelo art. 22, aplicável a decisões totalmente automatizadas. Esses artigos garantem ao titular dos dados que, se for o caso, ele seja previamente informado e tenha acesso (i) à informação acerca da existência de decisão automatizada, inclusive perfilação, e, pelo menos nestes casos, (ii) a informações significativas a respeito da lógica envolvida e (iii) da existência de consequências significativas previstas. No entanto, os autores reconhecem que algoritmos complexos, que empregam técnicas de aprendizado de máquina, apresentam barreiras técnicas na busca de uma explicação significativa. Desses três itens, aquele de mais difícil apreensão quanto a seu sentido diz respeito ao possível conteúdo de "informações significativas a respeito da lógica envolvida na perfilação ou na mineração".

Na direção oposta, Wachter, Mittelstadt e Floridi (2017) argumentam a favor da não existência desse direito à explicação. Os autores defendem que, embora o art. 22, item 3 da GDPR tenha previsto salvaguardas para o titular caso ele seja submetido a uma decisão automatizada, o direito à explicação não está entre eles. A sua única previsão se encontra no Considerando 71, que não é vinculante. Ainda, os autores argumentam que os arts. 13 e 14 estabelecem apenas um dever *ex ante* de notificar o titular a respeito da funcionalidade do sistema, de forma que não podem ser usados para requerer um direito *ex post* de explicação de uma decisão específica. No entanto, os autores admitem que dentro dos limites do direito de acesso previsto no art. 15, item 1, (h), é possível que a jurisprudência estabeleça um direito à explicação de decisões específicas.

Uma forma de terceira via é adotada por Selbst e Powles (2017) ao argumentarem a favor de um alargamento do conceito do direito à explicação, sem se prender ao momento em que ele pode ser exercido, isto é, se pode ser exigido pelo titular *ex ante* ou *ex post*, e se deve ser de uma decisão específica ou sobre o sistema de tomada de decisão. Os autores alegam que, se de fato garantido, mesmo um direito à explicação que incida apenas sobre a lógica envolvida, permitiria ao titular inferir como isso se aplica a uma decisão específica. Portanto, para esses autores, a grande preocupação que se deve ter na efetivação de um direito a explicação é se ele garante aos titulares meios para entender a lógica do sistema de decisão automatizada a qual foram submetidos e, com isso, exercer seus direitos.

Dados esses argumentos, defendemos que no art. 20, §1º, da LGPD estão as bases teóricas e legais para um direito à explicação. No mesmo sentido que argumentado por Selbst e Powles, não é necessário que a lei estabeleça procedimentos e parâmetros rígidos para o cumprimento dessa norma, desde que esse os titulares, através do exercício desse direito, realmente tenham acesso e possam compreender da lógica normativa (não a técnica) envolvida na decisão, possibilitando assim o exercício de outro direitos (sejam eles direitos previstos pela própria LGPD ou direitos mais amplos trazidos pelo ordenamento jurídico).

Renato Leite Monteiro (2018) sustenta, ainda, que o princípio da transparência e o microssistema de proteção ao consumidor em relações de concessão de crédito já criavam um direito à explicação nesse âmbito específico. A Lei Geral de Proteção de Dados, então, para o autor, reforça e amplia esse direito para qualquer tipo de tratamento automatizado de dados.

No entanto, a lei ainda põe a salvo os segredos comerciais e industriais, sem definir seus limites, devendo ser observados caso a caso. A respeito desse ponto, o art. 20, §2º, possui uma disposição de grande importância e que não pode ser negligenciada, que vai além da simples salvaguarda de se obter intervenção humana no processo de decisão. O dispositivo

prevê a possibilidade de, negada a informação sob o argumento da proteção do segredo comercial, a Autoridade Nacional de Proteção de Dados poderá apurar, mediante auditoria, a verificação de aspectos discriminatórios nos processos automatizados de tomada de decisão. Tal possibilidade pode servir como boa razão para que as empresas forneçam informações necessárias. Porém, para que isso seja efetivo, a autonomia da Autoridade Nacional e um quadro multi-disciplinar de especialistas serão fundamentais.

Outro ponto relevante trazido pela LGPD pode ser observado com a conjugação do art. 20, §1º, e o art. 12, §2º. Esse último estabelece que dados anonimizados (que, via de regra, não são considerados dados pessoais), serão considerados como pessoais caso sejam utilizados para a formação do "perfil comportamental de determinada pessoa natural, se identificada". Esse artigo ainda pode ser objeto de controvérsia, uma vez que condiciona a sua incidência a uma situação muito específica e de difícil verificação, uma vez que o perfil comportamental não precisa necessariamente identificar uma pessoa para que seus interesses sejam afetados, conforme argumentado no tópico 2.

Por esse motivo, Bruno Bioni (2019) defende que a identificação de determinada pessoa natural diz respeito não à identificação dela em uma base de dados de maneira abstrata, mas sim na sua identificação como pessoa que sofreu as consequências daquela atividade de tratamento de dados. Assim, segundo o autor, a lei brasileira teria uma abordagem em que "o foco não está no dado, mas no seu uso – para a formação de perfis comportamentais – e sua consequente repercussão na esfera do indivíduo (Bioni, 2019, p.80)." Por esse mesmo motivo, esses dados anonimizados usados para a formação do perfil comportamental, deverão ser considerados como dados pessoais pelo controlador no momento de explicar uma decisão automatizada, ampliando ainda mais as obrigações que recaem sobre os direitos previstos no art. 20.

Até o momento, argumentou-se que as proteções contra violações causadas por decisões automatizadas se tornam mais fortes ao incorporarem um caráter coletivo. No entanto, deve-se notar também que algumas proteções individuais, principalmente o direito à explicação, podem desempenhar outro papel importante. O pedido de explicação da decisão e a accountability algorítmica são importantes não apenas para evitar discriminação e erros. O que talvez seja mais importante, nesses casos, é o fato de que, ao procurar uma explicação para a decisão, as regras que regem esse processo de tomada de decisão se tornam explícitas. Ou seja, as variáveis consideradas, o objetivo da categorização realizada e a legitimidade de determinado processo decisório são expostos, abrindo a possibilidade de questionar os parâmetros adotados e, em um sentido mais amplo, a possibilidade de crítica.[18]

Ainda, uma última e importante ferramenta legal para combater a possível inefetividade do exercício de direitos individuais para problemas em escala coletiva, conforme demonstrados no início deste trabalho, o texto do art. 22 da LGPD mostra-se promissor:

> Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Ao dispor expressamente que os direitos dos titulares, o que inclui direito de revisão e explicação, pode ser "exercido em juízo individual ou coletivamente", decisões que afetem grupos, como narrado anteriormente, poderiam ser questionadas através de ações coletivas, dando maior efetividade à proteção jurídica

e reduzindo a assimetria de poder existente entre os grandes controladores de dados e os titulares.

Essa possibilidade de ação coletiva dos interessados, juntamente com a possibilidade de se tomar ações preventivas sem que direitos concretos tenham sido lesados, seria uma opção muito mais interessante para lidar, por exemplo, com o caso de discriminação de grupo citado na seção anterior, referente aos anúncios direcionados.

Se pela GDPR aqueles que não tiveram seus dados tratados ou mesmo que se sintam ameaçados em terem seus direitos lesados teriam poucas opções, todas individuais, para agir em defesa de seus interesses, pela LGPD alguma sociedade civil que represente legitimamente os interesses do grupo prejudicado, conforme as leis brasileiras, ou mesmo um grupo de sujeitos que se sintam coletivamente lesados, poderiam atuar preventiva e coletivamente para que os interesses do grupo fossem respeitados enquanto tal, evitando esse direcionamento enviesado e discriminatório.

Outro ponto da LGPD a ser contraposto à GDPR diz respeito à possibilidade dos indivíduos, na maior parte das vezes simples consumidores, de comprovarem o pontencial discriminatório do tratamento dado aos dados ou mesmo de comprovar dano concreto sofrido. Antoinette Rouvroy (2016), em um estudo para o Comitê Consultivo da Convenção 108 do Conselho Europeu, defende que a inversão do ônus da prova em casos em que há suspeita de discriminação gerada, mesmo que indiretamente, por atividades automatizadas de tratamento de dados no processo decisório, seria uma medida importante para garantir os direitos e garantias fundamentais dos titulares. Assim, a autora sugere que o controlador de dados é quem deveria provar que esse tratamento automatizado não gerou efeitos discriminatórios. Argumentamos aqui que a Lei Geral de Proteção de Dados permite essa inversão do ônus da prova, ao menos em processos judiciais, conforme o art. 42, §2º, em parâmetros parecidos com os defendidos pelo estudo citado anteriormente:

> Art. 42. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Além disso, o mesmo artigo que traz essa previsão, também ressalta, mais uma vez, o caráter coletivo das proteções trazidas pela lei, admitindo danos patrimoniais e morais, em caráter individual ou coletivo, bem como a ações coletivas para reparação de danos coletivos:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

No mesmo sentido do que foi argumentado até aqui, Zanatta (2019b; 2020) sustenta que a LGPD carrega consigo a tradição da tutela coletiva, harmonizando um sistema protetivo em conjunto com o Código de Defesa do Consumidor. Assim, os dispositivos supracitados da LGPD, em conjunto com o restante

do ordenamento e da tradição jurídica brasileira, segundo o autor, faz com que a Lei Geral de Proteção de Dados também passe a "*compor a disciplina comum das ações coletivas*" (Zanatta, 2020, p.2).

Por fim, há de se ressaltar os princípios trazidos pela LGPD. Como foi dito antes, a LGPD possui um caráter muito mais principiológico do que a GDPR. No entanto, isso não significa, necessariamente, uma menor proteção aos titulares, mas sim que é preciso de um maior trabalho interpretativo e regulatório para entender e definir as obrigações que recaem sobre as atividades de tratamento.

Além da privacidade, a lei brasileira elenca a autodeterminação informativa, o livre desenvolvimento da personalidade e os direitos humanos como alguns de seus fundamentos[19]. Ainda, no art. 6º são previstos 10 princípios gerais, dentre eles destacam-se o princípio da transparência[20] e da não discriminação[21], este último, vale ressaltar, que não é expressamente previsto na GDPR.

Portanto, ao empregar técnicas de tomada de decisão automatizada e de profiling, o controlador deve adotar medidas para que todos esses princípios sejam respeitados. Há então obrigações prévias de garantir que as técnicas empregadas não sejam discriminatórias, de assegurar que o titular possa ser informado e compreender a natureza do tratamento realizado a seu respeito, bem como ter o poder de influenciar esse tratamento, seja corrigindo informações errôneas ou complementando aquelas insuficientes.

Na mesma linha, Rafael Zanatta defende que o art. 20 da LGPD cria uma obrigação dialógica entre o controlador e o titular:

> Nesse sentido, a ação de "encaixar uma pessoa", a partir de seus dados pessoais e dados anonimizados, em um perfil social e *inferir algo sobre ela* implica em obrigações de três naturezas: (i) *informacional*, relacionada à obrigação de dar ciência da existência do perfil e garantir sua máxima transparência, (ii) *antidiscriminatória*, relacionada à obrigação de não utilizar parâmetros de raça, gênero e orientação religiosa como determinantes na construção do perfil, e (iii) *dialógica*, relacionada à obrigação de se engajar em um "processo dialógico" com as pessoas afetadas, garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e como decisões são tomadas (Zanatta, 2019a, p.22).

Essa obrigação dialógica, em combinação com a possibilidade de ações coletivas para combater danos e discriminações sistêmicas, a reversão do ônus da prova e a sólida principiologia adotada, podem fazer com que a LGPD, se for aplicada dessa maneira, seja vista como uma legislação de proteção de dados com propostas promissoras no que tange a regulamentação de sistemas de tomada de decisão automatizada.

Por fim, podemos observar que o cenário brasileiro já vem se organizando de forma a garantir proteções aos titulares através de demandas coletivas antes mesmo da entrada em vigor da Lei Geral de Proteção de Dados. Em agosto de 2018, o Idec (Instituto Brasileiro de Defesa do Consumidor) ajuizou Ação Civil Pública em face Concessionária da Linha 4 do Metrô de São Paulo, questionando o uso de câmeras de coleta de dados faciais e emocionais de passageiros.[22] Em decisão liminar, a coleta foi considerada ilegal pelo Tribunal de Justiça de São Paulo e interrompida.

Em fevereiro de 2020, em uma ação conjunta, seis entidades (Defensoria Pública do Estado de São Paulo, Defensoria Pública da União, Instituto Brasileiro de Defesa do Consumidor (Idec), Intervozes e ARTIGO 19, com apoio do Coletivo de Advocacia em Direitos Humanos [CADHu]), cobrou informações do Metrô de São Paulo a respeito da implementação de um

sistema de reconhecimento facial, solicitando uma avaliação prévia de impacto dos riscos, não só ligados à proteção de dados dos passageiros, mas também levantando a preocupação com os potenciais discriminatórios dessa tecnologia.[23]

Esses são dois importantes exemplos que reforçam a importância de uma perspectiva regulatória de atividades de tratamento de dados automatizadas (no caso, o reconhecimento facial e de emoções de passageiros do metrô) que leve em conta sua dimensão coletiva.

5. Considerações Finais

Argumentamos que sistemas de tomada de decisão automatizada e técnicas de *profiling* operadas pelo aprendizado de máquina são fenômenos que emergem e causam conseqüências em uma escala supra-individual e representam uma ameaça devido a seu potencial discriminatório. Assim, demonstramos que a regulamentação dessas atividades de processamento de dados deve ao menos considerar sua escala coletiva. O Artigo 22 da GDPR e seu direito de não estar sujeito à tomada de decisão totalmente automatizada é um exemplo de uma norma que pode ser importante, mas possui suas limitações, especialmente quando vista como um direito a ser exigido pelo titular dos dados individualmente.

Finalmente, apresentamos um arcabouço da Lei Geral de Proteção de Dados do Brasil referente à regulamentação da tomada de decisões automatizada e argumentamos que ela fornece alternativas importantes que merecem ser estudadas, com uma vasta gama de ferramentas para tutela coletiva, forte principiologia e um rol de direitos que permite que titulares, órgãos públicos do poder judicário como Ministério Público e Defensoria Pública, organizações da sociedade civil e também a Autoridade de Proteção de Dados criarem um robusto ecossistema de fiscalização e proteção dos titulares.

Referências

Angwin, J., Parris Jr, T. (2016, 28 de outubro) Facebook Lets Advertisers Exclude Users by Race. ProPublica https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Article 29 Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. (WP251rev.01). Acesso em 21 de maio de 2018, disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Banisar, D. (2011). Data Protection Laws Around the World Map. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1951416

BIONI, B. (2019). Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense.

Doneda, D. (2006) Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar.

Edwards, L., Veale, M. (2018) Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? IEEE Security & Privacy, 16(3), pp. 46–54.

Edwards, L. Veale, M. (2017) Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, Duke Law & Technology Review, 16(1), pp. 18-84.

Goodman, B. Flaxman, S. (2017) European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". AI Magazine, 38(3) pp. 50–57.

Hildebrandt, M. (2008) Defining Profiling: A New Type of Knowledge? In: Hildebrandt, M.; Gutwirth, S. (Eds.) Profiling the European Citizen: Cross-Disciplinary Perspectives. Cham/SWI: Springer Science, pp. 17-44.

Kaminski, M. Malgieri, G. (2019) Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations. U of Colorado Law Legal Studies Research Paper 19(28). Acesso em 5 de outubro de 2019, disponível em https://ssrn.com/abstract=3456224.

Kuner, C. e outros. (2017) Editorial: Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge? International Data Privacy Law, 7(1), pp. 1-2.

Larons, J.; Mattu, S.; Kirchner L.; Angwin, J. (2016) How We Analyzed the COMPAS Recidivism Algorithm. Acesso em 3 de outubro de 2020, disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Mann, M. & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 6(2). doi:10.1177/2053951719895805.

Mantelero, A. (2016) Personal Data for Decisional Purposes in the Age of Analyitics: From an individual to a collective dimension of data protection. Computer Law & Security Review, 32(2) pp. 238-255.

Martins, P. (2020) Categorizando Dados em um Contexto de Big Data: Em defesa de uma abordagem funcional. In XXIII Congresso Ibero-Americano de Direito e Informática, 2020, São Paulo. Memórias do XXIII Congresso Ibero-Americano de Direito e Informática. Timburi: Cia do eBook, p. 633-643.

Mendoza, I. Bygrave, L. A. (2017) The Right Not to be Subject to Automated Decisions Based on Profiling. In: Synodinou, T. Jougleux, P. Markou, C.; Prastitou, T. (Eds.) EU Internet Law: Regulation and Enforcement. Cham/ SWI: Springer, p. 77-98.

Mittelstadt, Brent. (2019) From Individual to Group Privacy in Big Data Analytics, Philosophy & Technology, 3(4), pp. 475–494.

Monteiro, R. L. (2018) Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais?, Instituto Igarapé, Artigo Estratégico nº 39.

Rouvroy, A. (2013) The end(s) of critique: data behaviourism versus due process. In: Hildebrandt, M.; De Vries, K. (eds.). Privacy, Due Process and the Computational Turn: the philosophy of law meets the philosophy of technology. Nova Iorque: Routledge, pp. 143-167.

Rouvroy, A. Berns, T. (2015). Governamentalidade algorítmica e perspectivas de emancipação:o díspar como condição deindividuação pela relação? Tecnopolíiticas e Vigilância. 18(2), pp. 36-56.

Rouvroy, A. (2016) "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. Council of Europe, Directorate General of Human Rights and Rule of Law. vol. T-PD-BUR (2015)09REV, 2016, pp. 1-37.

Schermer, B. (2011) The limits of privacy in automated profiling and data mining. Computer law & security review. 27, pp. 45-52.

Schermer, B. (2013) Risks of Profiling and the Limits of Data Protection Law. In: Custers, B. Calders, T. Schermer, B. Zarsky, T. (Eds.) Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. Berlin: Springer-Verlag, pp. 137-152.

Seaver, N (2019). Knowing Algorithms. In: Verseti, J., Ribes, D. (Eds.) digitalSTS: A Field Guide Study for Science & Technology Studies. Princeton & Oxford: Princeton University Press, pp. 412-422. Acesso em 20 de janeiro de 2020, disponível em https://digitalsts.net/wp content/uploads/2019/11/26_digitalSTS_Knowing-Algorithms.pdf.

Selbst, A. D.; Powles, J. (2017) Meaningful Information and the Right to Explanation. International Data Privacy Law. Oxford: Oxford University Press. 7(4), pp. 233-242.

Taylor, L. Floridi, L. Van der Sloot, B. (2017) Group Privacy: New Challenges of Data Technologies. Springer International Publishing.

Veale, M. Edwards, L. (2018) Clarity, surprises, and further questions in the Article 29Working Party draft guidance on automated decision-making and profiling. Computer law & security review, 34, pp. 398-404.

Wachter, S. (2019) Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. Acesso em 25 de maio de 2019, disponível em: https://ssrn.com/abstract=3388639

Wachter, S. Mittelstadt, B. Floridi, L. (2017) Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 7(2), pp. 76–99.

Zanatta, R. (2019a) Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Acesso em 19 de novembro de 2019, disponível em: http://rgdoi.net/10.13140/RG.2.2.33647.28328.

Zanatta, R. (2019b) A tutela coletiva na proteção de dados pessoais, Revista do Advogado, São Paulo, 39 n.144 (Nov. 2019), pp.201-208.

Zanatta, R. (2020) Tutela coletiva e coletivização da proteção de dados pessoais, In: PALHARES, F. (org.), Temas Atuais de Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, pp. 345-374.

Notas Finais

1 A Lei nº 14.010 de 2020 adiou a vigência das sanções previstas pela LGPD (arts. 52, 53 e 54) para 1º de agosto de 2021. Já a Medida Provisoria nº 959 de 2020, que previa o adiamento da vigência dos demais artigos da LGPD foi convertida na Lei nº 14.058 de 2020 com a remoção do dispositivo que previa esse adiamento. Deste modo, a LGPD passou a vigorar com com a sanção da Lei nº 14.058 em 18 de setembro de 2020.

2 Tradução livre do original "The process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category".

3 Tradução livre do original "The predictive models or supra-individual profiles assigned to individuals are based on infra-individual data deriving from a large number of individuals. In this process, data from any individual is just as valid as data from any other – *your data is as good as your neighbours*".

4 Para um aprofundamento sobre o que é Group Profiling, ver Hildebrandt, M. (2008) e Mittelstadt, B. (2019).

5 Sobre aprendizado de máquina, ver Seaver, N (2019).

6 Tradução livre do original "The aim of the processes of group profiling or clustering on the other hand is to highlight previously unknown, socially and visually imperceptible categories on the basis of data analysis without any reference to pre-existing information about these new groups or categories. Inclustering processes, individuals are placed by another person – which can be an automaticdata processing system – into socially and existentially a-significant "categories", which areimperceptible (because they emerge only as the process unfolds), and most often without anypossibility of being aware of what is happening or recognising themselves."

7 Tradução livre do original "what matters is whether the user behaves similarly enough to the assumed group to be treated as a member of the group".

8 Na GDPR, a definição de dados sensíveis [special category data] é trazida por seu art. 9 (1). A LGPD traz a mesma definição em seu art. 5º, II.

9 Para um aprofundamento na inadequação da categorização de dados sensíveis como um rol de "tipos" de dados pessoais mais suscetíveis a levarem a discriminações, ver Martins, P. (2020).

10 Como exemplo, uma reportagem do MIT Technology Review demonstra de forma interativa, a partir da base de dados do COMPAS, as dificuldades de se definir métodos justos e não discriminatórios para a predição algorítmica. Disponível em: https://www.technologyreview.com/s/613508/ai-fairer-than-judge-criminal-risk-assessment-algorithm/ Data de acesso: 6 de janeiro de 2020.

11 A Tomada de decisões e tratamento de dados automatizados são mencionados nos seguintes artigos da GDPR: 2(1), 4(2) and 4(4), 14(2)g, 15(1)h, 20(1)b, 21(5), 22(1), 35(3)a

12 Tradução livre do original "how can informed consent be obtained in relation to a process that may be inherently nontransparent (a 'black box')?".

13 Tradução livre do original "few do so without what is often described as a "human in the loop"- in other words they act as decision support systems, rather than autonomously making decisions."

14 Tradução livre do original "some evidence that even where systems are explicitly intended only to support a human decision maker, for reasons of trust in automated logic, lack of time, convenience or whatever, then the system tends to de facto operate as wholly automated".

15 Sobre governamentalidade algorítmica, ver Rouvroy, A. Berns, T. (2015)

16 Tradução livre do original: "In other words, the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned. At its most extreme, the decision may lead to the exclusion or discrimination of individuals.".

17 Tradução livre do original "For example, an advert targeted to those with "black-sounding" first names, suggesting that the aid of a criminal defence lawyer may be needed, does little to harm the reputation of the particular black, Harvard security professor, Latanya Sweeney, that was investigating the phenomenon when it occurred to her, but may arguably create a penumbra of racial bias and expectations of illegal behaviour around the entire group of black people, some of whom will be more vulnerable than our professor subject. (...) There is no reason why such decisions should not fall within art 22—it is the decision that concerns the data subject that triggers it, even if the data used to make the decision comes partly or wholly from elsewhere. In fact such "peer related" factors are the norm rather than the exception in machine learning".

18 Antoinette Rouvroy define crítica, nesse contexto, como "uma prática que suspende o julgamento e uma oportunidade de praticar novos valores, precisamente com base nessa suspensão. Nesta perspectiva, a crítica visa a construção de um campo de categorias oclusivas em si, e não na subsunção de um caso particular sob uma categoria pré-constituída". A autora argumenta que as práticas de tratamento de dados e profiling tornam a crítica difícil, ou em alguns casos, impossível. Para um maior desenvolvimento do argumento, ver- Rouvroy, A. (2013).

19 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos I - o respeito à privacidade; II - a autodeterminação informativa; VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

20 Art. 6º VI: transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do traamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

21 Art 6º IX: não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

22 A petição da Ação Cível Pública está disponível em https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Data de acesso: 03 de outubro de 2020.

23 Mais informações podem ser encontradas em: https://idec.org.br/noticia/acao-questiona-falta-de-transparencia-e-solicita-informacoes-sobre-licitacao-do-metro-de-sp Data de acesso: 03 de outubro de 2020.