REVISTA DOS TRIBUNAIS ONLINE®



THOMSON REUTERS

# O ARTIGO 20 DA LGPD E OS DESAFIOS INTERPRETATIVOS AO DIREITO À REVISÃO DAS DECISÕES DOS AGENTES DE TRATAMENTO PELOS TITULARES DE DADOS

Article 20 of the GDPL and the interpretative challenges to the right of data subjects to review the decisions of processing agents

Revista de Direito e as Novas Tecnologias | vol. 8/2020 | Jul - Set / 2020
DTR\2020\10211

**Micaela Barros Barcelos Fernandes**
Doutoranda em Direito Civil pela UERJ. Mestre em Direito da Empresa e Atividades Econômicas pela UERJ. Mestre em Direito Internacional e da Integração Econômica pela UERJ. Pós-graduada em Direito da Economia e da Empresa pela FGV/RJ. Graduada em Direito pela UFRJ. Advogada. Membro das Comissões de Direito Civil e de Defesa da Concorrência da OAB – Seção RJ. mibbf@yahoo.com.br

**Camila Helena Melchior Baptista de Oliveira**
Mestranda em Direito Civil pela UERJ. Graduada em Direito pela UERJ. Advogada. camilamelchior@hotmail.com

**Área do Direito:** Constitucional; Digital
**Resumo:** Este artigo trata dos desafios para interpretação do artigo 20 da Lei Geral de Proteção de Dados, que outorga aos titulares o direito à revisão das decisões que afetem seus interesses e sejam tomadas por agentes de tratamento, com base em tratamento unicamente automatizado de dados pessoais. Buscou-se, de um lado, contribuir para uma interpretação que confirme efetividade às normas de proteção à privacidade, a autodeterminação, e proteção contra discriminação dos titulares de dados, mas, de outro, que não impeça a inovação, o desenvolvimento de produtos e serviços suportados no uso de dados, inclusive por via da proteção ao segredo empresarial (industrial e comercial), considerando a atual preponderância de modelos de negócio que dependem cada vez mais do acesso e processamento massivo de dados.

**Palavras-chave:** Lei Geral de Proteção de Dados – LGPD – Direito à revisão – Direito à explicação – Segredo empresarial
**Abstract:** This article deals with the challenges for the interpretation of article 20 of the General Data Protection Law, which grants data subjects the right to review decisions made by processing agents based on the solely automated processing of personal data that affect their interests. On one hand, we tried to contribute to an interpretation that confirms the effectiveness of privacy protection, self-determination, and protection against discrimination against data subjects, but on the other hand, with an interpretation that does not prevent innovation, development of products and services supported in the use of data, including through the protection of business (industrial and commercial) secrets, considering the current preponderance of business models that increasingly depend on massive data access and processing.

**Keywords:** General Data Protection Law – GDPL – Right of review – Right of explanation – Business secret

**Sumário:**



## Introdução

Entre as várias questões trazidas pelo advento da Lei 13.709/2018 (LGL\2018\7222), a Lei Geral de Proteção de Dados (LGPD), inclui-se a dúvida sobre o alcance e os efeitos do seu artigo 20, que prevê aos titulares o direito à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

O enfrentamento das questões relacionadas ao chamado direito à revisão passa necessariamente pelo entendimento dos objetivos buscados pelo legislador quando da aprovação da norma legal, mas também da compreensão de que a LGPD se insere no ordenamento jurídico brasileiro, passando a integrá-lo e a ser integrada por ele.

A premissa que se coloca como chave para interpretação do chamado direito à revisão, portanto, é a de que o dispositivo que o prevê se insere em um sistema jurídico complexo, porém, unitário, o qual deve ser observado em sua integralidade no momento da aplicação pelo intérprete.

Assim, há que se atentar aos interesses tutelados pela norma específica, assim como a outros interesses com os quais aqueles se conjugam no ordenamento brasileiro, ora refletidos na própria LGPD, ora em outros diplomas legais. O objetivo de todo intérprete deve ser contribuir para aplicação da normativa de maneira que a tutela por ela pretendida seja eficaz.

Com o intuito de contribuir para a compreensão do contexto no qual se insere o direito à revisão previsto na LGPD e como o seu artigo 20 pode ser interpretado e aplicado, o presente trabalho se divide em seis partes. A primeira, em que são apresentados os princípios gerais da LGPD, com possíveis nortes de interpretação para as regras contidas na nova legislação, inclusive aquelas referentes ao direito à revisão. A segunda em que são propostas considerações sobre a amplitude do artigo 20 que trata do direito à revisão, para que sejam apontados seus alcances e limites. A terceira, em que se toma a experiência comparada sobre a revisão da fórmula algorítmica, especificamente o RGPD (Regulamento Geral de Proteção de Dados) no qual a lei brasileira se inspirou em grande parte, para referência de caminhos possíveis de interpretação em situações de dúvida sobre o conteúdo do direito à revisão. Na quarta parte, são apresentadas considerações sobre a ponderação que deve ser feita entre o direito à revisão e a observância aos segredos comercial e industrial, estes que podem ser utilizados pelos agentes de tratamento de dados como instrumentos de proteção de seus algoritmos. Na quinta parte, aborda-se o balanceamento do respeito à privacidade, à autodeterminação informativa e outros valores tutelados pela LGPD e os incentivos ao desenvolvimento tecnológico, bem como a questão do tratamento discriminatório feito pelo algoritmo, com distinção entre situações de discriminação possível e discriminação ilícita ou abusiva. Na sexta e última parte, são trazidas algumas considerações relativas a fatores regulatórios e técnicos que podem afetar o direito à revisão das decisões automatizadas, bem como questionada a atuação de outros órgãos de fiscalização, que pode se somar à atuação da ANPD.

A perspectiva adotada buscou, de um lado, garantir eficácia às normas de proteção à privacidade, autodeterminação e proteção contra discriminação dos titulares de dados, mas, de outro, não impedir a inovação, o desenvolvimento de produtos e os serviços suportados no uso de dados, considerando que vivemos em tempos em que os modelos de negócio dependem cada vez mais do seu acesso e processamento massivo.

## 1.Interpretação do artigo 20 em visão consistente com os princípios da LGPD

Como pressuposto ao exercício do direito à revisão de decisões automatizadas de dados pessoais, a Lei Geral de Proteção de Dados – LGPD, instituída pela Lei 13.709/2018 (LGL\2018\7222), previu que o titular dos dados deverá ter acesso, sempre que solicitado, a informações claras e adequadas sobre os procedimentos utilizados para se chegar a decisões que interfiram em sua esfera jurídica, resguardando-se os segredos comercial e industrial do controlador (art. 20, § 1º, da LGPD).[1]

Referida norma evidencia que o chamado direito à revisão, para além de instrumentalizar a proteção dos dados pessoais almejada pela LGPD por meio do processo de revisão propriamente dito, abrange o direito à explicação acerca da forma como os dados do titular são captados e utilizados pelos agentes de tratamento. Nesse sentido, a finalidade precípua do dispositivo é estabelecer balizas para as decisões automatizadas, de modo a evitar que resultados sem transparência reflitam posições discriminatórias[2], sem se descurar da proteção ao desenvolvimento econômico e tecnológico, bem como da livre-iniciativa e livre-concorrência (art. 2º, V e VI[3]).

Afinal, sabe-se que os algoritmos, cujo uso é cada vez mais frequente na época do *Big Data*, não processam dados de forma imparcial, sendo plenamente possível que incorporem "visões, idiossincrasias e valores das pessoas e empresas que os desenvolveram, assim como podem ser incompletos ou tendenciosos os dados utilizados para informar a tomada de decisão",[4] de modo que fatores discriminatórios ou premissas equivocadas acabam por interferir nas escolhas dos indivíduos e no seu acesso às diferentes oportunidades que se colocam.

Sob essa perspectiva, o direito à explicação deve incidir sobre qualquer forma de tratamento de dados pessoais, desde a coleta, mas, especialmente, sobre a sua utilização e controle dos seus resultados, evitando que o tratamento crie obstáculos ao livre desenvolvimento da personalidade dos titulares dos dados.

Mais do que isso, o direito à explicação dos critérios e os procedimentos utilizados pelo controlador para alcançar a decisão automatizada decorrem da própria autodeterminação informacional do cidadão, que

deve possuir o controle de seus dados pessoais, bem como dos princípios da LGPD que estabelecem a clareza e o acesso a informações pelo titular dos dados[5].

Esta interpretação é a mais consistente com os princípios arrolados pela LGPD, entre os quais o princípio do livre acesso (art. 6º, IV, art. 9º; e arts. 18, 19 e 20 da LGPD), o qual garante aos titulares consulta gratuita e adequada sobre a forma, duração e finalidade do tratamento, bem como sobre quais de seus dados pessoais foram coletados, seja o tratamento automatizado ou não[6].

Já o princípio da transparência (art. 6º, VI, art. 9º; art. 10, § 2º; art. 18, I, II, VII e VIII; e art. 20, da LGPD) prevê o dever de *accountability* dos agentes de tratamento, o qual requer seja garantido o necessário compartilhamento de "informações claras, precisas e facilmente acessíveis" sobre o tratamento dos dados pessoais, inclusive no que tange à segurança das informações, bem como sobre os próprios agentes de tratamento, resguardados os segredos comercial e industrial.

A seu turno, o princípio da qualidade dos dados (art. 6º, V, da LGPD) também assegura que os dados coletados e tratados devem ser exatos, claros, relevantes e periodicamente atualizados conforme a necessidade e de acordo com a finalidade do tratamento. Em consequência, o titular dos dados deve ter acesso aos dados tratados para que possa verificar a exatidão de tais informações, podendo requerer a revisão das decisões automatizadas em caso de incompatibilidades[7].

No mesmo sentido, o princípio da não discriminação (art. 6º, IX) veda que o tratamento de dados seja realizado para fins discriminatórios ou abusivos, decorrendo daí a necessidade de serem concedidas informações acerca do tratamento automatizado que, muitas vezes, engloba tais riscos. Nessa esteira, o direito à explicação serve também à concretização dos princípios da prevenção (art. 6º, VII, da LGPD) e da responsabilização e prestação de contas (art. 6º, X, da LGPD), de maneira que garante-se ao titular dos dados o acesso a informações para que este possa verificar se o agente de tratamento adota, de modo adequado, medidas de segurança aptas a evitar o surgimento de danos decorrentes do seu tratamento e a proteger os dados pessoais nos termos da lei.

Por fim, em decorrência do princípio da finalidade, o agente de tratamento deve informar os fins legítimos que o tratamento busca alcançar[8] e, para concretizar tal obrigação, o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizem (art. 37 da LGPD), de forma a informá-las quando solicitado pelo titular dos dados pessoais.

Conclui-se, assim, que aquilo que o artigo 20 tutela, a despeito de sua redação lacônica, é mais do que uma formal possibilidade de revisão de dados por parte do titular. A sua previsão acaba por impor ao agente de tratamento prontidão para esclarecimentos e revisão de procedimentos a qualquer tempo, especialmente em situações em que o processamento está sujeito a contínuas mutações. Esta revisão deve ser constante, e não apenas sob demanda do titular, mas inclusive por iniciativa própria ou por iniciativa de parceiros de negócios, ou quaisquer terceiros implicados na cadeia de dados, de modo a garantir a observância de todos os princípios anunciados no artigo 6º da LGPD, notadamente os da finalidade, da transparência e da não discriminação.

Importa, portanto, perquirir qual a extensão de tal direito à revisão, bem como as hipóteses em que os segredos comercial e industrial constituirão óbice ao exercício de tal direito.

**2.Alcance do direito à revisão**

Para que os interesses contemplados pela LGPD sejam efetivamente tutelados, o direito à revisão previsto no artigo 20 da LGPD não deve se restringir, na prática, apenas à revisão de um resultado passível de questionamento pelo titular dos dados, ou seja, incidir apenas no momento em que este resultado lhe é apresentado, portanto, necessariamente depois de sua inserção e de seu processamento automatizado.

A considerar a literalidade do *caput* do artigo 20 (conforme sua redação final, tendo em vista que o dispositivo legal teve uma redação original, alterada pela Medida Provisória 869/2018 (LGL\2018\12628), depois novamente alterada pela Lei 13.853/2019 (LGL\2019\5777)), a LGPD, diferentemente de outras normas, como a Lei de Cadastro Positivo[9], só prevê expressamente a possibilidade de o titular dos dados pedir a *revisão* de decisões automatizadas, o que sugere acesso sempre em momento posterior à coleta de dados e desenvolvimento do algoritmo que os processa:

"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. (Redação dada pela Lei nº 13.853, de 2019 (LGL\2019\5777))

§ 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." (grifos nossos)

Entretanto, como já apontado na primeira parte deste trabalho, o direito à revisão do artigo 20 contempla também o direito à explicação sobre o uso dos dados, em interpretação consistente com todos os princípios informadores da disciplina da proteção de dados. Os termos revisão e explicação, a rigor, referem-se a duas etapas distintas do tratamento de dados; não são sinônimos.

Apesar de o *caput* do artigo 20 da lei mencionar expressamente *revisão*, se lido em conjunto com vários outros dispositivos, entre os quais, o seu § 1º com os incisos I, VI e IX do artigo 6º, que tratam dos princípios da finalidade, da transparência e da não discriminação, respectivamente, o artigo 9º, que prevê o direito de acesso às informações sobre o tratamento dos seus dados, e o artigo 19, que se refere à confirmação de existência ou acesso a dados pessoais mediante requisição, permite outro entendimento.

Portanto, o termo revisão mencionado no *caput* do artigo 20, em consistência com toda a base principiológica da LGPD, compreende também a possibilidade de explicação sobre quais dados especificamente são utilizados e para que fins. O direito à revisão do artigo 20 é, pois, um direito à revisão *lato sensu*, amplo, de que são espécies o direito à explicação sobre o uso dos dados, desde a sua solicitação e/ou captura, e sua revisão, pós processamento e tomada de decisão.

Cabe, sem prejuízo, a ponderação de que não há exatamente um *direito* à revisão, na medida em que a revisão prevista consiste em verdade em um instrumento de proteção do titular de dados para proteção dos seus direitos, estes, sim, de privacidade, autodeterminação e não discriminação ilícita ou abusiva. A revisão não deve ser entendida como um fim em si, mas um instrumento para o atingimento de certos fins, estes efetivamente tuteláveis como direitos do titular.

A esta ponderação, adicione-se a questão sobre o que se deve entender como *decisões tomadas unicamente com base em tratamento automatizado* para que se deflagre a possibilidade de o titular pedir a revisão de decisões que afetem seus interesses.

A LGPD, diferentemente do Regulamento Geral de Proteção de Dados (RGPD)[10], norma europeia na qual o texto brasileiro se inspira, mas não copia exatamente, não proíbe o tratamento totalmente automatizado de dados. Muito pelo contrário, ela expressamente o autoriza no artigo 20, prevendo, em proteção aos titulares, o direito à revisão.

Compreende-se que é diante da automatização e tratamento massivo de dados que o risco de os dados pessoais dos titulares serem mal utilizados e causarem eventuais prejuízos se configura, ou se amplia, a ponto de justificar uma previsão específica do legislador sobre este risco (no caso da União Europeia, inclusive pela vida de vedação, via de regra).

Todavia, a expressão *unicamente* contida no artigo 20 da LGPD pode ser capciosa. Em primeiro lugar, a mera presença de uma pessoa na cadeia de etapas decisórias que levam a um determinado resultado não é assecuratória de decisões justas, em conformidade com o ordenamento jurídico. E, algumas vezes, tal presença pode ser apenas formal, mas não substancial.

Se há, por exemplo, uma pessoa que age em nome do agente de tratamento, mas atua como simples comunicante de uma decisão tomada por algoritmo, como um atendente em um banco que comunica a um cliente sobre a negativa de financiamento solicitado depois da inserção dos dados em um computador, tal situação não pode se confundir com aquela em que o resultado que afeta os interesses do titular resultou de processo decisório em que há efetiva interferência humana na análise de crédito.

Deve-se também considerar que um processo decisório totalmente automatizado não necessariamente conduz a uma decisão final injusta, assim como aquele que conta com interferência humana não necessariamente conduz a uma decisão final de acordo com a legalidade constitucional, em que eventual classificação é justificada e amparada no ordenamento, se a interferência humana foi feita, por exemplo, de maneira indevidamente discriminatória.

Embora se reconheça que, com a automatização os riscos de processamentos que levam a resultados indevidamente discriminatórios aumentam, eles não estão necessariamente vinculados a um processo de decisão unicamente automatizada. A pressuposição de que o problema de decisões que violam a normativa vigente e garantias de não discriminação decorrem somente da automatização, como parece ter sido a escolha estrutural da lei, pode resultar em situações injustas, mas aparentemente não questionáveis. Os intérpretes e os aplicadores da lei devem estar atentos a esta possibilidade.

Cabe, portanto, uma interpretação funcional do dispositivo, para que seja alcançado o objetivo do legislador, isto é, garantir ao titular de dados um tratamento não discriminatório e que respeite a privacidade e a autodeterminação do titular dos dados, como se depreende de outros dispositivos contidos na lei, notadamente aqueles relacionados aos princípios tratados na primeira parte deste

trabalho, e de outras normas relacionadas ao tratamento de dados já existentes no ordenamento. O dispositivo foi previsto em proteção das pessoas cujos dados estão sendo tratados para que não sofram com efeitos que estejam em desacordo com o ordenamento jurídico, e é por este norte que sua interpretação deve ser realizada, tanto para ampliar quanto para reduzir seu campo de aplicação.

Justamente em decorrência da atenção que deve ser dada aos objetivos da previsão legal do direito à revisão, cabe ressalvar que o remédio previsto no artigo 20 para a hipótese de um resultado de processamento indevidamente discriminatório pode ser inócuo. Lembre-se de que sua redação foi sucessivamente alterada em intervalos curtos de tempo e antes mesmo da entrada da LGPD em vigor. A versão final acaba por incorrer em risco de *looping* eterno, uma vez que não obriga que a revisão dos dados seja humana.

Portanto, ainda que o titular possa pedir a revisão do resultado, esta poderá ser feita por meio de novo processamento automatizado, e assim o titular poderá novamente pedir outra revisão, em repetição infinita de execuções. Mais importante do que saber como eventual revisão no resultado é providenciada, é assegurar que o resultado esteja em linha com a legalidade do ordenamento. E eventual ilegalidade pode se dar em mais de uma etapa do processamento, originando resultados que devem poder ser questionados pelos titulares de dados cujos interesses tenham sido atingidos.

Então, importa saber, na prática, qual a amplitude do direito à revisão – em outras palavras, qual o grau de transparência e de explicação que pode ser exigido pelo titular ao agente de tratamento, e em que momento este direito pode ser exercido. Pode ele saber quais dados de sua titularidade foram inseridos, mas não necessariamente a fórmula de processamento, os critérios para a tomada da decisão? O fato de a decisão ser automatizada sempre deve ser comunicado ao titular a cada etapa do processamento?

Estas questões, todas do interesse do titular, naturalmente, se conectam também com outros interesses, ora dos próprios agentes de tratamento, ora de eventuais terceiros de alguma maneira afetados pelo tratamento de dados (outros titulares). Sob a perspectiva dos agentes, que possuem enorme diversidade em configuração, tamanho e interesses, sabe-se que os dados de titulares podem ser usados em situações múltiplas, algumas com fins econômicos, outras não.

Tome-se, por exemplo, uma seguradora de saúde que utiliza os dados de um segurado para fins de cobertura de um tratamento médico, uma secretaria de saúde municipal que precisa desenvolver uma política de atendimento em postos de saúde em vigência de grave epidemia e precisa fazer estatísticas com dados de todos os cidadãos, um condomínio de apartamentos residenciais que utiliza os dados dos condôminos para fins de administração das despesas comuns, ou mesmo de seus visitantes para fins de segurança interna, um escritório de advocacia que utiliza dados dos clientes para fins de defesa de seus interesses, ou uma pequena padaria que guarda o endereço dos clientes para os quais faz entrega – as possibilidades são infinitas. Há situações muito diferentes e para os fins mais variados: algumas em que há interesse público a ser levado em conta, outras não, mas, sob o aspecto do direito à revisão, todos os agentes de tratamento devem atuar com base no mesmo dispositivo legal.

Justamente porque em função do suporte fático e dos objetivos na utilização dos dados, existem situações em que há nenhum ou quase nenhum processamento, e outras em que ele é intenso. Pode-se dizer que muitas vezes o que importa não é exatamente o dado, que talvez isolado nada represente de importante para o agente, mas a informação que resulta do tratamento do dado, pós-tratamento.

Por esta razão, o princípio de transparência (artigo 6º, VI, da LGPD) impõe não apenas transparência sobre quais dados estão sendo coletados, mas para quê e como os dados estão sendo tratados – em função dos objetivos do tratamento e das informações efetivamente resultantes, é que as partes (titulares e agentes) podem compreender e se posicionar quanto à defesa dos seus respectivos interesses particulares, sendo possível fazer a ponderação destes com outros interesses também protegidos em nosso ordenamento.

O intérprete da lei que atuará em cada caso concreto só terá condições de verificar quais mecanismos de proteção de múltiplos interesses incidem (e como incidem), ao conhecer não apenas os dados utilizados, mas quem os usa e quais os fins de sua utilização, que podem, dependendo das circunstâncias, afetar mais ou menos os direitos de privacidade e autodeterminação, e se coordenar com outros direitos que devem também ser ponderados no balanço de interesses em jogo.

### 3.Conteúdo do direito à revisão: entre a fórmula algorítmica e a sua racionalidade

Diante do exposto, importa saber o que se revisa, exatamente. O *output* (resultado), o processo (a metodologia, o algoritmo) e o *input* (os próprios dados lançados, o que inclui dados de terceiros, também titulares, e não apenas do titular que solicita a revisão). Sobre o que o titular tem ingerência?

E, no outro lado desta questão, a que deveres de informação os agentes de tratamento estão vinculados? A resposta a esta pergunta é fundamental para orientação do agir de todas as partes nestas relações. E ela pode ser determinante, do ponto do intérprete, para saber como agir. Por

exemplo, um empreendedor, ao saber exatamente quais deveres e riscos assumirá em novo negócio com relação a dados de terceiros, pode decidir, inclusive, por não empreender, ou por empreender sabendo do tamanho dos riscos, e das medidas que deve tomar em segurança dos interesses de terceiros e seus próprios.

O desafio é que algumas vezes, mesmo o agente de tratamento, não tem acesso preciso de todas estas informações, seja porque encomendou o algoritmo, ou parte dele, de terceiro, seja porque o algoritmo pode usar mecanismos de *machine learning* ou *deep learning*[11]. Muitas vezes, portanto, os resultados são atingidos sem que seja possível reconhecer os padrões adotados pela inteligência artificial, feitos com base em estatísticas e correlações sobre as quais os seres humanos não têm controle.

Ainda que haja dificuldade de compreensão, tal fato não afasta o direito à revisão de que é titular a pessoa humana afetada pelo uso dos dados. Neste cenário, ganha ainda mais relevância a adoção de salvaguardas adequadas pelos agentes de tratamento que serão mais bem explicitadas adiante – se o algoritmo usado para determinado tratamento de dados se tornar uma caixa-preta, fechada em sua lógica, o controlador deverá adotar mecanismos para assegurar que do seu uso não se originem resultados que violem as normas de proteção da pessoa humana previstas no ordenamento, o que lhe impõe o dever legal de estar constantemente revisando o algoritmo, seja por meio de testes, ou de auditorias técnicas, internas ou externas, com adoção de procedimentos para garantir a tutela dos interesses de todas as pessoas afetadas.

### 3.1.A experiência comparada – Grupo de Trabalho da Diretiva 95/46/EC: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

Na tentativa de oferecer um norte de interpretação quanto à extensão do direito à explicação como expressão do direito à revisão, deve-se observar os parâmetros utilizados pelo Grupo de Trabalho instituído pelo artigo 29 da Diretiva 95/46/CE (Grupo de Trabalho)[12], para interpretar o art. 22 do Regulamento Europeu Geral de Proteção de Dados Pessoais, que inspirou a LGPD. O Grupo de Trabalho entende que três medidas explicativas primordiais devem ser tomadas no caso de decisões automatizadas.

A primeira delas, informar ao titular dos dados o seu envolvimento nesse tipo de tratamento. Ressalve-se, entretanto, que o excesso de informação pode acabar se tornando ineficaz como mecanismo de proteção dos interesses do titular. Afinal, se, para cada passo em um processo decisório, houver aviso por parte do agente de tratamento, correr-se-á o risco de o titular simplesmente saturar, e, para seguir adiante em negociação do seu interesse que envolva processamento de seus dados, declarar que toma conhecimento da situação, sem realmente tomar (pense-se em sucessões de cliques de autorização para um determinado cadastro eletrônico feito pela Internet, por exemplo).

Em segundo lugar, o conceito de *meaningful information* ganha relevância – o agente de tratamento de dados não tem que oferecer informações complexas, mas sim informações úteis ao titular, portanto, quais dados pessoais foram utilizados, de que forma e qual a finalidade do seu uso. A lógica é de tentar facilitar o entendimento, pelo modo como as informações devem ser passadas[13], recomendando-se que, quando possível, o controlador utilize efeitos visuais ou técnicas interativas que facilitem a compreensão.

A título exemplificativo, em matéria de perfilização, são informações relevantes as categorias de dados que foram ou serão utilizadas, as razões pelas quais tais categorias são pertinentes, o modo como os perfis são criados (por exemplo, a partir de estatísticas – informações que podem ser de difícil extração em processos de *machine learning* ou *deep learning*) e sua relevância para a decisão automatizada. Para facilitar o processo de transparência, é preciso, ainda, que os titulares dos dados pessoais disponham de mecanismos para checar em que perfis estão incluídos.

Sob essa perspectiva, portanto, é imprescindível que o titular dos dados receba informações suficientes à compreensão das razões que levaram à certa decisão automatizada, sem que seja necessário partir para uma explanação complexa acerca dos algoritmos utilizados ou para a divulgação do algoritmo por completo – que seguramente esbarraria na proteção aos segredos comerciais e industriais.

Para elucidar a questão, pense-se na hipótese destacada pelo Grupo de Trabalho em que determinado controlador de dados utiliza o sistema de *credit scoring* para avaliar pedidos de empréstimo. O controlador deve explicar de que modo o processamento desses dados ajuda na tomada de decisões justas e responsáveis, fornecendo detalhes sobre as principais características consideradas na tomada da decisão, a fonte dessa informação e a sua relevância. Tais dados podem incluir informações fornecidas pelo titular no formulário de solicitação, condutas prévias como atrasos de pagamento da conta, bem como registros públicos de informações sobre fraude e insolvência. Acresce-se a tais sugestões, que os controladores também devem indicar, no primeiro contato com o seu cliente, quais sistemas de bureaus de crédito, como o oferecido pelo Serasa, serão utilizados para a captação dos dados pessoais.

Partindo-se para a terceira medida explicativa, o Grupo de Trabalho propõe que o controlador de dados explicite o significado e as consequências previsíveis de determinado tratamento de dados pessoais ao seu titular. No caso das decisões automatizadas do aplicativo da Uber, por exemplo, que atribuem notas de 1 a 5 estrelas aos passageiros com base no monitoramento de seus comportamentos conforme parâmetros preestabelecidos, os usuários são informados de que atitudes contrárias às diretrizes da comunidade – como tratar todos com respeito e respeitar a lei – podem resultar em diminuição da nota. Além disso, a Uber fornece dicas objetivas para que os usuários tenham a oportunidade de aumentar seu conceito no aplicativo, como não pedir para o motorista exceder o limite de velocidade ou avançar sinais vermelhos, não deixar lixo no carro, usar o cinto de segurança, não fazer o motorista esperar, entre outras. A consequência do descumprimento de tais diretrizes é a diminuição da nota do usuário que, nos casos mais graves, pode levar à sua exclusão da plataforma.

Seguindo a mesma linha informativa, o Grupo de Trabalho cita a hipótese das companhias de seguro que utilizam processo de decisão automatizada para definir os prêmios de determinado seguro de automóveis, com base no monitoramento do comportamento de direção dos clientes. Para explicitar as consequências previsíveis de determinado comportamento na lógica do algoritmo, a seguradora deve indicar que a direção perigosa pode interferir na lógica do algoritmo e resultar no pagamento de prêmio de valor mais elevado. Seria interessante, nesses termos, o fornecimento de um aplicativo que comparasse os resultados de motoristas fictícios, incluindo um com hábitos de direção perigosa, como aceleração rápida e frenagem de última hora, bem como o uso de gráficos que aconselhassem como melhorar esses hábitos e reduzir os prêmios.

Por fim, o Grupo de Trabalho recomenda que, em qualquer caso, os agentes de tratamento tomem salvaguardas adequadas para prevenir erros, inacurácias e discriminações que podem resultar de decisões totalmente automatizadas, o que impõe a todos que delas se utilizam a realização de constantes avaliações sobre os seus resultados, notadamente, como se viu, nas hipóteses em que o algoritmo é dotado de maior opacidade.

As medidas devem se dar de forma cíclica, vale dizer, não incidem somente no estágio de *design* do sistema, mas também continuamente no processo de perfilização que possa atingir a pessoa humana, visto que os resultados dos testes dessa fase do processamento devem alimentar novamente o sistema de *design*, evitando que eventuais problemas já identificados voltem a ocorrer.

As salvaguardas sugeridas de modo não exaustivo aos controladores de dados são as seguintes: (i) verificação regular da garantia de qualidade dos sistemas para assegurar que os indivíduos sejam tratados de maneira justa e não discriminatória; (ii) auditoria algorítmica, que teste os algoritmos usados e desenvolvidos pelos sistemas de *machine learning* e *deep learning* de modo a verificar se realmente estão funcionando como pretendido e não produzindo resultados discriminatórios, errôneos ou injustificados; (iii) contratação de auditor independente, especialmente quando as decisões automatizadas forem tomadas com base em perfis e tiverem um alto risco de impacto sobre a pessoa humana, fornecendo aos auditores todas as informações necessárias sobre como o algoritmo ou sistema de *machine learning* funciona; e (iv) na hipótese de algoritmos desenvolvidos por terceiros, exigência de garantias contratuais de que auditorias e testes foram realizados e de que o algoritmo está em conformidade com os padrões acordados. Pode-se pensar, ainda, em mecanismos de certificação para operações de processamento e elaboração de códigos de conduta para processos de auditoria envolvendo *machine learning*.

O controlador de dados também pode adotar medidas específicas como (i) garantir a minimização de dados, de modo a restringir ao máximo o uso de dados pessoais, notadamente quando é criado ou aplicado o processo de perfilização; (ii) usar técnicas de anonimização ou pseudonimização no contexto de criação de perfil; (iii) proporcionar meios facilitados para que o titular dos dados expresse seu ponto de vista e conteste a decisão tomada pelo controlador de dados; e (iv) criar Comitês de Revisão Ética para avaliar os possíveis danos e benefícios para a sociedade de mecanismos que utilizam perfilização.

Todas essas medidas auxiliam a maior transparência e controle sobre o uso de algoritmos em cumprimento ao disposto no art. 50, § 2º, I, *d*, da LGPD[14], que dispõe que o controlador de dados deve aditar "políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade", de modo a assegurar que os dados sejam coletados na medida da necessidade do tratamento e para o cumprimento da finalidade informada aos seus titulares, evitando-se desvios injustificáveis ainda que diante da opacidade inerente aos sistemas algorítmicos.

Além disso, a adoção das salvaguardas adequadas pode auxiliar o controlador de dados na apresentação do relatório de impacto à proteção de dados pessoais, previsto no art. 5º, XVII, da LGPD, traduzido na "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Afinal, adotando técnicas de transparência e minimização dos possíveis riscos no tratamento de dados associados ao desenvolvimento da

personalidade e cidadania do seu titular, o controlador poderá demonstrar o *compliance* com a proteção de dados pessoais.

A crítica que se faz, porém, é a de que não é possível extrair o grau de exigibilidade do referido relatório de impacto, na medida em que os arts. 4º, § 3º[15], e 38[16] da LGPD, parecem inferir que a sua apresentação só seria necessária quando houvesse solicitação da autoridade nacional. Além disso, a LGPD não dispôs acerca dos efeitos de eventual violação da obrigação de elaborar o relatório por parte dos controladores. Talvez se pudesse pensar que, em hipóteses de alto risco, os relatórios de impacto se tornariam obrigatórios – e não meramente recomendáveis[17].

### 3.2.Entre a opacidade e a transparência: a transparência em excesso e a possibilidade de manipulação de resultados do tratamento efetuado por determinado algoritmo

A transparência é princípio a ser observado no melhor interesse do titular, mas em excesso pode causar problemas, como o da já mencionada saturação da atenção da pessoa titular dos dados, resultando em pouca eficácia na efetiva proteção de seus direitos. Outro problema é permitir, a quem tem acesso à explicação e revisão sobre as decisões automatizadas, a manipulação do processamento e, em consequência dos resultados, um risco que deve ser igualmente considerado pelos desenvolvedores de algoritmos e todos os agentes de tratamento.

Esta manipulação pode ocorrer inclusive pelo próprio titular, em situação que pode se caracterizar como de abuso do direito, para obtenção de um resultado que lhe é favorável, mas em desacordo com a legalidade do ordenamento, e afetando indevidamente interesse de terceiros.

Ilustra-se a situação com singelo exemplo do *site* de mídia e entretenimento *buzzFeed* que, pelo processamento de algoritmos, realiza testes simples relacionados aos mais variados temas, para captura de dados. A pessoa interessada responde perguntas que possuem alternativas em múltipla escolha, recebendo determinado resultado ao final como: "quem é você na academia?" "Será que você manda bem no *home office*?" "Você é novaiorquino ou parisiense de coração?" – entre outros.

Na hipótese de um teste de "quem é você no seriado americano Friends", se a pessoa conhecer as principais características dos personagens, poderá manipular suas respostas pessoais sobre gostos e personalidade próprios, para que o resultado do algoritmo indique que ela se parece mais com o personagem de sua preferência. O exemplo é simplório. Na prática, têm-se teorias que envolvem o processamento de dados e técnicas de *machine learning* ou *deep learning,* bem como segredos comerciais e industriais que devem ser protegidos.

Evidencia-se, portanto, que a LGPD não almeja exigir dos controladores a transparência em excesso do tratamento realizado, o que poderia perpetuar ingerências dos titulares dos dados que não têm por objetivo a proteção dos seus dados pessoais ou do livre desenvolvimento da sua personalidade e que, portanto, não merecem tutela do ordenamento jurídico. Prepondera, nesse caso, a proteção ao livre desenvolvimento econômico e tecnológico, bem como à livre-iniciativa e concorrência, que também constituem fundamentos da lei de proteção de dados.

### 3.3.Direito à explicação contrafactual

Em algumas situações, pode ser útil que a explicação seja contrafactual, ou seja, se baseie em exercício de suposição sobre como o resultado seria sem certo processamento ou como o processamento deveria se dar para que outro resultado ocorresse. A ideia elaborada pelos autores Sandra Wachter, Brent Mittelstadt e Chris Russel[18] tem por base a premissa de que a explicação adequada é aquela que auxilia os titulares dos dados a compreenderem os motivos que levaram à determinada decisão automatizada.

Nesse sentido, o controlador de dados, quando instado a fornecer explicações sobre determinada decisão automatizada, deve fazer uma declaração *de como o mundo teria que ser diferente para que determinado resultado desejável ocorresse*. Por exemplo, se determinada decisão automatizada nega um pedido de empréstimo, o controlador indicará as medidas necessárias para que o titular dos dados tenha o resultado desejado de concessão do empréstimo – como a comprovação de renda anual em determinada faixa de valor, a retirada do nome do titular de cadastros negativos de crédito, entre outros.

Segundo os autores, na prática, são essas as informações que devem ser oferecidas em matéria de decisões de inteligência artificial ao titular dos dados. Explica-se ordinariamente o porquê de determinado fato ter ocorrido, sem que se adentre em explicações técnicas que explicitem as relações causais que acarretaram determinado resultado no tratamento de dados.

Nesse contexto, Caitlin Mulholland e Isabella Frajhof afirmam que a análise contrafactual serve à demonstração de que o tratamento de determinado algoritmo não é discriminatório, já que ajusta as formas de explicar sistemas de inteligência artificial com a capacidade cognitiva humana em compreender explicitações[19].

De fato, não se pode negar a importância do método de explicação contrafactual notadamente em sistemas de *machine learning* ou *deep learning*, em que não é possível explicitar as causalidades operadas pelo sistema, que escapam à compreensão humana. No entanto, mesmo nesses casos, como se viu, deve haver um controle do algoritmo por meio de medidas e procedimentos para prevenir erros, inacurácias e discriminações que podem resultar de decisões totalmente automatizadas, garantindo-se que tais decisões sejam tomadas por parâmetros merecedores de tutela pelo ordenamento jurídico[20].

Já na hipótese de algoritmos cuja forma de atuação, procedimentos e combinações de dados utilizados são conhecidos pelo controlador de dados, a técnica da explicação contrafactual pode se mostrar insuficiente, na medida em que, somente por meio das informações recebidas pelo titular sobre o que tem que ser alterado para se chegar ao resultado desejado, não é possível verificar e questionar a legitimidade dos critérios (conhecidos e) adotados pelo algoritmo para se chegar a determinada decisão e a sua conformidade com o ordenamento jurídico compreendido em sua unidade.

Relembre-se aqui que, ao fornecer *meaningful information,* o controlador não deve informar apenas os dados que foram utilizados, mas também, sempre que possível, a forma como foram utilizados para que se possa verificar se esta é capaz e destinada a atingir a finalidade almejada pelo tratamento. Sendo assim, se tais informações são conhecidas devem ser informadas ao titular dos dados, a fim de seja possível averiguar se o tratamento exercido pelo controlador é merecedor de tutela.

Exemplos de informações relevantes sobre a forma de tratamento dos dados que devem ser transmitidas são as combinações de dados feitas pelo algoritmo, os critérios utilizados para alcançar determinado resultado, se eventual perfilização era necessária ao alcance da finalidade do tratamento e o porquê, entre outros.

Frise-se, por fim, que tais informações devem ser passadas ao titular dos dados de forma clara, objetiva e simplificada[21], sendo certo que o dever de transparência do controlador será exercido de forma abusiva se, em razão da complexidade e desorganização da mensagem, não for possível a sua compreensão pelo titular dos dados.

**4.A observância dos segredos comercial e industrial. A sempre necessária ponderação entre interesses**

Sem prejuízo de a LGPD impor ao agente de tratamento o dever de permanente prontidão para esclarecimentos e revisão de procedimentos de tomada de decisão automatizados, justamente porque atenta à existência de diversos interesses que devem ser balanceados, o § 1º do artigo 20 estabelece que o dever de esclarecer a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada observará os segredos comercial e industrial.

Esta é uma exceção prevista para proteger o agente de tratamento como agente econômico que é, criador e promovedor da circulação de riquezas, não apenas em benefício próprio, mas da própria livre-iniciativa (artigos 1º, IV, e 170 da Constituição da República). A LGPD se insere em um sistema jurídico complexo, que contempla múltiplos valores, e que deve ser observado em sua integralidade no momento da aplicação pelo intérprete. Assim, há que se atentar aos interesses tutelados pelo *caput* do artigo 20, como também a outros interesses com os quais aqueles se conjugam no ordenamento brasileiro, ora refletidos na própria LGPD, ora em outros diplomas normativos. Por isso mesmo, o legislador estabeleceu que a LGPD tem por fundamento o respeito à privacidade e à autodeterminação informativa, mas também a vários outros valores aos quais estes dois se somam, inclusive o desenvolvimento econômico e tecnológico, a inovação (artigo 2º, V), a livre-iniciativa e a livre-concorrência (artigo 2º, VI).

É neste contexto que exsurge a proteção ao segredo empresarial, gênero do qual são espécies o segredo comercial e o segredo industrial, expressamente referidos nos §§ 1º e 2º do artigo 20 da LGPD; e no artigo 6º, VI, que trata do princípio da transparência, contudo, ressalva a proteção aos segredos comercial e industrial; além de outros em diversas passagens da LGPD[22].

O segredo, do ponto de vista empresarial, encerra situação de fato, em que determinada sociedade empresária possui conhecimentos técnicos ou de outra natureza que lhe dão vantagem na concorrência, seja para entrar no mercado, seja para disputá-lo em condições favoráveis[23]. O segredo (por exemplo, o *know-how* sobre certo processo ou aplicação), se tiver uso na produção industrial, será chamado de segredo industrial[24], e, se tiver uso no comércio ou na prestação de serviços, será chamado segredo comercial.

A proteção do segredo no ordenamento brasileiro está assentada também no artigo 195 da Lei 9.279/1996 (LGL\1996\56), a chamada Lei da Propriedade Industrial, que estabelece o crime de concorrência desleal para quem, seja por acesso lícito (por exemplo, por força de um contrato ou relação de trabalho) ou ilícito, divulga, explora ou utiliza, sem autorização do titular, o segredo empresarial[25]. Naturalmente, informações que são de conhecimento público não podem ser segredos empresariais, tampouco aquelas que sejam evidentes para pessoas com conhecimento técnico no assunto.

Os algoritmos, como sequência de instruções de processamento e solução de problemas que são para o cumprimento de objetivos definidos por seus programadores, portanto, guias de processamento de dados amplamente adotados por agentes de tratamento, podem ser classificados de diversas maneiras e, dependendo da forma de proteção que lhe for conferida por quem o desenvolveu ou adquiriu, podem ser considerados segredos de indústria ou de comércio[26].

Quando protegidos sob a forma de segredo empresarial, o seu titular, único autorizado a ter acesso à sequência de instruções, poderá invocar a necessidade de exclusividade para proteger seu negócio. Este argumento deve ser respeitado por terceiros, inclusive os titulares de dados processados. Esta foi justamente uma exceção prevista pelo legislador diretamente na LGPD, porque contrapõe dois interesses particulares, de um lado, o do titular de dados, e de outro, o do agente de tratamento que é titular de segredo industrial ou comercial.

No entanto, a ponderação sobre estes interesses deverá ser feita caso a caso. Isto porque o segredo empresarial pode também ser elemento de abuso do controlador de dados, que pode utilizar o argumento apenas para se proteger contra questionamentos dos titulares dos dados e de eventuais entes de fiscalização, mas no fundo não ter, de fato, um segredo empresarial que justifique a recusa à explicação ou à revisão da decisão pela qual é responsável.

A própria LGPD, se, de um lado, prevê o respeito ao segredo industrial ou comercial no § 1º do artigo 20, de outro, logo em seguida, no § 2º, diz que, em caso de não oferecimento das informações solicitadas a respeito de critérios e procedimentos adotados para a decisão automatizada fundado justamente no segredo, a autoridade nacional de proteção de dados poderá realizar auditoria para verificar eventuais aspectos discriminatórios, ou seja, a autoridade terá acesso ao segredo, com o fim de verificação de conformidade e não violação de regras de não discriminação pelos agentes de tratamento de dados. A lei, entretanto, não deixa clara a consequência posteriormente a esta verificação. Pode ocorrer de se constatar a inexistência de segredo a preservar, hipótese em que a informação deveria ser simplesmente liberada para acesso pelo titular de dados, ou, até mesmo, pode constatar a existência de segredo, porém, com mecanismo que atue de maneira discriminatória em desfavor do titular de dados, hipótese em que o agente de tratamento deve ser conduzido a corrigir a falha para não haver discriminação abusiva ou ilícita no processamento de dados, com alteração do resultado, mas mantido o segredo empresarial resguardado.

Ainda, sobre a possibilidade de ponderação de interesses, sem prejuízo desta verificação, que cabe ser feita pela ANPD na forma expressamente prevista em lei, mas também sempre ao Judiciário, que não pode se furtar do exame de qualquer ilegalidade[27], há outras ponderações que podem ser feitas, todavia, não com base especificamente no § 2º do artigo 20.

Embora transversal, a LGPD não afasta a incidência de outras normas sobre a matéria de que trata. Assim, fornecedores de produtos ou serviços deverão prestar contas aos titulares de dados também com base em outras normas, por exemplo, o Código de Defesa do Consumidor, o Marco Civil da Internet e outras que inclusive preveem a tutela de interesses públicos. Por exemplo, em segurança pública, saúde coletiva etc.

Como os mecanismos de balanceamento entre os diversos interesses, de natureza pública ou privada, funcionarão em complementariedade, dependem da atuação não apenas dos próprios particulares, como também da ANPD e outros órgãos de fiscalização e tutela. O ordenamento, ao fim, resulta do que o setor privado realiza (alguns em excesso, outros em carência) e do que o setor público também faz, ora coordenando, ora orientando, ora fiscalizando e punindo.

### 5.Balanceamento do respeito à privacidade e autodeterminação e os incentivos ao desenvolvimento tecnológico. Distinção entre discriminação e discriminação ilícita ou abusiva

Dos valores que têm sido mencionados em conexão à LGPD, o mais citado é o da privacidade, cujo respeito é colocado como fundamento da lei logo em seu artigo 2º, I. No entanto, a norma legal também enuncia outros fundamentos. A autodeterminação informativa é prevista expressamente em seguida, no inciso II do mesmo artigo 2º, e, no que tange especificamente à atividade econômica, o desenvolvimento econômico e tecnológico e a inovação são referidos no inciso V, e a livre-iniciativa, a livre-concorrência e a defesa do consumidor no inciso VI.

A LGPD não os enuncia por mera retórica. Os algoritmos, como mecanismos de processamento massivo de dados criados para o cumprimento de certas finalidades, têm implicação econômica, política e social. Podem ser aplicados para os mais diversos usos e fins, privados ou públicos, afetam os setores comercial e industrial, assim como a criação, a análise e a consecução de políticas públicas por todos os entes de Estado.

Na era da economia 4.0, pós-quarta revolução industrial, já é sabido que os dados pessoais albergam imenso valor econômico e político e, embora a LGPD seja transversal e tenha atentado a este impacto, como evidenciado no rol dos fundamentos de sua disciplina de proteção (artigo 2º), bem como na

enumeração dos princípios que devem nortear todas as atividades de tratamento de dados (artigo 6º), ela não configura legislação definitiva na oferta de instrumentos de proteção a todos os interesses atingidos. Seja porque não trata de todos os aspectos, seja porque, mesmo dos aspectos que trata, não é a única lei a tratar.

Daí a importância em considerar outros mecanismos de tutela destes interesses, outros instrumentos jurídicos com os quais a LGPD deve se coordenar, por exemplo, mas não apenas, aqueles previstos nas normas de proteção ao consumidor (Lei 8.078/1990 (LGL\1990\40)) e à concorrência (Lei 12.529/2011 (LGL\2011\4796)), que afetam a dinâmica de atuação dos agentes privados, com impacto nos mercados e nos modelos de negócios.

A proteção a todos os valores contemplados na LGPD deve existir, mas não sufocar a inovação. Entretanto, a lei não faz escalonamento, não diferencia *startups* de garagem, empreendedores pequenos ou em começo de atividade e grandes empresas, que atuam por via de sociedades já consolidadas. Adicione-se à falta de escalonamento que a interpretação da LGPD passa também pela consciência de que ela pode ser uma norma de intenção bastante protetiva da privacidade, porém, em uma sociedade que na prática não prestigia tanto este valor[28], inibindo talvez investimentos que permitiriam desenvolvimento econômico e fazendo com que eles aconteçam em outros lugares.

Como premissa para qualquer abordagem sobre o tema na orientação jurídica sobretudo aos agentes econômicos, é preciso antes distinguir a discriminação da discriminação ilícita ou abusiva. Na iniciativa privada, todos os mecanismos de formação de oferta de serviços ou produtos partem de alguma discriminação, porque partem de alguma classificação necessária à composição da oferta.

Por exemplo, no setor audiovisual, a indústria produz, entre vários materiais, também filmes pornográficos, de conteúdo exclusivamente adulto. Obviamente, a discriminação que impõe restrição de acesso a crianças e adolescentes tanto na criação destes produtos como na sua divulgação e comercialização, não é contrária ao Direito. Muito pelo contrário, a segmentação do público, conforme discriminação por faixa etária, é que garante a conformidade das práticas dos agentes econômicos que atuam neste segmento de mercado ao nosso ordenamento jurídico.

Não se pode, obviamente, pressupor que qualquer discriminação seja em si violadora de direitos, devendo ser confrontada apenas aquela que não é amparada pelo nosso ordenamento jurídico. Usando a expressão adotada pela LGPD, a discriminação chamada ilícita ou abusiva (art. 6º, IV), a qual pode ter origem em fonte legal (quando a própria norma pode ser objeto de questionamento pela via da ação direta de inconstitucionalidade, por incompatibilidade com o sistema de valores consagrado no quadro constitucional) ou em fonte convencional (quando, no exercício de sua autonomia privada, um agente – público ou privado – toma decisões que violam direitos, devendo ser refreado pelas vias de aplicação da lei, sejam administrativas ou judiciais).

Neste diapasão, agentes públicos e privados tomam suas decisões sobre suas formas de atuar e seus modelos de negócio com base em decisões econômicas (que incluem todas as considerações sobre racionalidade econômica e viabilidade comercial do negócio), em limitações técnicas (há que se ter o cuidado para que limitações técnicas não sejam utilizadas como escudo contra questionamentos de ordem jurídica, mas elas de fato existem em muitas situações), e em limitações jurídicas (que incluem restrições, mas também objetivos – o Direito tem igualmente natureza promocional e incentivadora de condutas em conformidade com um quadro de valores instituído em nossa Constituição). Estes saberes costumam ser segmentados, mas a LGPD evidencia a necessidade, que sempre existiu, de várias pessoas com conhecimentos diferentes se sentarem à mesma mesa para deliberar sobre qualquer conduta que afete direitos de terceiros, inclusive as relativas à criação, produção e circulação de riquezas.

Além da variedade da natureza das considerações que devem ser tomadas pelos agentes econômicos, as questões trazidas pelo advento da LGPD também conduzem à percepção de que a preocupação sobre todos os impactos no processamento de dados pessoais não deve recair apenas sobre o resultado do processamento, ou o *output*, mas, antes, desde a concepção dos produtos e serviços e durante todo o seu desenvolvimento e operação.

No entanto, a LGPD, embora enuncie vários fundamentos, entre eles a autodeterminação informacional, na prática, traz mais instrumentos focados na tutela da privacidade, e poucos elementos concretos que auxiliem quem vai aplicar o direito nos casos concretos, no dia a dia, a se orientar sobre como agir em observância ao fundamento da autodeterminação, ou aos outros fundamentos que enuncia. A LGPD não oferece claramente parâmetros que auxiliam os intérpretes a saberem como agir em consonância com todos os princípios em que se baseia. Daí a importância de conectá-la a outros documentos legais, revelando a complexidade da análise a ser feita pelo intérprete. Feitas todas as ponderações, é possível dar melhor resposta às dúvidas que apareçam relacionadas aos casos concretos.

Assim, mecanismos de discriminação com base em dados podem ser em alguns casos perfeitamente compatíveis com a legalidade constitucional e, em outros, não. Certas práticas, como de *geoblocking*

(bloqueio de oferta de produtos ou serviços a certo grupo de pessoas conforme o dado geográfico) e *geopricing* (diferenciação de preços de produtos ou serviços conforme o dado geográfico) ou quaisquer formas de discriminação de grupos podem fazer sentido em certas circunstâncias.

Em termos de política de saúde, por exemplo, durante o surto de sarampo nos anos de 2019 e 2020 em regiões do território brasileiro, apenas alguns Estados, mais afetados pela doença, expandiram a cobertura de vacina e, mesmo neles, apenas parte da população passou a ser vacinada em complementação ao esquema regular de vacinas – o grupo alvo de trabalho, definido com base em critérios de racionalidade científica, que incluem, entre outras considerações, submissão à imunização anterior e esquemas de vacinação pré-realizados por pessoa. Esta diferenciação faz parte da execução de uma política de saúde justificável, tendo em vista que não há vacina para todos, e sua adoção precisa ser realizada de forma que produza os melhores resultados para a população.

Outro exemplo de uso de dados e discriminação aplicada em conformidade com a legalidade constitucional é o que se refere ao enfrentamento da pandemia do coronavírus em 2020 (covid-2019). De acordo com dados pessoais obtidos pela Polícia Federal (no controle de fronteiras) e pelos serviços de atendimento em saúde nas três esferas da Administração (Municípios, Estados e União) sobre circulação e condições de saúde pessoas, processados em conjunto com dados científicos sobre contaminação temporal e geográfica, foi possível tomar decisões impondo medidas de segurança e redução de impactos para toda a população. As medidas incluíram imposição de exame para casos suspeitos, notificação de resultados, restrição de atividades e mobilidade (isolamento e quarentena), tudo para enfrentamento da pandemia. Tais decisões importaram em substancial restrição de direitos[29], porém, justificáveis dentro do nosso quadro constitucional, em momento de priorização da saúde pública e concretização do princípio da solidariedade constitucional.

Especificamente nas relações privadas, é possível haver também discriminação quando há racionalidade econômica, autorizando tratamentos não igualitários, por exemplo, na composição do valor do prêmio no contrato de seguro de automóvel, normalmente mais barato para mulheres, diante das estatísticas que evidenciam que elas se expõem menos aos riscos.

A questão se complica quando, embora as discriminações decorram de racionalidade econômica, violam direitos fundamentais. Discriminações que violam interesses de grupos vulneráveis podem ser questionadas. Algumas são mais facilmente identificadas como violadoras, mas, em certos casos, a identificação da violação é dificultada, pois depende da consideração de inúmeras variáveis, que devem se ponderar em um ordenamento que é complexo, porém, uno.

A definição de quais discriminações são possíveis e quais não são, bem como de quais parâmetros devem ser adotados pelos agentes de tratamento, já era um desafio antes mesmo do uso da inteligência artificial, mas, com ela, a questão se tornou mais urgente, pois os efeitos de discriminações em desacordo com a legalidade constitucional foram enormemente multiplicados em tempos de economia 4.0 e processamento massivo de dados.

Há situações em que a discriminação contida em uma decisão com suposta racionalidade econômica (resultante de um processamento de dados, via algoritmo ou não, embora cada vez mais as decisões sejam automatizadas) pode se revelar violadora de direitos e em desconformidade com o ordenamento.

A título de ilustração, um dos episódios alardeados na mídia sobre uso de dados em violação a direitos durante 2018 e 2019 foi o caso Decolar. O Departamento de Proteção e Defesa do Consumidor (DPDC), órgão integrante do Ministério da Justiça, multou a sociedade empresária que vendia pacotes de viagens em R$ 7.500.000,00[30], pela prática de discriminação dos consumidores com base em critério geográfico: dependendo da localidade do consumidor, as ofertas eram diferentes[31]. O algoritmo adotado pela Decolar estava provocando uma discriminação que foi entendida como abusiva, o que gerou a responsabilidade administrativa da sociedade empresária. Neste caso, a LGPD, ainda não em vigor, sequer foi necessária para a responsabilização, pois o próprio CODECON foi suficiente (embora a LGPD reforce a proteção ao titular de dados, neste caso, também consumidor).

Esclareça-se que a discriminação pode estar contida no algoritmo ou na escolha comercial que o precede (e que, de alguma forma, será refletida no algoritmo; afinal, ele é sempre programado pelos desenvolvedores conforme pré-orientações dos gestores das sociedades)[32]. A elucidação sobre a intencionalidade da discriminação e sobre a forma de produção da decisão que se revele indevidamente discriminatória é importante para fins de polícia administrativa e na esfera penal. Entretanto, para fins de responsabilização civil, o que importa é o prejuízo injusto sofrido pela vítima da discriminação ilícita ou abusiva.

Sobre o uso de dados sensíveis, eventualmente, a expressa utilização e inserção de um dado sensível na fórmula algorítmica, o que, à primeira vista, pode parecer indevidamente discriminatório, pode ser um mecanismo adequado justamente para se evitar a discriminação ilícita ou abusiva. Neste sentido, pode ser necessário reconhecer, diferentemente da classificação proposta pela LGPD, que distingue

dados gerais e dados sensíveis, que todos os dados podem ser de alguma maneira sensíveis, a depender do tratamento a ser feito deles, como sugerido pelo próprio § 1º do artigo 10 da lei[33].

**6.Fatores regulatórios, técnicos, e a atuação de outros órgãos de fiscalização em soma às atribuições da ANPD**

Outra consideração que pode ser adicionada ao caldo de variáveis aqui levantado é que quanto maior a regulação de certa atividade econômica, ela pode ser mais orientada por comandos legais que imponham ou flexibilizem o uso de dados, ou permitam a discriminação com base neste uso.

No âmbito do direito da concorrência, que também impacta a dinâmica de atuação dos agentes econômicos, sabe-se, por exemplo, que é possível criar, por via da exceção regulamentar, situações que, sob outras circunstâncias, seriam julgadas como violadoras do direito da concorrência, *v.g.*, tabelamento de preços em certas atividades[34], ou prestação de serviços em regimes de concessão por área, com regras de tarifação predefinidas, as quais, se fossem praticadas em regime de livre mercado, poderiam ser tomadas como de cartelização e sujeitas às penalidades da lei. Da mesma maneira, é possível cogitar de situações que, por força de regulação, excepcionem a própria LGPD.

Além desta variável resultante da regulação, há também a questão da limitação técnica. É possível que, em dado momento do estado da ciência, de fato, haja impossibilidade de certo controle no tratamento de dados que acabe ocasionando limitações a direitos dos titulares. Com relação a tal hipótese, é necessário afirmar que as limitações podem ser de tal ordem que simplesmente impeçam o exercício da atividade. Em outras palavras, a tutela ao bem da privacidade, da autodeterminação informacional, do direito à não discriminação ou de quaisquer valores enunciados como fundamentos da LGPD, pode impedir o lançamento de certos produtos ou serviços no mercado, que, embora tenham racionalidade econômica, sejam violadores de direitos.

Também pode haver situações de uso do argumento técnico apenas como desculpa, seja porque colocam, por exemplo, pessoa interposta que não tem treinamento ou capacidade para intervir na decisão resultante de um processo de análise e decisão de um algoritmo (um atendente bancário, por exemplo), seja porque a pessoa que fica na linha de frente até tem condições de intervir, mas pode laconicamente dizer que não tem, para evitar questionamento pelo titular de dados sobre o resultado produzido. Os intérpretes e aplicadores da lei deverão estar atentos a estas possibilidades.

Por fim, certos atos em violação a normas jurídicas podem ser programados justamente pelo uso da tecnologia, por exemplo, paralelismos conscientes de conduta, que simulam cartéis, mas criados com uso de robôs. Que agentes concorrentes ajam, até certo ponto, conforme seus pares atuantes no mesmo mercado é algo natural e esperado, mas o comportamento uniforme produzido por meio de processamento de dados, à semelhança de suposta combinação que seria feita presencialmente pelos agentes, pode ser caracterizada como prática anticoncorrencial[35], a exigir resposta das autoridades competentes.

Neste contexto, cabe a pergunta sobre quais fases afinal estão cobertas pelo direito à explicação e o direito à revisão – desde a concepção pelo agente de tratamento sobre a forma de uso dos dados, sua obtenção, a metodologia de tratamento até o controle sobre o resultado –, mas também a quem compete a fiscalização sobre estes direitos à explicação e revisão das decisões tomadas, tendo em vista que elas afetam não apenas diretamente as pessoas titulares dos dados, como também terceiros, ou toda a coletividade, e direitos tutelados por outras normas jurídicas.

Cabe, portanto, a reflexão sobre as sobreposições de competências. Embora o § 2º do artigo 20 da LGPD só se refira à ANPD, a autoridade nacional a quem cabe precipuamente zelar pela proteção dos dados pessoais, nos termos da legislação (artigo 55-J, I), bem como fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso (artigo 55-J, IV), a LGPD não tem o condão de suprimir a competência de outros órgãos do Estado que tenham poderes de polícia para atuar, seja em tutela preventiva ou corretiva de interesses sobre os quais lhes competem defender.

Na experiência comparada, inclusive, temos visto estas intercessões. Autoridades de defesa da concorrência, em face da economia cada vez mais digitalizada e das mudanças na dinâmica dos mercados decorrentes de processamento massivo de dados, têm atuado, ora ladeadas por autoridades de proteção de dados, ora sozinhas, para endereçamento de questões que dizem respeito a um só tempo à proteção de privacidade e autodeterminação, mas também a interesses econômicos dos cidadãos impactados pelos modelos de negócios, desde seus momentos constitutivos até sua efetiva operação. No Brasil, é provável que o mesmo movimento ocorra e o Conselho Administrativo de Defesa Econômica (CADE) também atue em casos de intercessão com a ANPD, ora sozinho, ora em colaboração.

A atenção a questões não expressamente contempladas na LGPD precisa acontecer juntamente com a atenção à própria LGPD. Em relação aos mercados digitais, já é consenso que, em função dos algoritmos e do processamento massivo de dados, o equilíbrio entre custos e resultados tem sido tremendamente impactado. Em consequência, a metodologia de avaliação da legalidade das condutas tomadas pelos agentes econômicos tem passado por bastante debate e revisão por parte das autoridades de defesa da concorrência.

Ainda que haja incerteza sobre quais são, afinal, os fins do direito antitruste[36], já é consenso que os avanços tecnológicos impõem necessariamente mudança na metodologia de análise dos fatos. Estas questões inclusive transbordam o aspecto econômico, pois têm consequências políticas e são capazes de influenciar eleições, como vimos na experiência norte-americana, revelada pelo escândalo *Cambridge Analytica*.

**Considerações finais**

Este trabalho tratou dos desafios interpretativos relacionados ao artigo 20 da LGPD, cuja leitura não pode ser feita de forma isolada em relação a outros dispositivos da lei ou a todo o ordenamento jurídico brasileiro. Propôs-se perspectiva ampliada das questões, em que se entendeu o direito à revisão também como direito à explicação e, ainda, em que a revisão não se entende como exigível somente com relação às decisões tomadas por processamento unicamente automatizado de dados, mas também em quaisquer decisões tomadas pelos agentes de tratamento, em interpretação que nos pareceu mais consistente com os fundamentos e princípios da LGPD.

As mudanças tecnológicas afetaram inevitavelmente a diversidade das contratações (que é ampla em decorrência do prestígio à autonomia privada) e a dinâmica das negociações. Neste contexto, há vários desafios interpretativos ao direito à revisão previsto na LGPD, alguns a que se buscou responder com base na experiência comparada. O exame do tema exige cuidado porque a literatura tem adotado referências tomadas com relação ao RGPD, todavia, ainda que o regulamento europeu tenha inspirado a LGPD, retrata outra realidade fática e jurídica. A LGPD não é mera reprodução do regulamento europeu e, ainda que fosse, se insere em outro ordenamento jurídico, outro espaço geográfico com diferentes realidades.

O direito à revisão está muito relacionado ao conceito de processamento massivo de dados, em que o volume de dados e informações efetivamente influi na composição e no funcionamento dos algoritmos que suportam as tomadas de decisões. O processamento massivo não muda as relações jurídicas apenas sob aspecto quantitativo, no sentido de que tecnologia usada pode acelerar e potencializar a realização de atividades. O processamento massivo também tem impacto qualitativo, pois as decisões tomadas pelos agentes de tratamento ficam mais opacas, menos transparentes, especialmente a partir da adoção das ferramentas de *machine learning*, em que o usuário deixa de ver como as decisões são tomadas e, sobretudo de *deep learning*, que permitem a conexão de várias unidades de processamento de dados mediante o conceito de redes neurais, em execução de processamento pesado de dados, ampliando o impacto da tecnologia.

O algoritmo, como equação matemática que encerra uma finalidade, deve ser analisado justamente em função de sua finalidade, a qual deve ser buscada, pelo intérprete, para avaliação da conformidade do processamento de dados com a legalidade constitucional. O exame jurídico, portanto, não deve se preocupar com a complexidade matemática, mas, sim, com a complexidade finalística, teleológica, e quais os caminhos que foram tomados para a decisão que resulta do processamento de dados.

A opacidade é um desafio da interpretação, seja porque entender o racional adotado pelo algoritmo será cada vez mais difícil, seja porque a própria lei em alguns casos reduz a transparência, embora a consagre como princípio; por exemplo, quando preserva a fórmula algorítmica sob o manto do segredo empresarial. Todavia, o fato de existir o desafio da opacidade não pode impedir os titulares de dados de terem a proteção a que têm direito com relação a seus interesses pessoais, sejam de natureza patrimonial, seja existencial. Por outro lado, o intérprete deve estar atento para o fato de que, além dos interesses de cada titular, há outros, que ora se contrapõem e devem ser devidamente sopesados por via de ponderação.

Resta, por fim, saber se a nova norma jurídica ganhará a força que dela se espera para a proteção de todos os valores que enuncia, em parte inspirados na realidade europeia, embora o cenário brasileiro seja de um ambiente bem mais tolerante a violações de privacidade. A interpretação e a aplicação da norma podem, na prática, ganhar contornos diferentes daqueles previstos pelo legislador nacional.

**Referências bibliográficas**

ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN WP 251 rev. 01, p. 21, last Revised and Adopted on 6 February 2018. Disponível em: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053]. Acesso em: 25.03.2020.

COUTINHO, Diogo R.; KIRA, Beatriz. Por que (e como) regular algoritmos? In: *Jota*, 2 de maio de 2019. Disponível em: [www.jota.info/tributos-e-empresas/regulacao/por-que-e-como-regular-algoritmos-02052019]. Acesso em: 25.03.2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FORGIONI, Paula A. *Os fundamentos do antitruste*. 7. ed. São Paulo: Ed. RT, 2014.

FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. In: *Revista*, 5 de dezembro de 2018. Disponível em [www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018]. Acesso em: 15.03.2020.

FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. In: *Jota*, 26 de dezembro de 2018. Disponível em: [www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018]. Acesso em: 25.03.2020.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

GUTIERREZ, Andriei. É possível confiar em um sistema de Inteligência Artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de *accountability*. In: MULHOLLAND, Caitlin; FRAZÃO, Ana (Coords.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Ed. RT, 2019.

MALDONADO, Viviane Nóbrega *et al.* (Coords.) *LGPD*: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin Sampaio; FRAJHOF, Isabella Z. Inteligência artificial e a lei geral de proteção de dados: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. MULHOLLAND, Caitlin; FRAZÃO, Ana (Coords.) *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Ed. RT, 2019.

OLIVEIRA, Marco Aurélio Bellizze. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018 (LGL\2018\7222). In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. In: *International Data Privacy Law*, 233, 2017. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125]. Acesso em: 25.03.2020.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MALDONADO, Viviane Nóbrega et al. (Coords.). *Comentários ao GDPR*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

VENTURA, Deisy de Freitas Lima; AITH, Fernando Mussa Abujamra; RACHED, Danielle Hanna. A emergência do novo coronavírus e a "lei de quarentena" no Brasil. *Revista Direito e Práxis*, Rio de Janeiro, 2020. Disponível em: [www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/49180/32876]. Acesso em: 15.03.2020. DOI: 10.1590/2179-8966/2020/49180

VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com a LGPD brasileira. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. In: *Harvard Journal of Law & Technology*, v. 31, p. 843, n. 2, p. 843, Spring 2018. Disponível em: [https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf]. Acesso em: 25.03.2020.

1 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.

2 Nas palavras de Ana Frazão, "sem a devida transparência, é muito provável que a programação possa estar permeada de vieses e preconceitos dos programadores, intencionais ou não, que podem levar a erros de diagnosticou a graves discriminações. Mais do que isso, é possível que as correlações encontradas no processamento sejam consideradas equivocadamente causalidades, fator que pode reforçar discriminações". (*sic*) (Fundamentos da proteção dos dados pessoais: noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 39.)

3 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor.

4 COUTINHO, Diogo R.; KIRA, Beatriz. Por que (e como) regular algoritmos. In: *Jota*, 2 de maio de 2019. Disponível em: [www.jota.info/tributos-e-empresas/regulacao/por-que-e-como-regular-algoritmos-02052019]. Acesso em 14.03.2020.

5 FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. In*: Jota*, 5 de dezembro de 2018. Disponível em: [www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018]. Acesso em: 15.03.2020.

6 Nas palavras de Danilo Doneda, "o indivíduo tem acesso ao bando de dados onde suas informações estão armazenadas, podendo obter cópias destes registros, com a consequente possibilidade de controle destes dados; depois deste acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo poder-se-á proceder a eventuais acréscimos". DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 182.

7 Rony Vainzof salienta a importância deste princípio: "Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta. Pior, uma vez coletado e tratado o dado pessoal impreciso, sem que seja sanada a respectiva imprecisão na fonte, o risco de que esse dado viciado seja tratado de forma permanentemente incorreta é bastante elevado. Assim, os controladores precisam adotar medidas, desde o momento da coleta, que, por padrão, garantam a precisão e, quando necessário, a atualização dos dados." (MALDONADO, Viviane Nóbrega et al. *LGPD*: Lei Geral de Proteção de Dados comentada. In: MALDONADO, Viviane Nóbrega et al. (Coords.). 2. ed. São Paulo: Thomson Reuters Brasil, 20119. p. 149.)

8 Nas lições de Marco Aurélio Bellizze Oliveira et al., a correlação que deve ser respeitada é entre "o tratamento dos dados e a finalidade informada", de modo que esse princípio "guarda estreita ligação com os princípios da adequação e da necessidade". (OLIVEIRA, Marco Aurélio Bellizze. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*, cit., p. 73-74.)

9 A Lei 12.414/2011, a chamada Lei de Cadastro Positivo, com redação alterada pela Lei Complementar 166/2019, por exemplo, prevê em seu artigo 5º que são direitos do cadastrado o acesso a informações sobre ele existentes no banco de dados (inciso II), a impugnação de qualquer informação erroneamente anotada (inciso III), o conhecimento de elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial (inciso IV), assim como da identidade do gestor e objetivo do tratamento dos dados (inciso V), solicitar a revisão da decisão realizada exclusivamente por meios automatizados (inciso VI), entre outros direitos. Há, portanto, na Lei de Cadastro Positivo, expressa referência às várias etapas de uso dos dados pessoais, sobre as quais o titular (no caso da Lei de Cadastro Positivo, identificado como cadastrado) deve ter acesso e ingerência.

10 O regulamento europeu de proteção de dados impede em regra a tomada de decisão automatizada em relação a pessoas em seu artigo 22: "*1. 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. 2. O n* o *1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos*

*interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. [...].”*

11 Pelo *machine learning*, o usuário deixa de ver como as decisões são tomadas, na medida em que a máquina desenvolve, por si, novas informações ou formas de processamento não necessariamente alcançáveis pelo próprio agente de tratamento de dados e pelo usuário. Já pelo *deep learning*, há conexão de várias unidades de processamento de dados por meio do conceito de redes neurais, em execução de processamento pesado de dados, ampliando o impacto da tecnologia de forma quantitativa, mas também qualitativa.

12 Na qualidade de órgão consultivo europeu independente em matéria de proteção de dados e de privacidade, o Grupo produziu parecer intitulado *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, de 3 de outubro de 2017. Disponível em: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053]. Acesso em: 12.03.2020.

13 Toma-se, por exemplo, a experiência com produtos farmacêuticos, lançados somente depois de pesquisa científica que exige conhecimento de informações complexas. As bulas de orientação aos pacientes devem ter informações básicas para que, mesmo um usuário de medicamento que não tenha qualquer formação técnica em área biomédica, consiga entender sobre condições de uso e segurança.

14 Art. 50. [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I – implementar programa de governança em privacidade que, no mínimo: [...] d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.

15 Art. 4º [...] § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

16 Art. 38. 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.

17 Neste sentido, também Ana Frazão: “Com efeito, Bryan Casey, Ashkon Farhangi e Roland Vogl mostram que o que se chama de *data protection by design* precisa levar em consideração diversos fatores complexos, tais como o estado da arte da tecnologia, os custos de implementação, a natureza, o escopo, o contexto e o propósito do tratamento de dados, assim como os riscos da probabilidade de violações aos direitos dos titulares e a gravidade dessas violações. Por mais que isso envolva uma atitude proativa dos controladores e possam existir hipóteses nas quais os altos riscos tornariam os relatórios de impactos obrigatórios – e não meramente recomendáveis –, é inequívoco que a autoridade responsável tem importante papel para aclarar essas dúvidas.” (FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. In: *Jota*, de 26 de dezembro de 2018. Disponível em: [www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018]. Acesso em: 15.03.2020.)

18 WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal of Law & Technology,* v. 31, n. 2, p. 843, Spring 2018. Disponível em: [https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf]. Acesso em: 15.03.2020.

19 Destacam as autoras: “No âmbito de *machine learning*, explicações sobre o estado interno ou a lógica de um algoritmo que resultaram em dada decisão, destinadas a sujeitos que não possuem qualquer expertise técnica, pode ser extremamente desafiador, não apenas para quem está tentando explicar, diante da complexa forma de trabalho destes códigos, mas principalmente para quem está recebendo a informação. Por sua vez, explicações contrafactuais no contexto de IA podem ser aplicadas de forma a descrever como o resultado alcançado pelo algoritmo depende de fatos externos ao seu funcionamento [...], auxiliando o titular dos dados a compreender como que o tratamento de dados se aplicou a ele, e como que a decisão poderia ter sido diferente diante de determinados fatores.” (MULHOLLAND, Caitlin Sampaio; FRAJHOF, Isabella Z. Inteligência artificial e a lei geral de proteção de dados: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. MULHOLLAND, Caitlin; FRAZÃO, Ana (Coords.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Ed. RT, 2019. p. 283-284.)

20 Quanto ao processo de *machine learning*, Andriei Gutierrez explica que também é possível informar os *inputs*, ou seja, os dados pessoais inseridos no sistema e utilizados pelo algoritmo para se chegar a determinado resultado, pois "é possível que se faça um registro dos *logs* de treinamento e calibragem dos sistemas de IA. A auditoria seria focada não no código-fonte, mas nesses *logs* que são os *inputs* paramétricos desse tipo de sistema de IA. Aliás, a construção e revisão desses parâmetros por equipes interdisciplinares e baseadas em amplo espectro de diversidade têm sido um mecanismo alternativo por empresas para evitar *bydefault* que esses sistemas tenham vícios de origem ou incorram em decisões ética ou legalmente condenáveis. Embora ainda não sejam um requisito regulatório, o registro desses *logs* podem ser um importante recurso para empresas preocupadas em demonstrar seu compromisso com responsabilidade e transparência". (GUTIERREZ, Andrei. É possível confiar em um sistema de Inteligência Artificial? Práticas em torno da melhoria da sua confiança, segurança e evidências de accountability. In: MULHOLLAND, Caitlin; FRAZÃO, Ana (Coords.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Ed. RT, 2019. p. 90.)

21 Na doutrina especializada: "Os *controllers* devem considerar sempre os titulares vulneráveis quanto ao entendimento das infinitas possibilidades de tratamento, notadamente quando ocorrer por meios digitais, em uma 'conduta silenciosa', pois o déficit informacional ganha relevância no ambiente digital, diante da velocidade das mutações do tratamento de acordo com o avanço tecnológico, aumentando, portanto, a necessidade de informações claras, completas e ostensivas aos titulares, que aceitam determinadas transações ao confiar voluntariamente nas informações concedidas pelos responsáveis." (VAINZOF, Rony. Dados pessoais, tratamento e princípios. In: MADONADO, Viviane Nóbrega et al. (Coords.). *Comentários ao GDPR*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 49.)

22 Artigos 9º, II, 10, § 2º, 18, V, 19, II, e § 3º, 38, 48, § 1º, III, 55-J, II, X, e § 5º.

23 BARBOSA, Denis Borges. *Uma introdução à propriedade intelectual*. 2. ed. Rio de Janeiro: Lumen Iuris, 2003. p. 649.

24 Pode ser, por exemplo, a proteção a um invento para o qual o criador, ao invés de buscar a obtenção de patente pelo Estado, que lhe assegura exclusividade na exploração, mas com prazo determinado, opta por manter a invenção em segredo, para garantir exclusividade na exploração por prazo indeterminado. Há, nos dois casos, a mesma criação com aplicação industrial, fruto da inventividade humana, mas submetida a dois modelos de proteção intelectual distintos, cada um com suas características e regime jurídico.

25 Art. 195. Comete crime de concorrência desleal quem: [...] XI – divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato; XII – divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; [...].

26 Ressalve-se que o segredo empresarial não é a única forma de proteção do algoritmo disponível para o seu desenvolvedor ou adquirente (portanto, o seu titular). O segredo é mais comumente adotado quando o titular da fórmula algorítmica pretende usá-la com exclusividade. Entretanto, quando o titular tenciona, por exemplo, via licenciamento, obter remuneração com a comercialização do algoritmo, o mais comum é a invocação da proteção autoral, mais especificamente pelas vias previstas na Lei do *Software* – Lei 9.609/1998.

27 Constituição da República – Art. 5º [...] XXXV – a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito; [...].

28 Com inspiração europeia, a LGPD foi bastante ciosa do respeito à privacidade, mas é importante sopesar criticamente se no contexto brasileiro, no qual se insere, afinal, nossa lei de proteção de dados, e diferente do europeu, referido valor tem o mesmo peso, e deve ser ponderado com a mesma força diante de outros valores que também integram nosso quadro constitucional.

29 VENTURA, Deisy de Freitas Lima; AITH, Fernando Mussa Abujamra; RACHED, Danielle Hanna. A emergência do novo coronavírus e a "lei de quarentena" no Brasil. *Revista Direito e Práxis*, Rio de Janeiro, 2020. Disponível em: [www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/49180/32876]. Acesso em: 15.03.2020. DOI: 10.1590/2179-8966/2020/49180

30 Ministério da Justiça. Secretaria Nacional do Consumidor – DPDC. Processo: 08012.002116/2016-21. Despacho 299/2018. Publicado no *Diário Oficial da União* em 18.06.2018, edição 115, Seção 1, p. 73.

31 Com relação a alguns produtos, os brasileiros tinham limitação de oferta, com negativa de vagas, e com relação a outros, os consumidores de certa região recebiam ofertas diferenciadas – os consumidores de SP recebiam preço mais caro.

32 Algoritmos não são neutros. Eles incorporam sempre visões de quem os desenvolve, tenham os desenvolvedores consciência ou não deste fato. (COUTINHO. Diogo R.; KIRA, Beatriz. Por que (e como) regular algoritmos? In: *Jota*, 2 de maio de 2019. Disponível em: [www.jota.info/tributos-e-empresas/regulacao/por-que-e-como-regular-algoritmos-02052019]. Acesso em: 24.10.2019.

33 Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

34 Ainda que sob críticas que possam ser feitas, do ponto de vista econômico, sobre a (baixa) racionalidade desta prática.

35 FORGIONI, Paula A. *Os fundamentos do antitruste*. 7. ed. São Paulo: ed. RT, 2014. p. 349-350.

36 Em discussão conhecida como *hipster* antitruste, na qual a doutrina especializada tem se voltado a questões que apareceram no momento de criação desta área do direito, para definição dos seus objetivos primordiais, entre a consagrada tutela da oferta de produtos e serviços aos consumidores e a expansão para compreensão de outras tutelas, como autonomia decisória dos cidadãos com relação ao que e como consumir, a proteção a interesses dos trabalhadores, e até mesmo a preservação da democracia, tendo em vista que o poder político tem cada vez mais se conectado ao poder econômico.