Revista da Faculdade de DIREITO da Universidade Federal de Uberlândia

Internet das Coisas, Decisões Automatizadas e o Direito à Explicação

Internet of Things, Automated Decisions and the Right to Explanation

Patricia Strauss Riemenschneider[1]
Guilherme Antônio Balczarek Mucelin[2]

Resumo: Decisões que afetam a vida de todos são tomadas com base em dados coletados a todo momento por dispositivos digitais. Dados localizadores, escolhas de lazer e saúde são captados e tratados, de forma a traçar um "perfil" do usuário. O perfil é então cedido, gratuita ou onerosamente para grandes e pequenas corporações. Tais informações são posteriormente acessadas por empregadores, por exemplo, que podem descartar o candidato à uma vaga de emprego ou demiti-lo, por não ter alcançado o "score" desejado, ou por fornecedores, negando ao consumidor determinado bem de consumo por conta de tal perfil. As decisões automatizadas levam a um descarte do indivíduo, tendo por base números, gráficos e algoritmos. O presente estudo se dividiu em duas partes, sendo que a primeira tratou sobre a cessão de dados pessoais e a segunda discorreu sobre o direito à explicação. A pesquisa realizada chegou à conclusão de que um dos principais problemas na utilização de tais decisões é a que o indivíduo preterido não recebe explicação pela qual foi rejeitado. Assim, o objetivo do presente artigo é verificar a viabilidade do direito à explicação de acordo com a Lei Geral de Proteção de Dados e legislações correlatas, a partir de uma metodologia dedutiva, de abordagem bibliográfica e documental.

Palavras-chave: Direito à Explicação. Direitos da Personalidade. Internet das Coisas. Proteção de Dados.

[1] Doutoranda em Direito pela Universidade Federal do Rio Grande do Sul. Presidente do Instituto Brasileiro de Direito e Maternidade - IBDMater. Advogada com Graduação em Direito pela Universidade Federal de Santa Maria (UFSM). Mestre em Direito pela Universidade de Caxias do Sul (UCS). Pós-Graduada em "Environmental Policy" pela OU - Inglaterra. Pós Graduada em Droit Comparé et Européen des Contrats et de la Consommation - Université Savoie Mont Blanc - França. Pesquisadora do grupo de pesquisa CNPq da Universidade Federal do Rio Grande do Sul - UFRGS - "Mercosul , Direito do Consumidor e Globalização" liderado pela professora Cláudia Lima Marques. Atualmente é professora na graduação em Direito da Faculdade IMED (RS) e do Curso CEISC.

[2] Doutorando e mestre em Direito na Universidade Federal do Rio Grande do Sul. Especialista do Programa de Pós-Graduação Lato Sensu em Direito da Universidade Federal do Rio Grande do Sul - UFRGS, "O Novo Direito Internacional": Direito Internacional Público e Privado e Direito da Integração; especialista do Programa de Pós-Graduação Lato Sensu em Direito da Universidade Federal do Rio Grande do Sul - UFRGS, "Direito do Consumidor e Direitos Fundamentais"; Especialista em "Direito do Trabalho e Processual do Trabalho", pela IMED. Especialista em "Droit Comparé et Européen des Contrats et de la Consommation", da Université de Savoie Mont Blanc/França. Professor assistente na Universidade Federal de Goiás - UFG.

DOI: http://dx.doi.org/10.14393/RFADIR-v49n1a2021-56135

Abstract: Decisions that affect everyone's life are made based on data constantly collected by digital devices. Location data, health and leisure choices are captured and processed, to draw a "profile" of the user. The profile is then provided for free or charged, to large and small corporations. Such information is subsequently accessed by employers, for example, who can discard a candidate for a job vacancy or fire them, for not having reached the desired score. Automated decisions lead to an individual's disposal, based on numbers, graphs and algorithms. This study was divided into two parts, the first dealing with the transfer of personal data and the second dealing with the Right to Explanation. The research carried out may conclude that one of the main problems in using such decisions is that the neglected individual does not receive an explanation for why he was rejected. Thus, the objective of this article is to verify the feasibility of the right to explanation in accordance with the General Data Protection Law and related legislation, based on a deductive methodology, with a bibliographic and documentary approach.
Keywords: Data Protection. Internet of Things. Personality Rights. Right to Explanation.

1. Introdução

Em um mundo pós-moderno, digital e líquido, o direito à privacidade é um dos aspectos mais relevantes e instigantes na pesquisa jurídica contemporânea. O “direito de ser deixado só” não mais existe. Pelo contrário, há uma valorização extrema de informações e, os dados pessoais de cada indivíduo são a fonte dos desejos de corporações que conseguem, com base em sua coleta, traçar um perfil do sujeito, de forma até mesmo a antever reações comportamentais, de consumo e de trabalho.

Quando se fala em Internet das Coisas, vemos um sistema ainda mais sofisticado. O usuário terá seu perfil traçado pelos aplicativos que utiliza, por exemplo. Se terá conhecimento sobre os lugares que normalmente frequenta, restaurantes que solicita comida e gostos e desgostos em suas redes sociais. Assim, há a coleta e o tratamento de dados das pessoas, criando um perfil do indivíduo. Os dados são, de maneira rotineira, repassados a terceiros, sendo assim, manipulados e acessados por incontáveis sujeitos, importando em uma quebra da privacidade, eis que o indivíduo não tem ciência do destino que é dado aos seus dados.

As decisões automatizadas, baseadas primordialmente em estatísticas, também podem levar a discriminações no ambiente de trabalho e no mercado de consumo. Dessa forma, pessoas que não alcancem metas ou que não se adequem em horários e frequências estabelecidas pelo empregador, por exemplo, poderão indiscriminadamente não ser selecionadas, tendo por base somente ranking e scores, ao passo que, no que toca ao consumo, produtos e serviços poderão ser sumariamente negados sem que se saiba exatamente o porquê.

Nesse contexto, o objetivo do artigo é analisar o direito à explicação no direito brasileiro, a partir da análise da Lei Geral de Proteção de Dados e de legislações correlatas, utilizando-se, para tanto, da metodologia dedutiva, partindo-se da amplitude do ordenamento jurídico para verificar a viabilidade desse novo direito, a partir de uma abordagem bibliográfica e documental, bem como legislativa. Assim, o trabalho é dividido em duas partes: a primeira, aborda a problemática de dados pessoais, trazendo inquietações sobre o preço da conexão de tudo e de todos. Já na segunda parte, é tratado sobre o direito à explicação derivado de decisões automatizadas, por exemplo, aquelas nas quais o indivíduo pode ter sido preterido, sem não ter tido sequer conhecimento sobre as razões pelas quais foi descartado.

2. O preço da conexão de tudo e de todos: os dados pessoais

A sociedade está passando por um processo de transposição, a qual evidencia um processo de transformação digital (STOLTERMAN, FORS, 2004), informatizando e virtualizando todos os aspectos da vivência humana, como as relações afetivas, o comércio, a cultura, o trabalho, o lazer e todas as manifestações que eram eminentemente offline. Valorizam-se os sentidos, as imagens, os sons, os textos, a instantaneidade (MARQUES, 2004), dando azo à hiperconexão, que significa, segundo Magrani (2019, p. 20-21):

> Estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Esse termo possui alguns desdobramentos importantes. Podemos citar alguns deles: o conceito de always-on, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível (readily accessible); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de dados (always recording). O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (person-to-person, P2P), indivíduos e máquina (human-to-machine, H2M) e entre máquinas (machine-to-machine, M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, neste contexto, um fluxo contínuo de informações e uma massiva produção de dados.

A novidade, para além da conexão de todos, muito propiciada por sites e aplicativos de conversação instantânea, comunidades virtuais e redes sociais de todos os gêneros, é a conexão de tudo – das coisas que circundam as pessoas – com todos. A isso se dá o nome de Internet das Coisas.

A expressão Internet das Coisas (IdC) tem sua origem na língua inglesa, Internet of Things, e apareceu pela primeira vez em 1995 nas produções de Kevin Ashton, cofundador do MIT Auto ID Center (RIFKIN, 2016). Muito se tem escrito sobre o tema, mas seu conceito não encontra unanimidade na Academia (HELBERGER, 2016): dentre as diversas interpretações possíveis, pode-se, de maneira geral, estabelecer que se trata da conexão de objetos físicos à Internet, entre si e com o usuário, por meio de sensores e tecnologias wireless, tornando-os capazes de interagir com ambiente e com as pessoas (DUTTON, 2013), com capacidade de responsividade em tempo real.

Para tanto, cria-se um ecossistema tecnológico próprio (EVANS, 2011), o qual transmite e recebe informações (THIERER, 2014) e que se chama "rede das coisas" (ATZORI, 2010). Para Tidor apud KADOW (2016, p. 154):

> A Internet das Coisas conecta os humanos e as máquinas inteligentes de uma maneira nova, incrível e muitas vezes assustadora. Ela trata do movimento e da interação entre diversas áreas como pessoas, animais, veículos, correntes de ar, vírus e muitas outras coisas. Ela pode reconhecer relações e prever padrões muitas vezes complexos para a mente humana, pode

> descobrir as condições em que uma ponte se encontra, as mudanças na atmosfera. A Internet das Coisas pode ainda operar de maneira independente dos seres humanos e ficar cada vez mais inteligente com o tempo usando algoritmos adaptáveis.

A IdC não se trata exatamente de uma novidade: ela já é altamente utilizada no setor industrial, porque tem a capacidade de estabelecer conexões entre as máquinas para que elas funcionem sem a necessidade de ingerência humana contínua nas operações para as quais são programadas (EUA, 2015).

Em outro ponto, que interessa a este capítulo, diz respeito à utilização da rede inteligente pelas pessoas, pelos mais variados tipos de indivíduos que compõem a sociedade civil, que já percebem a IdC, mesmo em seu período ainda embrionário, como algo revolucionário que oferecerá inúmeros benefícios, especialmente nas tarefas do cotidiano (DAVIES, 2015), contudo, sem que se atentem aos riscos de sua utilização e da destinação das informações coletadas.

Mesmo tendo em vista o aspecto inovador e promissor que a IdC traz à sociedade, tanto com relação a novas experiências no mundo digital, quanto à facilitação da vida em geral, é certo que essa nova tecnologia também revoluciona o modo como aqueles que coletam nossos dados aprendem sobre os titulares dos dados e seus hábitos (HELBERGER, 2016), o que, em um primeiro momento, foi visualizado como uma oportunidade mercadológica para o oferecimento de produtos e serviços hiperpersonalizados (STOLPE, 2016), bem como maior controle no ambiente de trabalho.

Para tanto, a popularização da tecnologia é uma condição insuperável.

Em outros dizeres, conforme Magrani (2019, p. 22), "por isso, o avanço da hiperconexão depende do aumento de dispositivos que enviam e recebem estas informações"; e essa constatação já foi percebida por governos e megaempresas que investem bilhões em infraestrutura para conexão de banda larga, inclusive. Assim, para Evans (2011), em 2020 cinquenta

bilhões de dispositivos estarão conectados à Internet, significando uma média de 6,58 aparelhos conectados por pessoa. Até 2030, segundo as previsões de Rifkin (2016), estima-se que a quantidade será muito maior, chegando ao montante de cem trilhões de dispositivos ligados à IdC, sendo que em países com maior desenvolvimento a quantidade per capta poderá facilmente ultrapassar os cinco mil.

O resultado será uma intensa trama de sensores sem fio que circundará as pessoas e isso permitirá a coleta de dados pessoais e sensíveis de uma maneira jamais pensada, de forma que quem controlar tal fluxo de dados, sejam os fornecedores do mercado de consumo, sejam os empregadores do mercado de trabalho, seja até mesmo o Estado em todas as suas facetas, conhecerá todos os aspectos da vida dos consumidores/trabalhadores/cidadãos (HELBERGER, 2016), justamente por conta dessa capacidade de transformar dados e informações e, ainda, aglutinando-as às já disponíveis na Internet.

As informações coletadas nos aparelhos que não são componentes da estrutura IdC, como celulares e computadores, divergem daquelas que são provenientes da rede inteligente. Em outras palavras, a qualidade das informações se diferencia. Enquanto a pessoa, ao entrar em um aplicativo ou site, fornece dados à plataforma somente quando utiliza o dispositivo, na IdC os dados serão coletados 24 horas por dia, 7 dias por semana (HELBERGER, 2016), sendo capaz de criar um perfil completo de determinada pessoa. Um estudo interessante de Youyou, Kosinski e Stillwell aponta que, somente 150 a 200 likes em redes sociais permitem que o dispositivo tenha quantidade suficiente de informações sobre o usuário para que ele conheça mais a pessoa do que seu coabitante (YOUYOU, KOSINSKI & STILLWELL, 2015).

Por essas razões, os dados coletados por "smart things" têm alto potencial de uso por parte dos fornecedores de produtos e serviços, sejam eles diretos, sejam eles invisíveis na arquitetura do comércio eletrônico,

como seguradoras e garantidoras de crédito (MARQUES, 2017). Assim, mesmo que a coleta de dados não seja restrita à estrutura da IdC, percebe-se que as informações coletadas por ela fornecem inúmeras oportunidades à população com relação a produtos e serviços mais personalizados, de acordo com a preferência e os costumes individuais de cada um, já que o usuário da smart thing interage diretamente com o dispositivo, fazendo com que os fornecedores troquem a publicidade de massa por uma publicidade direcionada com grande precisão com relação a determinadas situações ou especificidades do momento (HELBERGER, 2016). O uso desses dados, contudo, não se restringe à publicidade.

Na Internet das Coisas, a duração temporal do relacionamento com que manuseia os dados é bruscamente alterada, já que estabelece uma longa e dinâmica interação da pessoa com os que tratam tais dados, já que suas informações pessoais ficam circulando na rede smart (COGNIZANT, 2015) com uma perenidade equivalente à vida útil do bem. E mesmo após a vida útil do bem, mesmo que haja previsão legal para que tais dados sejam excluídos, em verdade, eles dificilmente o serão (MEDIUM, 2017).

É importante notar que os produtos e serviços da IdC são smart justamente porque sua funcionalidade alimenta um fluxo contínuo de dados pessoais que traduzem hábitos e usos pessoais, a fim de prover uma performance com feedbacks em tempo real. Significa estabelecer que, para atingir a total funcionalidade da IdC, as pessoas têm como condição insuperável o fornecimento de dados, chegando ao ponto em que o pagamento ou a prestação de serviços públicos não se adstringirá mais somente à contraprestação pecuniária ou ao pagamento de taxas, incluindo também todas as informações coletadas. Essa valorização extrema das informações, consequência da conexão de tudo e de todos em uma única rede, "tira a humanidade da era da privacidade, uma característica dominante da modernidade" (RIFKIN, 2016, p. 96) para uma era de vigilância, classificação e controle (RODOTÁ, 2008) despercebidas. Em

outros temos, em vez de passarmos para uma sociedade tecnológica transparente, como deveria ser idealmente, passaremos a uma sociedade de vigilância velada, uma vez que os "invisíveis" megapoderosos dos dados terão acesso a todas as informações de cada um sem mesmo que se saiba ou se anua nesse sentido. A privacidade, neste momento, ganha uma nova definição, transformando-a no "direito de manter o controle sobre as próprias informações" (RODOTÁ, 2008, p. 92).

A sociedade pós-moderna é marcada pela rapidez e pela simultaneidade em que as coisas ocorrem, revelando a fragilidade das relações interpessoais (BAUMAN 2003). No mesmo compasso, o desenvolvimento tecnológico acompanha essa mesma velocidade, despejando nas pessoas um sem-fim de informações, as quais não são capazes de absorver e processar, o que dá causa, entre outros fatores, ao mal-estar do indivíduo. A tecnologia, como uma maneira de remediar a situação, cria mecanismos e dispositivos cada vez mais interativos e conectados à Internet, a fim de tornar o cotidiano mais facilitado, tanto na seara empresarial quanto na vida privada, reforçando a fragilidade das relações interpessoais e aumentando as relações com as coisas.

Para Luño (1998), o desenvolvimento da tecnologia e da Internet não poderá ser suprimido, já que significa um avanço irrenunciável e um signo de progresso do tempo atual, não se devendo, contudo, tomar uma posição passiva com relação aos riscos inerentes ao ambiente virtual. Neste sentido, o que deve estar claro é que com "o tratamento das informações pessoais por meios informáticos e telemáticos, a intimidade das pessoas encontra-se mais exposta a vulnerações, posto que, como afirmamos linhas atrás, esses meios facilitam enormemente o tratamento dessas informações" (PEREIRA, 2005, p. 144).

Na Internet das Coisas não é diferente. Ela é desenvolvida para facilitar a vida na pós-modernidade, através de coleta e processamento de dados das pessoas que utilizam os dispositivos que compõem a rede

inteligente a fim de criar um perfil apurado do usuário. Pelo uso dessa rede smart, a transmissão de dados e informações se torna cada vez mais comum e facilitada, o que colabora para a ruptura de direitos de privacidade dos consumidores/trabalhadores/cidadãos quando eles não sabem quem manipula seus dados tampouco o destino a eles dado.

Sustenta-se que a utilização dessas informações deveria ser restringida somente para aquilo que foram coletadas, mas os detentores desses dados os utilizam de maneira indiscriminada, principalmente para fins publicitários e para a sua venda ou cessão a terceiros, em geral, outros fornecedores ou prestadores de serviços na sociedade da informação (PEREIRA, 2005), bem como empregadores, os quais verdadeiramente desvendam a vida do consumidor/trabalhador/cidadão sem sua autorização e até mesmo sem o seu conhecimento (SILVA, 2001), o que é uma grave violação ao direito à privacidade.

A privacidade no Brasil é um direito tutelado constitucionalmente, fazendo parte do rol de direitos e garantias fundamentais do cidadão, insculpido no art. 5º, inciso X, da Constituição Federal, de modo expresso, tornando inviolável a vida privada das pessoas, assim como sua intimidade, a honra e a imagem. No mesmo sentido, o inciso XI do referido artigo dispõe a respeito do sigilo de dados, que é protegido pelo manto da inviolabilidade.

Por se tratar de um direito fundamental de sede constitucional, é princípio norteador das demais normas a preservação da privacidade no âmbito pessoal, jurídico, comercial e relacional, explicando Doneda (2011, p. 103):

> (...) no panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da 0 personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

Aplicando também a essa situação, o Código Civil brasileiro, Lei Federal de âmbito geral, elenca a privacidade no capítulo de direitos da personalidade, possibilitando a proibição da divulgação de escritos, transmissão da palavra ou o manejo da imagem de uma pessoa, caso tais atos lhe atinjam a honra, boa fama ou respeitabilidade. Especificamente para o mercado de trabalho, "as regras sobre a proteção de dados e privacidade dos trabalhadores são quase inexistentes" (GLOBAL UNION, 2017, p. 4).

Na seara digital, o Marco Civil da Internet põe a proteção da privacidade como um princípio do uso da Internet no país, sendo sua garantia condição para o pleno exercício do direito de acesso à Internet, no sentido de que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou comunicações deverão obrigatoriamente respeitar os direitos à privacidade, à proteção dos dados pessoais e ao sigilo nas comunicações privadas. Ainda, temos a recente Lei Geral de Proteção de Dados, a qual estabelece que a disciplina da proteção de dados pessoais tem como fundamentos o respeito à privacidade e a autodeterminação informativa, além de estipular inúmeros direitos e deveres para todos os que se envolvem em tratamento de dados, seja ele qual for, excetuando apenas algumas hipóteses legalmente previstas.

Ainda, destaca-se que, quando se trata de matéria de tecnologia, em que a capacidade de aglutinação de dados por tais instrumentos é invisível e abstrata, não havendo transparência a respeito daquilo que é coletado e como é utilizado, ultrapassando a finalidade do uso pretendido pelo consumidor/trabalhador/cidadão, o consentimento para a utilização de tais elementos pessoais, assim como sua proibição específica, torna-se obscuro. Ou seja, não sabendo a pessoa quais informações os controladores estão utilizando, o sujeito se torna ainda mais vulnerável.

Finkelstein (2011) alerta que há entidades denominadas provedores de vias que identificam precisamente onde, quando e quão rápido o

indivíduo acessa cada site, documentando que lojas visitou, por quais links se interessou, em qual ordem e por quanto tempo. Este aspecto da preocupação com a proteção da privacidade decorre de um manejo ativo do consumidor na busca por informações na internet, momento em que seus dados são coletados e associados para a criação de um ambiente publicitário voltado aos supostos interesses do consumidor.

Por outro lado, a Internet das Coisas capta as informações das pessoas de maneira mais sutil, através dos hábitos de localização, alimentação, lazer, saúde e consumo que identifica a partir do uso de seus dispositivos. Nesse sentir, Finkelstein (2011) também refere que a comercialização dos dados coletados pelos sites para outros fins, para empresas comerciais ou de prestação de serviços não coligadas à empresa que os coletou, merece maior atuação do Direito em defesa dos usuários e de sua privacidade (FINKELSTEIN, 2011).

Almeida refere que, mesmo que a Internet não seja um lugar privado, é preciso que se mantenha a privacidade, pois um indivíduo qualquer, ao sair do âmbito privado, não deixa sua privacidade à disposição no ambiente virtual (ALMEIDA, 2016). Muito embora o direito à privacidade baseie-se na noção de ser deixado só (DONEDA, 2006), o uso de dispositivos de IdC impede que o usuário esteja totalmente sozinho, diante da permanente conexão com os servidores que captam seus dados e informações e os repassam constantemente aos proprietários da tecnologia.

O ponto a ser refletido é exatamente o fato de que, em razão do uso das ferramentas que compõe a IdC, a possibilidade de controle pelo trabalhador dos dados que quer ou não que sejam utilizados ou transmitidos, já que a captação de informações é constante e, muitas vezes, irrestrita, é quase nenhuma. Decorrente disso, decisões que afetam nossas vidas estão sendo tomadas com base nesses dados e por meios digitais, o que pode ser um problema para o trabalhador, principalmente com relação à

discriminação na fase pré-contratual, mormente tendo em conta a seleção automatizada de currículos

3. AI Black Box, a pessoa/trabalhador e o Direito à Explicação

Está em trâmite no Senado Federal o Projeto de Lei 4.496, que tem por objetivo alterar o artigo 5º da Lei Geral de Proteção de Dados Pessoais, ao acrescentar o inciso XX à referida disposição legal e fornecer um conceito de decisão automatizada, a qual teria a seguinte redação (SENADO, 2019):

> XX – decisão automatizada: processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, inteligência artificial, aprendizado de máquina, ou outra técnica computacional.

Segundo a justificativa oficial, a LGDP carece de aperfeiçoamento para dar efetividade à tutela pretendida pela legislação de dados, já que, em nenhum momento, decisão automatizada foi definida, deixando lacunas de interpretação que, a depender do juiz, poderia ou não surtir os efeitos protetivos (que estão entranhados durante toda a narrativa da Lei). Nesse sentido, atentou-se ao fato de que existem diversos tipos de decisões automatizadas, sendo umas mais simples, facilmente compreensíveis, com as baseadas em regras ou algoritmos preestabelecidos, ao passo que outras são mais sofisticadas, geralmente menos explícitas e aplicam técnicas de aprendizado de máquina (machine learning) ou de inteligência artificial (SENADO, 2019).

Reafirmando a importância dos dados pessoais, inclusive dos trabalhadores, e de acordo com LOPES (2018, p. 3):

> Ocorre que, como tais algoritmos são treinados a partir de dados já existentes, há o risco de que eles repliquem ou até mesmo exacerbem padrões históricos indesejados de inequidade ou discriminação, ainda que não intencionalmente. Por exemplo, um sistema de análise e filtragem de currículos que se baseie apenas

> nas taxas de sucesso anteriores dos candidatos muito provavelmente reproduzirá vieses exibidos em modelos tradicionais e não automatizados de contratação, compreendendo a ausência de mulheres ou negros no passado como um padrão a ser replicado.

Isso se mostra relevante ao Direito do Trabalho especialmente na fase pré-contratual, no momento da seleção de currículos, mas também na fase contratual, como, por exemplo, na distribuição de prêmios, na verificação de horas trabalhadas e também em desligamentos baseados em decisões puramente automatizadas, de acordo com as metas da empresa, por exemplo, que nem sempre são claras e transparentes. É nesse sentido que se fala em tais decisões como um obstáculo, porque os resultados não são realizados por humanos ou até mesmo em compasso com regras algorítmicas legíveis por humanos, mas somente por técnicas matemáticas que se apresentam com menor capacidade de serem investigadas (EDWARDS; VEALE, 2018).

Trazendo uma ilustração de fora do Direito do Trabalho, podemos perceber o quão será difícil a um consumidor, por exemplo, que solicita um empréstimo a uma instituição financeira e que o mesmo seja negado, perceber que seus dados foram inseridos erroneamente ou comprovar que o sistema foi discriminatório, com base em gênero ou condição sexual, idade ou estado de saúde – o que muito se aproxima do conceito de dados sensíveis, de modo que suas contratações futuras restem sempre prejudica por esse sistema automatizado (EDWARDS; VEALE, 2018). Essa falta de transparência, que se dá em todos os setores da vida onde haja contratações e contatos, o que se pode chamar de opacidade, em virtude do funcionamento de difícil entendimento de algoritmos e dados que alimentam o sistema, dá ensejo ao que autores convencionaram denominar de "caixa preta da inteligência artificial", ou "the AI black box", no inglês (PASQUALE, 2015).

Por isso, voltando à justificativa do Projeto de Lei que tende a conceituar decisões automatizadas, temos que (SENADO, 2019):

> A inclusão dessas técnicas avançadas no conceito de "decisão automatizada" é essencial, em particular, para garantir o chamado "direito à explicação", previsto no § 1º do citado art. 20. Trata-se do direito do cidadão a "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada". Embora, em geral, os responsáveis pelo tratamento de dados não se neguem a prestar informações sobre decisões automatizadas baseadas em algoritmos tradicionais, na maioria dos casos, eles não fornecem esclarecimentos apropriados para decisões baseadas em técnicas de inteligência artificial ou outras igualmente complexas. Portanto, de modo a complementar o texto da LGPD, apresentamos a presente iniciativa, que estabelece a definição da expressão "decisão automatizada", de modo a não deixar dúvidas quanto a extensão desse conceito. Dessa forma, garantiremos que a proteção estabelecida no texto legal se torne plena.

O Regulamento Europeu sobre Proteção de Dados Pessoais foi no mesmo sentido, em seu Artigo 22(3), o qual estabelece que, para a celebração de um contrato, quando for baseado no consentimento explícito para o tratamento de dados, o responsável por tal manuseio deverá aplicar as medidas adequadas para resguardar os direitos, liberdades e interesses do titular, designadamente o direito de, pelo menos, "obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão" (UNIÃO EUROPEIA, 2016), que pode ser traduzido como o direito de receber uma explicação para uma decisão automatizada específica depois de realizada (MENDOZA, 2017). A LGPD brasileira elenca expressamente esse direito (BRASIL, 2018):

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Podemos observar que o direito à explicação deriva de maneira direta do princípio da transparência, previsto na maioria das leis de proteção de dados do mundo (GREENLEAF, 2017), tendo como objetivo garantir aos titulares dos dados "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" em conjunto com os critérios de legitimidade, segurança, justiça e não discriminação (BRASIL, 2018), de forma a transformar a caixa preta opaca em uma caixa, pelo menos, translúcida.

Segundo Frazão (2018), nem o GDPR nem a LGPD definem de forma clara os pressupostos básicos para o reconhecimento desse direito, como o que vem a ser decisão automatizada (o que deverá ser sanado caso o Projeto de Lei supracitado seja aprovado), quais os tipos de decisões automatizadas que afetam a esfera jurídica dos titulares dos dados, capazes de dar azo a tal direito, bem como o grau de transparência e explicação que será exigível nestas situações – em especial, nas relações de consumo, de trabalho e de direito público.

Em alguns casos, é mais fácil visualizar o impacto das decisões automatizadas na vida das pessoas: avaliações, rankings e scores; decisões automatizadas com efeitos jurídicos ou similares; monitoramento; tratamento de dados sensíveis; dados processados em deveras larga escala; "datasets" que foram misturados ou combinados; processamentos que impedem os titulares a exercerem determinados direitos, de utilizarem determinados serviços ou celebrarem contratos, independentemente de suas naturezas (COMISSÃO EUROPEIA, 2018). Em outros tantos casos, contudo, e que podem ter capacidade de intromissão da vida das pessoas igualmente, as controvérsias sobre o direito à explicação são ainda maiores, porquanto tais efeitos não são tão visíveis ou diretamente impactantes, como a publicidade individualizada ou mesmo indicações de programas de streaming e de seus conteúdos, como a Netflix e a Spotfy.

De qualquer sorte, tal direito ainda deve ser melhor desenvolvido, quiçá a partir de casos concretos levados ao Poder Judiciário, justo porque não há como impor aos que tratam os dados pessoais a exigência de uma transparência absoluta, até porque nossa LGPD coloca, como limitador, os segredos industriais e comerciais. O que deve existir, por parte desses agentes, é a oferta de informações que sejam compreensíveis para a pessoa média sobre a lógica envolvida nas decisões automatizadas e esclarecer, explicar os motivos pelos quais tal decisão foi tomada em detrimento de outra, incluindo, "(ii) as fontes de tais informações, (iii) como os perfis são criados, incluindo as estatísticas utilizadas, (iv) a razão de o perfil ser relevante para a decisão automatizada e (v) como as informações foram utilizadas para a decisão que afetou determinado titular" (FRAZÃO, 2018, p. 5).

O que não se pode admitir, em um contexto de tecnologia com progresso exponencial e de utilização de dados pessoais para os mais diversos fins, que não só os relativos à publicidade dirigida ou os relativos à personalização de produtos e serviços, é que os dados pessoais, coletados a todo o momento e independentemente de consentimento, muitas vezes até mesmo independente de conhecimento do titular dos dados, sejam utilizados contra as pessoas, contra os direitos sociais já adquiridos e que devem ser respeitados inclusive em ambiente digital – inclusive, entendimento esse do Conselho de Direitos Humanos da Organização das Nações Unidas, ainda em 2012, quando estabeleceu que os mesmos direitos que as pessoas têm offline devem ser também protegidos online (ONU, 2012). O direito à explicação é, em última análise, a humanização das decisões automatizadas.

4. Conclusão

A coleta de dados pessoais e seu redirecionamento para terceiros é um fato corriqueiro na contemporaneidade. A maioria das pessoas, no entanto, não têm ciência que suas preferências, localizadores e até mesmo gostos e

desgostos expostos em redes sociais servem de alimento para corporações que irão traçar o seu perfil. A Internet das Coisas, em especial, capta informações do indivíduo de maneira tênue, identificando hábitos de consumo, lazer e saúde.

Tais dados poderão ser utilizados de forma a preterir, por exemplo, em uma contratação trabalhista, pessoas que não se enquadrem nos "rankings" e "scores" dados por dispositivos cibernéticos. Assim, uma pessoa com problemas de saúde que teve diversas faltas ao trabalho, em seu último emprego, poderia ser descartada pela nova empresa, em uma decisão automatizada. Da mesma forma, o empregado que não cumpriu metas ou atingiu índices estabelecidos, poderia ser demitido. A vida privada é, assim, moldada, de forma a se encaixar, ou não, em "rankings" e "scores".

A Lei Geral de Proteção de Dados brasileira não define decisões automatizadas, permitindo lacunas de interpretação que poderão gerar menor proteção, com uma consequente repetição de inequidade e discriminação, por exemplo.

Duas são as principais colocações trazidas por essa pesquisa: a primeira é de que a utilização das informações deve ser restringida para a razão para a qual foram coletadas, sem que haja venda ou cessão a terceiros e a segunda é de que, os indivíduos, ainda que sujeitos a decisões automatizadas, tenham direito à explicação sobre as estatísticas, motivos e consequências de uma tomada de decisão que teve por base unicamente uma decisão automatizada. A humanização de tais decisões ocorreria, assim, a partir da efetivação do direito à explicação.

Referências

ALMEIDA, Juliana Evangelista de; ALMEIDA, Daniel Evangelista. A ditadura do algoritmo e a proteção da pessoa humana: uma análise do controle do si eletrônico. Revista de Direito Privado: RDPriv, São Paulo, v. 17, n. 69, p. 29-43, set. 2016.

AMÉRICO, Juliano. Microsoft planeja investir US$ 5 bilhões em Internet das Coisas. 2018. Disponível em: https://olhardigital.com.br/pro/noticia/microsoft-planeja-investir-us-5-bilhoes-em-internet-das-coisas/75001. Acesso em: 26 Maio 2019.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. Computer networks, v. 54, n. 15, p. 2787-2805, 2010.

BAUMAN, Zygmunt. Amor Líquido. Rio de Janeiro: Jorge Zahar Editor, 2003.

BRASIL, Lei de Proteção de Dados Pessoais. Lei Federal 13.709 de 14 de Agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 10 Mai. 2020.

BRASIL. Código Civil Brasileiro. Lei Federal 10.406 de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivIl_03/Leis/2002/L10406.htm. Acesso em 10 Mai. 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>). Acesso em 15 Mai. 2020.

CHING, Ke Wan; SINGH, Manmeet Mahinderjit. Wearable technology devices security and privacy vulnerability analysis. International Journal of Network Security & Its Applications, v. 8, n. 3, p. 19-30, 2016.

COGNIZANT. The rise of the smart product economy. 2015. Disponível em: https://www.cognizant.com/InsightsWhitepapers/the-rise-of-the-smart-product-economy-codex1249.pdf. Acesso em: 26 Maio 2019.

DAVIES, Ron. The Internet of Things Opportunities and challenges. European Parliamentary Research Service. 2015. Disponível em: <http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf>. Acesso em: 12 Maio 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], Joaçaba, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DUTTON, William H. The Internet of Things. 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324902>. Acesso em: 21 Abril 2020.

EDWARDS, Lilian; VEALE; Michael. Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? IEEE Security & Privacy, v. 16, n. 3, 2018, p. 46-54. Disponível em: https://ssrn.com/abstract=3052831. Acesso em: 4 Maio 2020.

ESTADOS UNIDOS DA AMÉRICA. United States Federal Trade Commission. "Internet of things: Privacy and security in a connected world." 2015. Disponível em: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Acesso em 18 Mai. Ag. 2020.

EVANS, Dave. The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, v. 1, n. 2011, p. 1-11, 2011.

EYRAUD, Benoït; VIDAL-NAQUET, Pierre. La vulnerabilité saisie par le droit. Revue Justice Actualités, 2013, p. 3-10.

FINKELSTEIN, Maria Eugênia. Direito do Comércio Eletrônico. Rio de Janeiro: Elsevier, 2011.

FRAZÃO, Ana. A nova Lei Geral de Proteção de Dados Pessoais Principais repercussões para a atividade empresarial: controvérsias em torno do direito à explicação e à oposição diante de decisões totalmente automatizadas. 2018. Disponível em: http://anafrazao.com.br. Acesso em: 14 Mai. 2020.

GLOBAL UNION. The future world of work. 10 principais princípios para a proteção e privacidade dos dados dos trabalhadores. 2017. Disponível em:

http://www.thefutureworldofwork.org/media/35502/10-principais-princ%C3%ADpios-para-a-prote%C3%A7%C3%A3o-e-privacidade-dos-dados-dos-trab.pdf. Acesso em: 5 Mar. 2020.

GREENLEAF, G. "European data privacy standards implemented in laws outside Europe". Privacy Laws & Business International Report, vol. 21-23, nº 18-2. Disponível em: https://ssrn.com/ abstract=3096314. Acesso em: 20 Mar. 2020.

HELBERGER, Natali. Profiling and Targeting Consumers in the Internet of Things–A New Challenge for Consumer Law. 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717>. Acesso em: 15 Abril 2020.

LOPES, Giovana Figueiredo Peluso. O "direito à explicação" de decisões automatizadas no âmbito do GDPR. In Anais de Resumos Expandidos do I Congresso de Ciência, Tecnologia e Inovação: Políticas e Leis. Anais. Belo Horizonte, Faculdade de Direito da UFMG, 2018. Disponível em: <https//www.even3.com.br/anais/observalei/131563-o-direito-a-explicacao-de-decisoes-automatizadas-no-ambito-do-gdpr->. Acesso em: 26 Mai. 2020.

LUÑO, Antônio Enrique Perez. Impactos Sociales y Jurídicos de Internet. 1998. Disponível em: <http://www.argumentos.us.es/numero1/bluno.htm>. Acesso em: 11 set. 2017.

MAGNUS, Tiago. Internet das coisas: entenda o investimento em IoT no Brasil. 2018. Disponível em: https://blog.opinionbox.com/internet-das-coisas-investimento-iot-no-brasil/. Acesso em: 10 Mai. 2020.

MAGRANI, Eduardo. Entre dados e robôs. Ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélogo, 2019.

MARQUES, Claudia Lima. A nova noção de fornecedor no consumo compartilhado: um estudo sobre as correlações do pluralismo contratual e o acesso ao consumo. Revista de Direito do Consumidor, São Paulo, v. 111, p. 247-268, maio/jun. 2017.

MARQUES, Claudia Lima. Confiança no Comércio Eletrônico e a Proteção do Consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: Revista dos Tribunais, 2004.

MARQUES, Claudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais. 8. ed. São Paulo: Revista dos Tribunais, 2016. p. 175.

MARQUES, Claudia Lima; MIRAGEM, Bruno. O novo Direito Privado e a proteção dos vulneráveis. São Paulo: Revista dos Tribunais, 2012.

MEDIUM. What happens with your personal data once it's online. 2017. Disponível em: https://medium.com/@cyberalterego/what-happens-with-your-personal-data-once-its-online-e17121724ac3. Acesso em: 20 Mai. 2020.

MENDOZA, Isak; BYGRAVE, Lee A. The right not to be subject to automated decisions based on profiling. In: SYNODINOU, Tatiani et al (eds.). EU Internet Law. Springer, Cham, 2017. p. 77-98.

PASQUALE, Frank. The Black Box Society: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PEREIRA, Marcelo Cardoso. Direito à Intimidade. Curitiba: Juruá, 2005.

Referências legislativas e documentos oficiais

RIFKIN, Jeremy. Sociedade com custo marginal zero: a Internet das Coisas, os bens comuns colaborativos e o eclipse do capitalismo. São Paulo: M. Books do Brasil, 2016.

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

SILVA, José Afonso da. Curso de Direito Constitucional Positivo. São Paulo: Malheiros, 2001.

STOLPE, Marco. The internet of things: Opportunities and challenges for distributed data analysis. ACM SIGKDD Explorations Newsletter, v. 18, n. 1, p. 15-34, 2016.

STOLTERMAN, Erik; FORS, Anna Croon. Information technology and the good life. Information Systems Research, Boston, p. 687–692, 2004.

TIDOR, Bruce. The internet of things. Oxford: The MIT Press, 2015. apud KADOW, André; CAMARGO, Carlos. internet das coisas: vulnerabilidade, privacidade e pontos de segurança. Revista Competência, v. 9, n. 1, p. 153-161, 2016.

UNIÃO EUROPEIA, 2016, Regulamento Geral sobre a Proteção de Dados. Regulamento (UE) 2016 - 679. Disponível em: https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX:32016R0679. Acesso em 05 Mai. 2020.

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans. Proceedings of the National Academy of Sciences, v. 112, n. 4, p. 1036-1040, 2015.

Artigo recebido em: 16/07/2020.
Aceito para publicação em: 18/08/2020.