

MESTRADO EM DIREITO

CIÊNCIAS JURÍDICO-CIVILÍSTICAS

DEFINIÇÃO DE PERFIS:

Utilização para Escolha da Contraparte Contratual

Isabella Juliane Cruz Martins

M

2020



Isabella Juliane Cruz Martins:

DEFINIÇÃO DE PERFIS: Utilização para Escolha da Contraparte Contratual



M. FDUP 2020

DEFINIÇÃO DE PERFIS:

Utilização para escolha da contraparte contratual

Isabella Juliane Cruz Martins



DEFINIÇÃO DE PERFIS:

Utilização para escolha da contraparte contratual

ISABELLA JULIANE CRUZ MARTINS

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para cumprimento dos requisitos necessários à obtenção do Grau Acadêmico de Mestre em Direito, Área de Especialização em Ciências Jurídico-Civilísticas, elaborada sob a orientação científica da Professora Doutora Maria Regina Gomes Redinha

NOTA INTRODUTÓRIA

A presente dissertação foi entregue no dia 15 de outubro de 2020, sendo as legislações utilizadas atualizadas até tal data.

Utilizaram-se as legislações sobre o uso e tratamento de dados de Portugal e do Brasil devido a serem normas que foram promulgadas quase simultaneamente, sendo influenciadas pelo Regulamento Geral de Proteção de Dados Europeu.

Quanto à gramática, utilizou-se a língua portuguesa na versão brasileira, tendo em vista a nacionalidade da autora. Ainda, utilizou-se o inglês americano no resumo, posto ser o, tradicionalmente, aprendido no Brasil.

Informa-se, ainda, que por conta da pandemia do COVID-19, a autora não teve acesso às fontes bibliográficas impressas em Portugal, razão pela qual não foram citadas obras atualizadas sem disponibilidade em sítios *on-line*.

Por fim, foram utilizadas notícias extraídas de jornais *on-line* ao abordar a utilização de dados pessoais em meio à pandemia do COVID-19, em razão da atualidade da matéria.

RESUMO

O aumento de dados pessoais disponíveis, juntamente com o desenvolvimento de novas tecnologias, fez com que os dados pessoais passassem a ser vistos como recursos econômicos, sendo o tratamento dos dados pessoais fundamental para o desenvolvimento da economia movida a dados.

Nesse sentido, foram criadas ferramentas *on-line* que realizam o tratamento dos dados disponíveis em inúmeros sítios *on-line*, sendo possível o tratamento automatizado dos dados, incluindo a definição de perfis, sem a necessidade de intervenção humana. Os perfis obtidos a partir de tal tratamento podem ser utilizados em diversas áreas da sociedade, sendo a escolha da contraparte contratual uma das áreas em que se observa uma maior utilização de tais tratamentos.

Entretanto, por serem utilizados dados histórico-sociais para analisar os dados inseridos nos algoritmos e a decisão ser tomada por meios probabilísticos, a definição de perfis automatizada tende a propagar preconceitos e discriminações históricas, ou ainda resultar em um perfil falso.

Diante da nova realidade, visando tanto a proteção da privacidade dos titulares de dados, como a não propagação de discriminação, desigualdades e preconceitos, surge a necessidade de regulamentar o tratamento automatizado de dados pessoais, incluindo a definição de perfis.

O presente trabalho tem como escopo questionar a regulamentação atual sobre a coleta, uso e tratamento de dados pessoais no direito europeu e português, dando uma indicação também da proteção conferida pela legislação brasileira.

Para tanto, partindo do Regulamento Geral de Proteção de Dados, e passando às legislações nacionais portuguesa e brasileira, serão analisadas as disposições referentes ao tratamento automatizado de dados, incluindo a definição de perfis, verificando em quais situações e com que condições as normas em análise permitem que sejam tomadas decisões automatizadas.

Ainda, será abordada a utilização da definição de perfis para a escolha da contraparte contratual, dando um enfoque aos contratos de trabalho. Nesse ponto, serão verificadas as consequências da utilização de um mecanismo automatizado para contratação, colocando em evidência a problemática da hipossuficiência e vulnerabilidade do titular de dados diante do responsável pelo tratamento, enfatizando a validade do consentimento para o tratamento.

Por fim, serão apresentadas possíveis soluções para os problemas apresentados, visando uma coexistência entre as vantagens advindas do tratamento automatizado de dados e a minimização dos problemas advindos da utilização de decisões automatizadas.

Palavras-chave: Definição de Perfis, Tratamento Automatizado, Regulamento Geral de Proteção de Dados, RGPD, Contrato de Trabalho, Algoritmos

ABSTRACT

The increase in available personal data, together with the development of new technologies, made personal data come to be seen as economic resources, so that the processing of personal data has become fundamental for the development of the data-driven economy.

For this reason, on-line tools have been created to carry out the processing of data available on numerous on-line sites, making it possible to automate the processing of data, including the definition of profiles, without the need for human intervention. The profiles obtained from such treatment can be used in different areas of society, being the choice of the contractual counterpart one of the areas in which a greater use of such treatments is observed.

However, because historical-social data are used to analyze the data inserted in the algorithms and the decision is made by probabilistic means, the automated profiling tends to propagate historical prejudices and discrimination, or even result in a false profile.

In view of the new reality, aiming at both the protection of the privacy of data subjects, as well as the non-propagation of discrimination, inequalities and prejudices, the need arises to regulate the automated treatment of personal data, including the definition of profiles.

The present work aims, therefore, to question the current regulations on the collection, use and treatment of personal data in European and Portuguese law, also giving an indication of the protection conferred by Brazilian legislation.

To do so, starting from the General Data Protection Regulation, and moving to Portuguese and Brazilian national legislation, the provisions regarding automated data processing will be analyzed, including the definition of profiles, verifying in which situations and under what conditions the standards under analysis allow automated decisions to be made.

In addition, the use of profiling to choose the contractual counterpart will be analyzed, focusing on employment contracts. At this point, the consequences of using an automated mechanism for contracting will be verified, highlighting the problem of the data subject's hypo sufficiency and vulnerability compared to the controller, emphasizing the validity of the consent for the treatment.

Finally, possible solutions to the problems presented will be presented, aiming at a coexistence between the advantages arising from the automated treatment of data and the minimization of the problems arising from the use of automated decisions.

Keywords: Profiling, Automated Treatment, General Data Protection Regulation, GDPR, Employment Contract, Algorithm

SUMÁRIO

RESUMO	1
ABSTRACT	1
LISTA DE ABREVIATURAS	7
INTRODUÇÃO	8
CAPÍTULO 1 – A PRESTAÇÃO FUNDADA EM ALGORITMOS. DECISÕES AUTOMATIZADAS. DEFINIÇÃO DE PERFIS.	11
1.1 Evolução da Utilização de Algoritmos para Tomada de Decisões	11
1.2 A Definição de Perfis	18
1.3 Decisões Automatizadas com base em Definição de Perfis	22
1.4 Decisões Individuais Automatizadas e Definição de Perfis no Regulamento Geral de Proteção de Dados	23
1.5 Outros Direitos Concedidos aos Titulares de Dados Pelo Regulamento Geral de Proteção de Dados	29
1.6 Decisões Individuais Automatizadas na Legislação Portuguesa. Leis 58/2019 e 59/2019, de 8 de agosto.	32
1.6.1 A Problemática do Consentimento na Lei 58/2019, de 8 de agosto.	33
1.7 Decisões Individuais Automatizadas na Legislação Brasileira. Lei 13.709, de 14 de agosto de 2018.	35
CAPÍTULO 2 – CONTRATAÇÃO AUTOMATIZADA. UTILIZAÇÃO DA DEFINIÇÃO DE PERFIS PARA ESCOLHA DA CONTRAPARTE CONTRATUAL.	38
2.1. A Utilização Da Definição De Perfis Para Escolha Da Contraparte Contratual ..	40
2.2 Responsabilidade Civil pela Contratação Automatizada no RGPD	41
CAPÍTULO 3 – A UTILIZAÇÃO DA DEFINIÇÃO AUTOMATIZADA DE PERFIS NOS CONTRATOS DE TRABALHO	43
3.1 A Utilização de Decisões Automatizadas em Contratos de Trabalho pela Legislação Portuguesa	47

CAPÍTULO 4 – POSSÍVEIS SOLUÇÕES PARA OS PROBLEMAS APRESENTADOS	
.....	51
CONCLUSÃO	53
BIBLIOGRAFIA	56

LISTA DE ABREVIATURAS

Art./arts.	Artigo/artigos
CRP	Constituição da República Portuguesa
CTP	Código do Trabalho Português
Ed.	Edição
LGPD	Lei Geral de Proteção de Dados
ML	“Machine Learning”
Nº	Número
P./p.	Página
RGPD	Regulamento Geral de Proteção de Dados
EU	União Europeia

INTRODUÇÃO

A evolução da tecnologia, juntamente com o desenvolvimento de sítios *on-line*, aplicativos e redes sociais que utilizam e armazenam os dados pessoais dos utilizadores, fez com que os dados pessoais passassem a ser considerados os principais recursos econômicos existentes na sociedade do século XXI.

Observou-se, então, um aumento no valor econômico dos dados pessoais, sendo os titulares de dados os principais produtos dessa economia movida a dados. Nesse contexto, tem-se falado em um capitalismo de vigilância, centrado na captura, armazenamento, tratamento e uso de dados pessoais (FRAZÃO, 2019, p. 24-31), sendo os dados tratados o produto de maior valor.

Chama atenção o fato de que os dados pessoais são captados de variadas formas e em diversos momentos, sendo certo que os titulares dos dados na maioria das vezes sequer sabem que seus dados estão sendo captados e tratados, sendo essa vigilância constante um dos fatores mais preocupantes da monetização dos dados pessoais.

Nesse cenário econômico, e com o aumento diário na quantidade de dados disponíveis, surgiu a necessidade de realização do tratamento de dados de forma cada vez mais rápida, barata e eficiente.

Houve, então, uma evolução nos algoritmos utilizados, passando a existirem algoritmos que “aprendem” com os dados disponíveis, e, com base neles, podem realizar inferências e correlações automatizadas, sem qualquer intervenção humana. O resultado do processamento automatizado de dados, quando utilizado de forma a surtir efeitos na esfera jurídica de um titular de dados, é chamado de decisão automatizada.

A utilização do tratamento automatizado de dados para tomada de decisões pode ser observada em diversas áreas da sociedade, sendo uma das formas mais comuns de utilização a definição de perfis dos titulares de dados. Assim, com base nos dados disponíveis em diversos bancos de dados *on-line*, um algoritmo pode “definir o perfil” de um indivíduo, definindo as tendências, personalidade e intenções do titular de dados.

Os perfis obtidos a partir do tratamento automatizado de dados passaram a ser vistos como de grande valor para grandes empresários, sendo utilizados tanto para perspectiva econômica externa, criando alvos de consumo, quanto na perspectiva interna, para contratação de funcionários ou concessão ou não de um empréstimo.

Certamente que do ponto de vista empresarial, as novas tecnologias de tratamento de dados contribuíram muito para o desenvolvimento econômico, tornando diversos processos mais rápidos, baratos e eficientes.

Entretanto, ao analisar a perspectiva do titular de dados, percebe-se que a utilização de decisões automatizadas tende a perpetuar riscos e problemas sociais, além de ter uma alta probabilidade de existirem resultados não condizentes com a realidade.

Um dos maiores problemas da utilização do tratamento automatizado de dados reside no fato de que as inferências e correlações realizadas pelos algoritmos utilizam dados histórico-sociais, tendendo a perpetuar práticas discriminatórias ou preconceituosas que ocorreram na sociedade.

Além disso, os resultados dos processamentos são probabilidades algorítmicas, as quais generalizam características para obtenção de perfis, sendo comum o enquadramento de titulares de dados em perfis que não condizem com suas características pessoais.

Levando em consideração o desenvolvimento tecnológico, a monetização dos dados pessoais e a vulnerabilidade do titular de dados, começou-se a perceber uma necessidade de regulamentação do uso e tratamento de dados.

Assim, observou-se uma movimentação global visando proteger os titulares de dados, sendo o Regulamento Geral de Proteção de Dados europeu, que passou a vigor em 2015, uma das primeiras normas atuais sobre o tema.

Fala-se em normas atuais, posto que já haviam disposições normativas sobre a proteção de dados, como por exemplo a Diretiva 95/46/CE que foi revogada pelo RGPD, mas a evolução tecnológica e o aumento nos dados disponíveis fez com que as disposições anteriores ficassem desatualizadas, deixando os titulares de dados desprotegidos em diversos aspectos.

Diante do cenário apresentado, percebe-se a importância do estudo das novas normas de proteção dos dados pessoais, principalmente no que diz respeito à proteção contra a definição automatizada de perfis e a utilização de tais perfis para escolha da contraparte contratual. É evidente a importância da análise da proteção conferida pelo RGPD, sendo também válida a análise de legislações nacionais para constatar a influência do Regulamento Geral de Proteção de Dados não apenas nos países da União Europeia, mas também em países terceiros.

Vale, ainda, destacar a utilização da definição de perfis para escolha da contraparte contratual em contratos de trabalho, mormente no que diz respeito ao tratamento automatizado de dados e definição de perfis para contratação dos funcionários.

A maior atenção aos contratos de trabalho é devido a grande desigualdade existente entre a parte contratante e a contratada, estando o candidato à vaga de emprego ou o empregado completamente sujeitos ao ordenado pelo empregador.

Inexistindo paridade entre as partes contratuais, surge a necessidade de o legislador suprir essa deficiência, dando origem a normas com caráter protecionista. Nesse sentido, é válida a contraposição entre as normas gerais e as normas específicas de determinadas matérias, sendo importante observar como cada situação merece um tratamento distinto ao se considerar as partes analisadas.

Evidente que o tratamento automatizado de dados, incluindo a definição de perfis, traz inúmeras vantagens para quem detém o controle dos dados, o qual obtém um resultado final de forma mais rápida e com menos custo.

O que deve ser levado em conta ao estudar a automatização do tratamento de dados é que, na grande maioria das vezes, o titular de dados encontra-se em situação de desigualdade com o responsável pelo tratamento, muitas vezes sequer sabendo sobre a realização do tratamento ou disponibilização dos dados.

Tem-se então a importância da busca de meios para minimização dos problemas advindos do tratamento automatizado de dados.

Pelo exposto, resta evidente a importância do estudo das normas que regulamentam o uso e tratamento dos dados pessoais, para que, compilando os diversos estudos e as diversas legislações, possa se chegar a uma possível conclusão do que seria o ideal para a coexistência da utilização do tratamento automatizado com a proteção do titular de dados.

CAPÍTULO 1 – A PRESTAÇÃO FUNDADA EM ALGORITMOS. DECISÕES AUTOMATIZADAS. DEFINIÇÃO DE PERFIS.

1.1 Evolução da Utilização de Algoritmos para Tomada de Decisões

O desenvolvimento tecnológico das últimas décadas, juntamente com o avanço do capitalismo, transformou a economia mundial, antes baseada na produção material fundamentada em trocas financeiras, em uma economia movida à dados, também chamada de economia da informação, transformando a coleta, o armazenamento e o tratamento dos dados pessoais em pilares da economia (VALVERDE TERRA, 2019, p. 615).

É certo que os dados pessoais sempre estiveram expostos em diversos tipos de situações, como em formulários de lojas ou currículos para vagas de emprego. Ocorre que com o advento de tecnologias avançadas de inteligência artificial, a coleta dos dados pessoais passou a ser realizada por meio de rastreadores e identificadores *on-line*, inseridos em sites, redes sociais, telefones celulares, entre outros, sendo realizada, muitas vezes, sem o conhecimento e/ou consentimento do usuário. Assim, foi possibilitada a coleta de uma enorme quantidade de novos dados para inúmeras finalidades, dentre elas a definição de perfis dos cidadãos ou trabalhadores, visando os classificarem utilizando os parâmetros introduzidos no algoritmo.

Com o aumento na quantidade de dados disponíveis, adveio a necessidade de aumentar a capacidade de armazenamento dos bancos de dados, surgindo então o que ficou conhecido como *Big Data*. Este consiste tanto em um grande armazenamento de dados e informações, como se refere às ferramentas e sistemas computacionais que analisam os dados armazenados, buscando correlações e padrões entre eles, para serem tomadas decisões com base nas inferências obtidas.

O tratamento dos dados pessoais, por sua vez, passou a ser realizado com a utilização de algoritmos sofisticados, que melhoram automaticamente com a experiência e com os dados históricos disponíveis (EDWARDS, 2017, p. 25), tendo habilidade de “aprender” e tomar decisão sem programação expressa, de forma rápida, barata e eficiente. O processo de aprendizagem algorítmica, chamado de “*machine learning*” (ML), consiste na capacidade de o algoritmo, ao tomar decisões, levar em consideração não somente dados que lhe foram inseridos diretamente, mas também dados externos, como os obtidos *on-line*, obtendo uma previsão com base em padrões de dados (KAMARINOU, 2016, p.6).

Assim, havendo uma maior quantidade de dados disponíveis, e algoritmos que conseguem processá-los em alta velocidade, tornou-se possível a formação de perfis comportamentais de pessoas, grupos ou famílias, sendo tais perfis uma nova “mercadoria”. Salienta-se que os dados disponíveis permitem, além da realização do perfil comportamental, a identificação de hábitos, inclinações, interesses e preferências (VALVERDE TERRA, 2019, p. 613).

Dessa forma, além de avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, é possível analisar como tal pessoa se enquadra em diversas áreas da sociedade (FRAZÃO, 2019, p. 32).

Os perfis obtidos com o tratamento dos dados disponíveis *on-line*, são, então, processados por algoritmos nos quais estão os dados inseridos pelo responsável pelo tratamento, sendo o resultado do processamento intitulado de decisão algorítmica. Essa decisão algorítmica, que pode ser objetiva ou subjetiva, geralmente gera uma consequência na esfera jurídica do titular de dados.

Como exemplos de decisões algorítmicas podem ser citados: (a) na área bancária a utilização para detectar fraudes, para analisar o grau de confiabilidade do indivíduo para concessão de empréstimos ou para definir quem terá crédito e a que taxa de juros; (b) na área comercial para prever preferências dos clientes e conceder recomendações de compra; (c) na área da medicina podem ser citadas previsões médicas com base no histórico familiar, podendo tais previsões serem levadas em consideração por planos de saúde ao estipular o valor do seguro; e (d) na área laboral, para detectar a capacidade e a habilidade para determinados empregos e funções, determinando quem será contratado para trabalhar em determinada empresa.

Resta evidente que, tanto a definição do perfil do titular dos dados, como as decisões tomadas a partir do perfil definido, são realizadas por meio de inferências realizadas a partir dos dados disponíveis, não se tratando de uma ciência precisa.

Nota-se que além dos dados diretamente disponibilizados pelo titular de dados, e relacionados com o objetivo final, os algoritmos utilizam dados histórico-sociais disponíveis *on-line* para tomar decisões, tentando enquadrar o perfil do titular de dados em um perfil social.

Certamente que o tratamento automatizado de dados pessoais traz inúmeras vantagens do ponto de vista empresarial, tendo em vista a simplificação da coleta de dados e diminuição do preço e da velocidade do processamento dos dados.

Contudo, ao analisar a perspectiva do titular de dados, podem ser percebidas inúmeras desvantagens. Em um primeiro momento, é perceptível que a vigilância constante dos indivíduos, com a captação de dados em todos os momentos, mitiga a autonomia e a privacidade da pessoa, que vê um de seus direitos de personalidade violados sem ter qualquer possibilidade de defesa.

Não há dúvidas de que a mineração algorítmica de dados acaba por revelar dados pessoais que os titulares não gostariam que fossem revelados, expondo indevidamente aspectos da intimidade e da personalidade do indivíduo. Ainda, deve ser evidenciado o fato de que os dados pessoais podem ser descobertos diretamente ou através de inferências realizadas a partir de outros dados disponíveis, sendo que, quanto mais dados são disponibilizados *on-line*, mais inferências podem ser realizadas.

A exposição de dados pessoais, por sua vez, ao revelar esferas da personalidade individual, viola a privacidade e a dignidade do titular de dados, podendo interferir na vida pessoal dos indivíduos e causar efeitos negativos em sua esfera jurídica. Como exemplo, pode ser citada a exposição de dados pessoais em ambientes de trabalho, causando a não contratação de um candidato à vaga de emprego, ou a demissão de um funcionário

No entanto, a utilização de dados pessoais obtidos contra a vontade do titular para tomada decisões é ilegal, afrontando o princípio da dignidade da pessoa humana e o direito à privacidade, além de ir contra o direito à autodeterminação informativa, consagrado no artigo 35º da Constituição da República Portuguesa¹. Tal direito pode ser entendido como o poder que o indivíduo tem de determinar como seus dados pessoais serão utilizados.

Entretanto, em um mundo no qual qualquer utilização da internet tende a captar dados pessoais sem os titulares sequer terem consciência, a aplicação do direito à autodeterminação

¹ Artigo 35.º, CRP - Utilização da informática: 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

informativa é de difícil execução, obstando que o indivíduo tenha meios de exercer seus direitos.

Outro grande problema da utilização de algoritmos para definição de perfis e tomada de decisões reside no fato de que os perfis definidos não necessariamente representam a realidade, mas sim uma versão da realidade resultante do processamento dos dados disponíveis, de forma que o resultado final tem o potencial de ser discriminatório, preconceituoso ou injusto.

O potencial discriminatório existe em razão de os algoritmos utilizarem como base no processo de “aprendizagem” e de tomada de decisões, dados históricos-sociais, tendendo a perpetuar os dados existentes. Assim, quanto mais reiterado for um dado, uma conduta ou uma característica em uma sociedade, maiores as chances de o algoritmo entender que aqueles dados são os idealizados naquele meio, enquadrando os indivíduos que os têm como desejados e os que divergem como indesejados.

Conclui-se que o resultado obtido do processamento de dados tende a perpetuar os preconceitos, injustiças e discriminações existentes no âmbito dos dados fornecidos, sendo que, quanto mais forte for determinado padrão em dada sociedade, maior é a chance de o algoritmo o replicar (FRAZÃO, 2019, p. 40).

Nesse passo, ao se tratarem de dados atuais ou de eventos que não tenham ocorrido muitas vezes no passado, as previsões, correlações e inferências algorítmicas tendem a ser imprecisas, posto que a falta de dados similares leva os algoritmos a entenderem que aquele comportamento não é desejado pelo grupo analisado (FRAZÃO, 2019, p. 34). Percebe-se, então, uma tendência em a decisão algorítmica deixar as minorias sociais em desvantagem, tendo em vista refletirem preconceitos e padrões sociais. Tal fato é provado por diversos estudos que mostraram que, em empresas que utilizam tecnologias algorítmicas para a contratação de empregados, características pertencentes a estereótipos históricos (sexo, raça, religião, orientação sexual) diminuem a possibilidade de um candidato ser chamado para uma entrevista de trabalho (TODOLÍ-SIGNES, 2018, p. 7), certamente pela inexistência de dados disponíveis sobre os grupos minoritários no mercado de trabalho.

Outro ponto a ser observado é que os algoritmos são criados por seres humanos, podendo perpetuar as falhas e vieses dos criadores, bem como serem desvirtuados a fim de privilegiar os interesses daqueles pelos quais foram criados ou para quem foram programados (FRAZÃO, 2019, p. 34).

Nesse diapasão, as decisões algorítmicas podem resultar em tratamento preferencial para uns e marginalização para outros (CHENEY-LIPPOLD, 2017, p. 189).

Ainda, devido ao resultado do processamento de dados ser probabilístico, podem existir decisões tomadas com fulcro em correlações e inferências realizadas em um dado, mas que não correspondem com a realidade. Assim, é comum a ocorrência de falsos positivos, quando um perfil com determinadas características é enquadrado em um grupo de indivíduos com as mesmas características, mas o dono do perfil, na realidade, não pertenceria a tal grupo, ou falsos negativos, quando uma pessoa é deixada de fora de um grupo do qual faria parte.

Resta evidenciado o problema inerente à utilização de dados obtidos a partir da realização de inferências e correlações em outros dados, tendo em vista a alta probabilidade de o dado não condizer com a realidade e o potencial lesivo de uma decisão que surte efeitos na esfera jurídica do indivíduo (KAMARINOU, 2016, p. 11).

É necessário, ainda, um maior cuidado ao se tratarem dados de categorias especiais (dados sensíveis), tais quais religião, raça e sexualidade, tendo em vista a potencial utilização discriminatória ou lesiva dos mesmos (VALVERDE TERRA, 2019, p. 608).

Deve-se chamar atenção ao fato de que, mesmo que os dados inicialmente processados não sejam de categorias especiais, os algoritmos podem inferir características personalíssimas a partir dos dados fornecidos, tornando um dado “normal” em um dado sensível.

Assim, a partir de um dado originalmente “inofensivo”, pode ser obtido um dado com características possíveis de serem discriminadas, podendo tal dado sequer ser condizente com a realidade. Os dados obtidos através do processamento de outros dados são intitulados “*bastard data*”.

Como exemplo, pode ser citada a possibilidade de determinação da origem racial e/ou condição econômica de uma pessoa, com base na região em que ela reside, ou ainda a realização de um perfil de consumo através do processamento de dados demográficos coletados através de cookies (KAMARINOU, 2016, p. 10).

Desde já insta ressaltar que o Regulamento Geral de Proteção de Dados confere uma especial proteção aos dados sensíveis, visando não perpetuar discriminações que podem advir do tratamento automatizado de dados².

Por fim, sendo a presente dissertação entregue em 2020, se faz necessário abordar a forma como os algoritmos estão sendo utilizados em meio à pandemia³ causada pelo COVID-

² Considerando 71, parágrafo 2º, RGPD: (...) A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

³ Segundo a Organização Mundial da Saúde (OMS), pandemia é a disseminação mundial de uma nova doença e o termo passa a ser usado quando uma epidemia, surto que afeta uma região, se espalha por diferentes continentes com transmissão sustentada de pessoa para pessoa.

19, sendo válida a problematização no que diz respeito à contraposição entre o direito individual e o direito coletivo.

Nesse sentido, tem-se assistido a um aumento na utilização e disponibilização de dados pessoais para tentativa de combate ao vírus. Como por exemplo, pode ser citada a utilização de dados de localização obtidos dos telefones celulares pessoais, para detecção de pessoas infectadas pelo vírus, ou a obtenção de dados de saúde pelo governo e por estabelecimentos para controlar a entrada de pessoas em determinados locais.

Em um primeiro momento, ao estudar a situação atual, deve ser levado em consideração que, embora tenham existido pandemias anteriores à do COVID-19, a tecnologia, os meios de comunicação e os meios de transporte existentes anteriormente nem se comparam com os atuais, não havendo uma forma certa para lidar com a situação. Assim, por se tratar de uma situação basicamente inédita, cada país passou a tentar combater o vírus de uma forma, passando a viger um estado de sítio na maioria das nações, com a utilização de decretos e medidas provisórias que permitem a utilização de dados pessoais para manterem isolados os cidadãos com suspeita ou confirmação de infecção.

Como por exemplo, podem ser citados os diversos aplicativos que surgiram em Portugal⁴, na China⁵ ou em Israel⁶ para detectar as pessoas confirmadas com o vírus, alertar a população da possibilidade de contágio em determinada região, ou ainda alertarem as autoridades se uma pessoa infectada sair de casa. Ainda, devido ao sistema de GPS ativo, tais dispositivos podem detectar onde a pessoa esteve nos últimos 14 dias, informando se ela esteve em um local em que tenha havido contágio ou notificando as pessoas próximas se há o risco de ela estar contaminada.

Nesse ponto, surge o questionamento sobre a obrigatoriedade da disponibilização e utilização de dados pessoais, como localização e históricos médicos, que, além de violar o direito à privacidade do indivíduo⁷, podem deixar dados pessoais disponíveis indefinitivamente para os desenvolvedores dos aplicativos ou dos governos que os utilizaram.

⁴<https://observador.pt/2020/04/28/como-sera-a-app-que-o-governo-quer-usar-para-rastrear-casos-de-covid-19-em-portugal/>. Consultado em 05 de outubro de 2020.

⁵https://www.uol.com.br/tilt/ultimas-noticias/rfi/2020/04/16/coronavirus-aplicativo-dos-contaminados-e-outras-tecnologias-ajudaram-a-china.htm?aff_source=56d95533a8284936a374e3a6da3d7996. Consultado em 05 de outubro de 2020.

⁶ <https://www.jpost.com/israel-news/israelis-dodge-covid-19-tracking-via>. Consultado em 05 de outubro de 2020.

⁷ Sobre o direito à privacidade nos tempos de pandemia, ver: GUIMARÃES, Maria Raquel; e REDINHA, Maria Regina - Through the Keyhole: Privacy in COVID-19 Times - A Portuguese Approach. Intersentia Online. 2020. Consult. em 13 de outubro de 2020. Disponível em: <https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/720?version=v-544bf2be-8004-f72f-8088-dea754a9a0da>

Além disso, em praticamente todos os países tem-se realizado a testagem de temperatura corporal para as pessoas poderem adentrar em supermercados, escolas, shoppings, lojas, entre outros. Vale informar que, embora a medição de temperatura não faça parte do objeto central da presente dissertação, por não se tratar de dado pessoal nos termos do RGPD, a obrigação do indivíduo em fornecer um dado de saúde a qualquer estabelecimento, sob pena de ver suprida sua liberdade de ir e vir, é de importante discussão.

Sobre o tema, a Comissão Nacional de Proteção de Dados alertou que os estabelecimentos de ensino que utilizarem e realizarem tratamento sobre os dados de saúde dos menores, têm a obrigação de cumprir os princípios e as regras legais de proteção dos dados pessoais determinados no RGPD. Nesse passo, a CNPD estabelece que

não basta o interesse legítimo do responsável ou de terceiro em prevenir o contágio da doença Covid-19 para se ter como lícito o tratamento. Não apenas porque o RGPD faz depender a consideração deste pressuposto de uma avaliação da não prevalência dos direitos e interesses dos titulares de dados, em especial quando estes sejam crianças, mas também porque em causa está um dado relativo à saúde, cujo tratamento está por regra proibido⁸.

Percebe-se que a CNPD tende a proteger a colheita e tratamento indiscriminado dos dados pessoais, buscando que sempre haja uma justificativa plausível para tanto.

Entretanto, há quem entenda que em situações de crise os direitos individuais devem sucumbir face aos direitos coletivos, de forma que, por conta da excepcionalidade da pandemia e dos riscos sociais advindos da inexistência de dados, a coleta e tratamento dos dados pessoais deve ser permitida sem justificativa prévia, visando evitar a propagação da pandemia.

Sopesando as perspectivas expostas, constata-se uma contraposição entre a defesa do macro e a do micro, entre os direitos coletivos e individuais. Se, de um lado, é louvável a proteção da sociedade, de outro, a disponibilização massiva dos dados pessoais, embora no presente seja justificada, gera uma perspectiva não desejada aos titulares de dados. Nesse diapasão, os dados obtidos sob ótica da proteção social, futuramente podem ser utilizados com outras finalidades, tendo em vista a possibilidade de serem armazenados e tratados, podendo ser utilizados para definir o perfil dos cidadãos.

⁸https://www.cnpd.pt/home/orientacoes/Orientacoes_medicao_temperatura_estabelecimentos_ensino.pdf. Consultado em 05 de outubro de 2020.

Vale ressaltar que grande parte dos aplicativos utilizados para combate à pandemia são de titularidade dos governos, sendo que a colheita de dados pessoais indiscriminada contribui, ainda, para a vigilância governamental.

São evidentes as vantagens da utilização de algoritmos para tomada de decisões, principalmente ao analisar da perspectiva social e empresarial, tendo em vista tornar o processo decisório mais rápido, com menos custo, e utilizando uma maior quantidade de dados.

Entretanto, deve-se chamar atenção que a coleta e tratamento indiscriminados de dados pessoais pode ensejar efeitos negativos não apenas ao titular de dados, que vê seus direitos à privacidade e dignidade suprimidos, como também à sociedade, tendo em vista perpetuar preconceitos e discriminações históricas.

1.2 A Definição de Perfis

O desenvolvimento de algoritmos mais eficientes e o aumento na quantidade de dados disponíveis, tornou possível a definição automatizada de perfis, podendo os perfis obtidos serem utilizados nas mais diversas áreas. Em razão da versatilidade no uso, os perfis passaram a ser considerados bens econômicos, sendo objeto de compra e venda.

Assim, em meio ao capitalismo de dados, os perfis passaram a ser considerados os bens de maior valor, razão pela qual foram alvo de especial atenção em diversas normas, e merecem uma análise pormenorizada.

Um perfil pode ser conceituado como uma ficha individual de cada sujeito, que o individualiza e o identifica como pertencente a determinado grupo ou categoria, contendo as tendências da pessoa, personalidade, histórico, entre outros.

O processo de realização de um perfil é chamado de “definição de perfil”, ou “*profiling*”, e é uma atividade de definição ampla, não circunscrita apenas à definição dada no meio jurídico. Assim, pode-se definir “*profiling*” como sendo o

“processo de descoberta de correlações entre diversos dados constantes de bases de dados que podem ser utilizados para identificar e representar um “sujeito” humano ou não humano (indivíduos ou grupos) e/ou a aplicação da definição de perfis (listas de dados correlacionados) para individualizar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria” (HILDEBRANDT, 2008, p. 19).

Em outras palavras, a definição de perfis consiste na descoberta de características parecidas entre diversos dados disponíveis, sendo que a existência da mesma característica presume o mesmo comportamento nos perfis. Assim, os perfis são como previsões baseadas nos comportamentos passados (HILDEBRANDT, 2008, p. 17).

Tem-se, então, que a definição de perfis é primordialmente probabilística, posto que prevê possibilidade da ocorrência de um comportamento com base na existência uma correlação entre determinados dados, determinada pela ocorrência da mesma correlação no passado (HILDEBRANDT, 2008, p. 22).

No que diz respeito à definição de “*profiling*” no meio jurídico, é importante focar a definição dada pelo Regulamento Geral de Proteção de Dados⁹, da qual podem ser extraídas 3 características principais: (a) é realizada de forma automatizada; (b) utiliza dados referentes a uma pessoa singular específica; (c) objetiva realizar inferências a partir da personalidade do titular de dados.

Antes de adentrar nas características da definição de perfis, vale salientar que, nos termos do regulamento, os perfis são definidos de acordo com os dados de uma pessoa singular, chamada de titular de dados¹⁰, sendo o perfil formado e aplicado na forma estipulada pelo responsável pelo tratamento dos dados¹¹. Evidencia-se que o regulamento não adentra na proteção de perfis de grupo, protegendo apenas os indivíduos singulares.

A característica de automatização da definição de perfil é devida ao fato de que a definição automatizada de perfis resulta de um processo de “mineração” algorítmica de dados disponíveis em grandes bancos de dados (*Big Data*). Assim, os algoritmos extraem padrões de correlação a partir de uma grande quantidade de dados, inferindo que os dados com determinadas características tendem a possuir determinado comportamento.

⁹ Artigo 4º, nº 4, RGPD: «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspectos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

¹⁰ Artigo 4º, nº 1, RGPD: «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

¹¹ Artigo 4º, nº 7, RGPD: “«Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

Nesse sentido, podem ser inferidas três etapas do processo de definição de perfis, quais sejam: (a) coleta de dados, (b) uso de algoritmos para desenvolver um modelo e (c) tomada de uma decisão com base nas informações e previsões obtidas (KAMARINOU, 2016, p. 8). Essa decisão final pode causar efeitos diretos ou indiretos na esfera jurídica do titular de dados, a depender da utilização direta ou indireta do perfil definido para enquadrar o titular como desejado ou não como contraparte contratual em determinada situação.

Evidencia-se que o resultado do processamento de todos os dados disponíveis de um indivíduo, juntamente com as correlações realizadas em dados de outras pessoas e dados sociais, tornam possível a definição do perfil de um indivíduo, existindo uma presunção comportamental a partir do perfil definido. Ou seja, a partir da personalidade e do comportamento histórico da pessoa e da sociedade, presume-se que, a pessoa titular de determinados dados, com determinadas características, se enquadra em um tipo de perfil, sendo previsto que pessoas com aquele perfil tende a ter determinado comportamento.

Vale ressaltar que o processamento algorítmico indica a existência de uma relação entre os dados, mas nem sempre explicam a razão da correlação (HILDEBRANDT, 2008, p. 18), apenas prevendo o comportamento provável do titular.

Resumidamente, pode-se inferir que o processo de definição de perfis se refere ao uso de algoritmos e outras tecnologias para criar, descobrir ou construir informações a partir de uma grande quantidade de dados, situada em diversos bancos de dados (HILDEBRANDT, 2008, p. 17).

Ressalta-se que, por conta de a precisão do perfil analisado depender não só da quantidade, mas também da qualidade dos dados inseridos, os perfis têm algumas limitações natas, como atraso de dados, falta de precisão e falta de transparência (OECD, 2018, p. 4).

Ainda, além de criar perfis descritivos sobre os indivíduos, os dados processados podem ser utilizados para verificar a existência de padrões predefinidos ou comportamentos tidos como anormais ou não desejados (KAMARINOU, 2016, p. 8). Dessa forma, verificada a existência de um comportamento “ruim”, determinado perfil pode ser descartado de uma seleção. Como exemplo, pode ser citada a não concessão de um financiamento para determinado indivíduo com fulcro na presunção de ele não irá realizar o pagamento, tendo em vista seu comportamento recorrente em se endividar, e no padrão social de que, as pessoas com tal tipo de histórico, tendem a não realizar o pagamento dos financiamentos concedidos.

Quanto aos dados utilizados para realizar a definição de perfis, deve-se atentar para o fato de que o Regulamento Geral de Proteção de Dados limita a possibilidade de utilização de

“*Big Data*” e de coleta e armazenamento de grande quantidade de dados ao prever os princípios da minimização de dados¹² e da limitação das finalidades¹³.

Conclui-se que o responsável pelo tratamento, ao definir um perfil, deve utilizar um algoritmo que colete e trate apenas os dados necessários para a finalidade do tratamento, sendo a finalidade definida pelo responsável.

Outro ponto importante a ser ressaltado é que o RGPD considera os perfis definidos como dados pessoais, os protegendo de forma equiparada¹⁴.

Saindo do âmbito do RGPD, é importante analisar as definições de “definição de perfil” trazidas por algumas legislações nacionais.

A legislação portuguesa¹⁵ conceitua a definição de perfis¹⁶ de forma similar ao RGPD, podendo ser extraídas as mesmas características previamente analisadas (automatização da definição dos perfis, utilização de dados pessoais de uma pessoa singular e realização de inferências a partir do perfil definido).

Destaca-se que o artigo 6º, número 2, da Lei 59/2019 de 8 de agosto, expressamente proíbe as definições de perfis que conduzam à discriminação de pessoas singulares com base em categorias especiais de dados pessoais¹⁷.

Já a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira (lei 13.709, de 14 de agosto de 2018), não traz uma definição concreta da expressão definição de perfil, mas

¹² Artigo 5º, n.º 1, “c”, RGPD: Os dados pessoais são: “c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

¹³ Artigo 5º, n.º 1, “b”, RGPD: Os dados pessoais são: “Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);

¹⁴ Considerando 72, RGPD: A definição de perfis está sujeita às regras do presente regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados.

¹⁵ Lei 59/2019 de 8 de agosto: aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

¹⁶ Art. 3º, 1, (f), L 59/2019: «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, a sua saúde, as suas preferências pessoais, os seus interesses, a sua fiabilidade, o seu comportamento, a sua localização ou as suas deslocações;

¹⁷ Artigo 6.º, Lei 59/2019 - Tratamento de categorias especiais de dados pessoais: 1 - O tratamento dos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como dos dados genéticos, dos dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dos dados relativos à saúde ou dos dados relativos à vida sexual ou à orientação sexual, só pode ser efetuado se for estritamente necessário, se estiver sujeito a garantias adequadas de proteção dos direitos e liberdades do titular dos dados, e se: a) For autorizado por lei; b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados. 2 - São proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais previstos no número anterior.

considera como dados pessoais os “utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada” (artigo 12, § 2º, LGPD).

Do conceito dado pela legislação brasileira extrai-se que, para que o perfil seja considerado dado pessoal, deva ser possível identificar a pessoa singular.

Em síntese, os perfis são basicamente modelos estatísticos, obtidos com a inserção dos dados pessoais em um sistema, que visam prever o comportamento do titular dos dados.

1.3 Decisões Automatizadas com base em Definição de Perfis

Diz-se automatizada uma decisão quando ela é tomada sem intervenção humana (BRKAN, 2017, p. 3), apenas com a utilização de algoritmos e dados disponíveis. Assim, uma decisão é automatizada quando um algoritmo, por meio de correlações entre dados, determina uma consequência para a situação analisada, podendo essa consequência ser vinculante, ou não.

Devido a existirem inúmeros tipos de decisões automatizadas, vale estabelecer que no presente trabalho serão abordadas as decisões individuais automatizadas, as quais, por analisarem dados pessoais, produzem efeitos jurídicos sobre uma pessoa singular (VERONESE, 2019, p. 397), merecendo atenção das normas regulamentadoras.

Dentre as decisões individuais automatizadas, chama a atenção as que são tomadas com base na análise do perfil individual, de forma que o algoritmo, ao verificar os perfis disponíveis, dá uma consequência relacionada à finalidade que lhe foi previamente estabelecida. Em tais casos, os perfis analisados podem ter sido obtidos por meio de formulários preenchidos pelos titulares de dados, por meio do processamento de dados disponíveis *on-line*, ou utilizando-se de ambas técnicas.

O resultado da decisão automatizada pode, ou não, ser vinculante. Quando a decisão automatizada pode ser revista por um indivíduo, ela é dita não vinculante. As decisões não vinculantes, por serem definidas com intervenção humana, tendem a ser menos injustas e mais transparentes, podendo o responsável pela decisão explicar o motivo dela. Nesse sentido, não priva o titular de dados de direitos fundamentais (BRKAN, 2017, p. 3) e viabiliza uma melhor aplicação das normas relativas ao uso e tratamento de dados pessoais.

O problema maior reside nas decisões automatizadas com caráter vinculante, quando o resultado do processamento automatizado é automaticamente aplicado e gera um efeito jurídico no titular de dados. Em tais casos o titular de dados teria sua esfera jurídica atacada, sem ter meios de saber a razão do ataque.

Como exemplo, pode-se citar a inserção de dados bancários e propriedades de um sujeito em um algoritmo, com o objetivo de determinar se ele teria credibilidade financeira suficiente para poder fazer um empréstimo bancário. Assim, o algoritmo, analisando os dados inseridos, os dados históricos da empresa e dados sociais obtidos *on-line*, verifica a tendência de indivíduos com aquele perfil em pagar ou não os empréstimos realizados, decidindo pela concessão ou não do empréstimo. Se o resultado obtido do processamento fosse enviado a um funcionário da empresa, e esse, analisando o caso, julgasse que a pessoa não seria adequada para o empréstimo, a decisão não seria considerada totalmente automatizada. A decisão somente seria considerada completamente automatizada no caso de o perfil analisado ser automaticamente descartado da lista de pessoas aptas a receberem um empréstimo, não tendo o indivíduo como saber o motivo do descarte.

São nos casos de decisões tomadas exclusivamente com base no tratamento automatizado que há a tendência de intervenção legislativa, ou proibindo tal tipo de decisão, ou providenciando medidas de segurança para tentar garantir os direitos mínimos do indivíduo.

Há essa tendência na regulação das decisões automatizadas devido à alta probabilidade de os algoritmos perpetuarem comportamentos sociais existentes nos bancos de dados, de forma que as decisões podem conter traços de preconceito, discriminação ou injustiça.

Assim, ao permitir que as correlações algorítmicas sejam avaliadas, a intervenção humana tende a minimizar os efeitos negativos das decisões automatizadas, podendo dar uma certa transparência à tomada de decisões e determinar se o processamento algorítmico foi realmente justo, útil e adequado (FRAZÃO, 2019, p. 35).

1.4 Decisões Individuais Automatizadas e Definição de Perfis no Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 – RGPD) concede ao titular de dados o direito pessoal de não ser sujeito a decisões tomadas de forma exclusivamente automatizada com base na definição de perfis¹⁸.

¹⁸ Artigo 22º, RGPD - Decisões individuais automatizadas, incluindo definição de perfis. 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 nº 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

Percebe-se a existência de três condições para que uma decisão automatizada ou definição de perfis seja proibida pelo regulamento: a decisão deve ser (a) individual, (b) baseada somente no processamento automatizado de dados e (c) precisa ter efeitos legais ou significantes para com o titular dos dados (BRKAN, 2017, p. 8).

A primeira condição resulta do artigo 1º do RGPD, o qual determina que o regulamento é aplicável apenas à proteção das pessoas singulares, presumindo-se excluídas do âmbito de aplicação do regulamento as decisões tomadas para um grupo ou uma coletividade. Tal exclusão, faz com que exista uma diferenciação no tratamento de dados singulares e dados coletivos.

Nesse sentido, a necessidade de individualização da decisão, acaba por possibilitar que as empresas se utilizem de formas automatizadas de tomada de decisão. Ora, boa parte das decisões automatizadas, incluindo a definição de perfis, são tomadas em uma perspectiva grupal, posto que há a tendência em separar os perfis com as mesmas características em grupos e tomar a decisão para todo o grupo, não para os perfis individualizados. Assim, para se esquivarem do âmbito de aplicação do regulamento, as empresas podem vir a adotar decisões coletivas sempre que possível (BRKAN, 2017, p. 9).

Uma possibilidade para impedir o desvirtuamento do regulamento, é considerar que uma decisão sobre um grupo é, na verdade, uma decisão sobre diversos indivíduos (BRKAN, 2017, p. 9), permitindo que incida as normas do RGPD sobre decisões automatizadas em relação à uma coletividade.

A segunda condição extraída do artigo 22, nº 1, RGPD, é que a decisão seja tomada exclusivamente por meio do processamento automatizado de dados. Há, assim, uma imposição do RGPD de que sempre exista algum tipo de intervenção humana durante o processo de tomada de decisão.

É importante, então, averiguar se qualquer tipo de intervenção humana seria suficiente a suprir a imposição dada pelo Regulamento, sendo necessária a verificação do nível de influência do indivíduo na decisão final. Nesse aspecto, não basta que o indivíduo possa intervir

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. 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

apenas para perpetuar o resultado do processamento, sendo necessário que a pessoa responsável possa influenciar na decisão final, a modificando ou rejeitando (TODOLÍ-SIGNES, 2018, p. 10).

Por fim, o RGPD estabelece que somente decisões automatizadas que produzam efeitos na esfera jurídica do titular de dados, ou o afete significativamente de forma similar, são proibidas. Assim, uma decisão que sirva apenas para pesquisa, não produzindo qualquer efeito relevante sob a esfera jurídica do titular de dados, mesmo que exclusivamente automatizada, não estaria sob o cerne do Regulamento Geral de Proteção de Dados.

Em contraposição às regras gerais de proibição, o número 2 do artigo 22, autoriza que sejam tomadas decisões automatizadas, incluindo a definição de perfil, em três situações, desde que observem as proteções do nº 3.

Destaca-se que o considerando 71 do RGPD determina que, mesmo quando o tratamento automatizado é permitido, devem ser tomadas medidas adequadas para proteção do titular de dados, sendo o direito de obter intervenção humana uma das medidas determinadas¹⁹. O referido considerando também dita regras para assegurar que o tratamento dos dados seja feito de forma equitativa e transparente, visando proteger os titulares de dados de possíveis

¹⁹ Considerando 71, RGPD: O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.

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

consequências negativas advindas da utilização de decisões automatizadas, incluindo a definição de perfis

Retornando às permissões concedidas para tomadas de decisões automatizadas, o art. 22, nº 2, (a), RGPD, traz as hipóteses em que o tratamento seja necessário para celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento.

Se faz necessário, então, saber quando o tratamento automatizado é considerado necessário para celebrar ou cumprir o contrato com o titular dos dados (MENDOZA, 2017, p. 15).

Extraí-se do conceito de necessidade 2 elementos principais, sendo eles: (a) a relação de causalidade existente entre o tratamento e o cumprimento da finalidade dele; e (b) a razoabilidade do processamento, ou seja, quando a finalidade do tratamento não pode ser razoavelmente atingida por outros meios²⁰.

É perceptível que o conceito de necessidade não exige que o tratamento seja absolutamente indispensável, mas sim que deve ser observada a proporcionalidade entre o fundamento para o tratamento dos dados e os direitos do sujeito (RUCKER, 2019, p. 66).

Nessa linha, há que objetivamente se avaliar a necessidade da utilização de decisões automatizadas, somente sendo permitida a automatização da decisão quando não for viável que ela seja tomada de outra forma (RUCKER., 2019, p. 150).

A segunda permissão de utilização de decisões automatizadas, incluindo a definição de perfis, dada pelo Regulamento Geral de Proteção de Dados, se dá quando elas forem autorizadas pelo direito da União ou do Estado Membro a que o responsável pelo tratamento estiver sujeito. Em tais casos, se faz necessário que estejam previstas em leis medidas adequadas para salvaguardar os direitos e legítimos interesses do titular de dados (artigo 22, nº, 2, b, RGPD).

Percebe-se que o RGPD concede aos legisladores nacionais e da União o poder de autorizar a tomada de decisões automatizadas em determinados casos (RUCKER, 2019, p. 150).

Por fim, o regulamento permite que sejam tomadas decisões de forma automatizada quando forem baseadas no consentimento explícito do titular de dados (art. 22, nº 2, c). Tal consentimento deve ser dado de forma livre, específica, informada e explícita (RGPD, art. 4º, nº 11), dizendo respeito apenas aos dados daquele que deu o consentimento.

Dentre as permissões dadas pelo regulamento, a do consentimento explícito se destaca como a mais controversa, posto que o consentimento tende a ser um fator não confiável em

²⁰ Considerando 39, RGPD: (...) os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. (...)

grande parte das situações, principalmente em se tratar de contratos nos quais há uma desigualdade entre as partes.

Sobre o tema, o considerando 43 do Regulamento²¹ presume que, nos casos em que há uma desigualdade entre as partes, sendo uma hipossuficiente ou vulnerável em relação à outra, o consentimento não é dado de livre vontade, não podendo ser utilizado como fundamento para justificar o tratamento de dados pessoais. Assim, o consentimento de um candidato a uma vaga de emprego, de um solicitante de crédito ou de seguro de saúde, não deve ser considerado requisito de validade para o tratamento automatizado de dados, excluindo-se, então, as hipóteses dos artigos 6º, número 1, alínea “a”, artigo 9º, número 2, alínea “a” e artigo 22º, número 2, alínea “c”.

Há ainda a presunção de que o consentimento não é dado de livre vontade nos casos em que a execução de um contrato depender do consentimento²², tendo em vista que a dependência do consentimento para a execução faz com que o indivíduo não tenha opção, a não ser consentir com as decisões automatizadas.

Ainda, nos termos dos dispositivos citados, o consentimento deve ser dado de forma clara e informada, se fazendo necessário que o titular de dados seja informado sobre a realização e as consequências da decisão automatizada ou da definição de perfis.

Vale salientar que, mesmo quando o consentimento for considerado válido, o tratamento de dados deve ser limitado ao necessário para atingir o propósito do tratamento (RUCKER, 2019, p. 90), tendo em vista os princípios da limitação das finalidades (artigo 5º, nº 1, “b”) e da minimização de dados (artigo 5º, nº 1, “c”).

Conclui-se que o consentimento somente pode ser considerado válido se o titular de dados foi informado sobre a possibilidade de a decisão ser tomada de forma automatizada, e pôde escolher o tipo de processamento utilizado, inexistindo qualquer intimidação, coerção, ou consequências negativas no caso de não ser dado o consentimento (GT 29, WP 259, p. 6).

²¹ Considerando 43, RGPD: “a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento. (...) Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução”.

²² Artigo 7º, 4, RGPD: “Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato”.

Finalmente, o artigo 22, nº 4, do RGPD, em concordância com o artigo 9º, RGPD, proíbe que sejam tomadas decisões automatizadas, incluindo a definição de perfis, com base em categorias especiais de dados pessoais (dados sensíveis)²³, somente as permitindo nas hipóteses em que haja o consentimento explícito do titular de dados ou se o tratamento de dados sensíveis for necessário por motivos de interesse público, sempre respeitando os direitos e liberdades e os legítimos interesses do titular.

Ressalta-se que o considerando 51 do Regulamento dispõe que “merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais”.

Evidente que a proibição do tratamento de dados sensíveis, ao manter as características físicas, de personalidade e opinião, longe do embasamento para a tomada de decisão, objetiva prevenir que não sejam tomadas decisões discriminatórias, desiguais ou preconceituosas.

Vale lembrar que as inferências algorítmicas podem transformar dados “normais” em dados sensíveis, devendo ser questionada a possibilidade de utilização dos “*bastard data*” no processo de definição automatizada de perfis.

Levando em consideração que o RGPD confere aos dados sensíveis uma proteção especial face às demais categorias de dados, em virtude dos riscos aos direitos e liberdades fundamentais advindos do tratamento deles, pode-se presumir que a proteção se estende aos dados especiais provenientes de “*bastard data*”.

Ora, o tratamento de um “*bastard data*” de categoria especial traz os mesmos riscos que o tratamento de dados sensíveis originários, sendo, inclusive, mais problemático, tendo em vista que o titular dos dados sequer sabe que o responsável pelo tratamento tem à disposição tal dado sensível.

Ademais, mesmo que o titular tenha dado o consentimento para o tratamento automatizado dos dados originários, o RGPD determina que haja um consentimento explícito para o tratamento de dados sensíveis, de forma que, uma vez descoberto um “*bastard data*” sensível, é necessário o consentimento expresso do titular para que possa ser realizado seu tratamento.

²³ Artigo 9º, 1, RGPD: 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Outro ponto importante de ser abordado é a imposição de uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais nos casos em que uma decisão automatizada produza efeitos jurídicos nos titulares. Referida imposição objetiva a identificação de possíveis riscos aos direitos individuais dos titulares²⁴ advindos do tratamento automatizado de dados pessoais.

Resta evidente a preocupação do legislador europeu com a utilização de decisões automatizadas, incluindo a definição de perfis, razão pela qual conferiu direitos e deveres específicos para o processamento automatizado de dados, na tentativa de conter os danos à esfera privada do titular de dados.

1.5 Outros Direitos Concedidos aos Titulares de Dados Pelo Regulamento Geral de Proteção de Dados

Saindo da esfera exclusiva das decisões automatizadas, incluindo a definição de perfis, é importante o estudo de direitos gerais do titular de dados concedidos pelo Regulamento Geral de Proteção de Dados. É importante observar que os artigos 12 a 14 do RGPD conferem ao titular de dados direitos anteriores à realização do tratamento, objetivando proteger o indivíduo, enquanto os artigos 15 a 19 tratam do momento posterior à realização do tratamento, visando a revisão, retificação e o apagamento dos dados.

O primeiro direito que pode ser observado é o direito à transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados, trazidas pelo artigo 12 do RGPD. Referido artigo determina que o responsável pelo tratamento deve dar ao titular de dados todas as informações relativas ao tratamento que será realizado, devendo as informações serem prestadas de forma clara e transparente.

Já os artigos 13 e 14 do Regulamento, conferem ao titular dos dados o direito de aceder, retificar, apagar ou limitar o tratamento dos dados pessoais.

²⁴ Artigo 35.º, RGPD: 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

Além disso, no caso de existirem decisões automatizadas, incluindo a definição de perfis, fica o responsável pelo tratamento obrigado a informar o titular de dados sobre a existência do processamento automatizado, além de conceder informações úteis relativas à lógica subjacente da decisão, bem como sobre a importância dela e as consequências previstas do resultado do tratamento²⁵.

Os artigos 13 e 14 trazem também normas específicas para o processamento de dados para decisões automatizadas, incluindo a definição de perfis, concedendo, além dos direitos já citados, o direito à obtenção de informação sobre a lógica envolvendo o processamento de dados (artigos 13º, nº 2, “f”; 14º, nº 2, “g”; e 15º, nº 1, “h”). Estariam incluídas em tal informação: (a) informação sobre os dados que serviram para as inferências da decisão automatizada; (b) informação sobre a série de fatores que influenciaram a decisão; (c) informação sobre a relativa importância de fatores que influenciaram na decisão e (d) uma explicação razoável sobre o porquê certa decisão foi tomada (BRKAN, 2017, p. 15).

De mais a mais, o artigo 15 confere uma espécie de “Direito à Explicação”, concedendo ao titular de dados o direito de saber quais dados estão sendo tratados, a forma que o tratamento foi realizado, as finalidades do tratamento, e de, inclusive, acessar os dados utilizados²⁶.

Há, ainda, o direito de retificação (artigo 16, RGPD), o direito ao apagamento dos dados (artigo 17, RGPD) e o direito à limitação do tratamento (artigo 18, RGPD). A leitura dos dispositivos citados faz concluir que o titular de dados tem o direito de revisar qualquer decisão baseada na utilização de seus dados pessoais (RUCKER, 2019, p. 151).

Conclui-se que o processamento de dados pessoais deve ser realizado de forma transparente em face da pessoa que tem seus dados pessoais coletados, utilizados, consultados ou processados (BRKAN, 2017, p. 14), visando que o sujeito entenda como o processamento foi realizado e o motivo da decisão tomada.

²⁵ Artigos 13 (2) (f) e 14 (2) (g), RGPD.

²⁶ Artigo 15º, 1, RGPD: 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Certamente que o envolvimento dos indivíduos em todas as etapas do processamento de dados diminui os riscos de manipulação dos dados pelos responsáveis pelo tratamento (OECD, 2018, p. 4), tornando possível que o titular conteste a decisão de forma fundamentada.

Ainda, o artigo 25 do RGPD estabelece o direito a proteção de dados desde a concepção e por defeito, prevendo a necessidade de aplicação de medidas técnicas e organizativas adequadas para aplicar com eficácia os princípios da proteção de dados e incluir as garantias no tratamento, tais quais a anonimização²⁷ e a pseudonimização²⁸.

Ocorre que, embora necessários, os direitos relacionados à revisão da decisão acabam sendo de difícil execução, principalmente em razão de a maioria dos algoritmos utilizados para o processamento de dados realizarem conexões entre os dados de forma tão complexa, rápida e eficiente, que se torna praticamente impossível saber o motivo da decisão obtida, ou quais dados foram utilizados para chegar no resultado.

Outro fator que dificulta a execução dos direitos de revisão é o processamento de dados anônimos (ex. localização do GPS), de dados tornados públicos pelos titulares e dados provenientes de “*Big Data*” (obtidos *on-line*), que, a depender da situação, podem não adentrar na proteção do Regulamento. Por serem dados com a origem de difícil identificação, ao serem processados juntamente com os dados pessoais, tornam praticamente impossível que o titular de dados exerça efetivamente seus direitos (TODOLÍ-SIGNES, 2018, p. 6).

Evidente que o conhecimento das informações e dados utilizados para chegar a uma decisão algorítmica, juntamente com a transparência do procedimento, é o que proporciona a efetivação dos direitos dados pelo RGPD, posto que somente sabendo o que fundamentou a decisão, é que uma defesa contra uma decisão preconceituosa, injusta ou discriminatória poderá ser exercida.

Nesse passo, uma solução para a falta de transparência seria a elaboração de algoritmos que, ao realizar o processamento de dados, deixe traços que possibilitem o rastreamento dos dados utilizados para que a decisão fosse tomada.

²⁷ Considerando 26, RGPD: Informações anónimas são as que não dizem respeito a “uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado”. Por isso, o RGPD não diz respeito ao tratamento dessas informações anónimas.

²⁸ Art. 4, 5, RGPD: «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

1.6 Decisões Individuais Automatizadas na Legislação Portuguesa. Leis 58/2019 e 59/2019, de 8 de agosto.

O Regulamento Geral de Proteção de Dados criou nos Estados-Membros o dever de “tomar as medidas necessárias para adaptar as respectivas legislações”, bem como “a possibilidade de especificarem mais a aplicação das regras de proteção de dados em determinados domínios” (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 1).

Visando a efetivação do regulamento, foram promulgadas as Leis nº 58/2019 e 59/2019, de 8 de agosto, visando assegurar a execução, na ordem jurídica portuguesa, do Regulamento Geral de Proteção de Dados.

Ambas as leis tendem a enfatizar o disposto no RGPD, trazendo dispositivos similares aos do regulamento, ou que visam limitar o tratamento dos dados determinado pelo RGPD.

A Lei 59/2019 restringe o âmbito de aplicação do regulamento, determinando, em seu artigo 5º, que “o tratamento de dados pessoais só é lícito se estiver previsto na lei e na medida em que for necessário para o exercício de uma atribuição da autoridade competente” (nº 1) ou se for necessário para a proteção dos interesses vitais do titular dos dados ou de outra pessoa singular” (nº 3).

Ainda, em relação aos direitos gerais dos titulares de dados, os artigos 13º a 19º da Lei 59/2019 praticamente repetem os direitos conferidos pelos artigos 12º a 19º do RGPD.

No que diz respeito às decisões individuais automatizadas, o artigo 11º, da Lei 59/2019²⁹, equivale ao artigo 22º do RGPD, proibindo a tomada de decisões de forma completamente automatizada e que tenham como fundamento a utilização de dados sensíveis.

O artigo 6º do referido diploma legal³⁰, por sua vez, proíbe o tratamento de categorias especiais de dados pessoais, apenas o permitindo em situações específicas. Ressalta-se que o

²⁹ Artigo 11.º, L 59/2019: Decisões individuais automatizadas. 1 — São proibidas as decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, exceto quando autorizadas por lei, desde que seja previsto o direito de o titular dos dados obter a intervenção humana do responsável pelo tratamento. 2 — As decisões a que se refere o número anterior não podem basear -se nas categorias especiais de dados pessoais previstos no artigo 6.º.

³⁰ Artigo 6.º, L 59/2019: Tratamento de categorias especiais de dados pessoais 1 — O tratamento dos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como dos dados genéticos, dos dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dos dados relativos à saúde ou dos dados relativos à vida sexual ou à orientação sexual, só pode ser efetuado se for estritamente necessário, se estiver sujeito a garantias adequadas de proteção dos direitos e liberdades do titular dos dados, e se: a) For autorizado por lei; b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados. 2 — São proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais previstos no número anterior.

número 2 do artigo 6º proíbe expressamente a realização de definições de perfis que conduzam à discriminação de pessoas singulares com base em dados sensíveis, percebendo uma maior preocupação do legislador português com a utilização de tal categoria de dados.

Constata-se que a legislação portuguesa, ao restringir as permissões para o tratamento de dados sensíveis, é mais protecionista que o RGPD³¹, o qual apresenta mais hipóteses que possibilitam o tratamento dos dados de categorias especiais.

Chama a atenção que a legislação portuguesa não coloca o consentimento explícito do titular de dados como uma das formas de permissão para o tratamento de categoria especiais de dados, certamente devido ao fato de tal consentimento ser facilmente manipulável.

Nessa margem, além de diminuir o rol de permissões para o tratamento de dados especiais, a lei 59/2019 reduz ainda mais as permissões no que diz respeito às definições de perfis, expressamente proibindo qualquer tipo de definição de perfil com base em dados sensíveis que desencadeie na discriminação do titular de dados.

1.6.1 A Problemática do Consentimento na Lei 58/2019, de 8 de agosto.

A Lei 58/2019 de 8 de Agosto, traz algumas normas que foram assinaladas pela Comissão Nacional de Proteção de Dados, na Deliberação/2019/494, como manifestamente incompatíveis com o Direito da União, sendo insuprível a antinomia com as normas do RGPD e com a Carta dos Direitos Fundamentais da União Europeia (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 2).

Dentre as normas assinaladas como incompatíveis com o RGPD, destaca-se o artigo 61º, número 2º³², que trata da renovação do consentimento, pelos motivos a seguir expostos.

Em um primeiro momento, vale ressaltar que o Regulamento Geral de Proteção de Dados distingue como fontes distintas e independentes de licitude do tratamento automatizado de dados pessoais: (a) o consentimento do titular de dados e (b) a necessidade do tratamento automatizado de dados para celebração ou execução de um contrato entre o titular de dados e o responsável pelo tratamento (artigo 6º e artigo 22º, RGPD).

³¹ O artigo 9º do RGPD apresenta 9 alíneas de exceção à proibição do tratamento de dados sensíveis.

³² Artigo 61.º, 2, L 58/2019 - Caso a caducidade do consentimento seja motivo de cessação de contrato em que o titular de dados seja parte, o tratamento de dados é lícito até que esta ocorra.

Destaca-se que o artigo 22º, 4, do RGPD, apenas permite o tratamento automatizado de dados sensíveis na hipótese de existir consentimento explícito do titular, nada mencionando sobre a necessidade do tratamento para celebração ou execução de um contrato.

Conclui-se que o tratamento de dados em virtude da necessidade para a celebração ou execução de um contrato não tem, nem pode ter, por fundamento o consentimento do titular (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 10), posto serem fundamentos distintos.

Assim, se o tratamento de dados for necessário para celebração ou execução de um contrato, a obtenção do consentimento do titular seria apenas uma formalidade, sendo a necessidade do tratamento a justificativa para sua realização.

De outro lado, nos casos em que o tratamento for realizado com base no consentimento do titular de dados, ele deve ser dado expressamente e de livre vontade, não se considerando que o consentimento foi dado de livre vontade “se o titular dos dados não dispuser de uma escolha verdadeira ou não puder recusar nem retirar o consentimento sem ser prejudicado” (considerando 42, RGPD).

Ainda, o considerando 43 do RGPD presume que o consentimento não foi dado de livre vontade se “a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução”.

Conclui-se que, nos termos do RGPD, a validade do consentimento somente vai ser analisada como causa de licitude do tratamento de dados nos casos em que o consentimento for o fundamento do tratamento, não se analisando, em tais casos, a necessidade do tratamento para a execução ou conclusão de um contrato.

Ocorre que o legislador português, ao transpor as regras relativas aos fundamentos de licitude do tratamento de dados, buscou solucionar o problema advindo do fato de o RGPD (artigo 22º, 4) não colocar a necessidade da realização do tratamento de dados, para execução ou celebração de um contrato, como fundamento para legitimar o tratamento dos dados pessoais sensíveis e para utilizar decisões individuais automatizadas, incluindo a definição de perfis.

Entretanto, na tentativa de sanar os problemas apontados, a legislação portuguesa acabou confundindo os dois fundamentos autônomos de legitimação do tratamento de dados (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 10) abordados.

Assim dispõe o artigo 61º, número 2, da Lei 58/2019, de 8 de agosto: “caso a caducidade do consentimento seja motivo de cessação do contrato em que o titular de dados seja parte, o tratamento de dados é lícito até que esta ocorra”.

Percebe-se a confusão entre os fundamentos de legitimidade para o tratamento de dados, quando a norma dispõe como lícito o tratamento até que ocorra a caducidade do consentimento motivo de cessação do contrato em que o titular de dados seja parte.

Ora, se a caducidade do consentimento para a realização do tratamento faz cessar o contrato, o tratamento dos dados passa a ser entendido como necessário para a execução do contrato, sendo então considerado uma condição de vigência. Assim, tendo em vista a necessidade do tratamento, o consentimento não pode ser considerado fundamento legal para o tratamento (GT 29, WP 259, p. 9).

Evidencia-se que o consentimento do titular somente deve ser fundamento de legitimidade quando o tratamento não for necessário para a execução do contrato. Isto pois, nos casos em que o tratamento é necessário para a execução do contrato, a falta do consentimento obstará a execução do contrato, retirando a possibilidade de se considerar o consentimento como obtido de livre vontade, indo contra o disposto no artigo 4º, alínea 11, do RGPD.

Ainda, segundo a Deliberação em análise, o artigo 7º, 4º, do RGPD, apenas regula a relevância do consentimento para tratamentos que não sejam necessários à execução de um contrato. Conclui-se que o tratamento de dados necessários à execução do contrato não tem, nem pode ter, o consentimento do titular como fundamento (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 10 V).

Pelo exposto, tendo em vista que o consentimento do titular de dados e a necessidade do tratamento de dados para celebração ou execução de um contrato entre o titular de dados e um responsável pelo tratamento são fontes distintas de licitude ou legitimação de tratamentos de dados pessoais, fica clara a confusão entre os dois fundamentos autônomos de legitimação do tratamento de dados na legislação portuguesa (COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, 2019, p. 10).

Assim, por conta da incompatibilidade entre a norma portuguesa e os artigos apontados do RGPD (artigo 4º, alínea 11, e artigo 6º, alíneas a) e b), RGPD), a Comissão Nacional de Proteção de Dados optou pela não aplicação do artigo 61º, número 2, da Lei 58/2019, de 8 de agosto nas questões a serem apreciadas.

1.7 Decisões Individuais Automatizadas na Legislação Brasileira. Lei 13.709, de 14 de agosto de 2018.

Seguindo a tendência mundial de regulamentação da proteção dos dados pessoais, o Brasil aprovou, em 28 de agosto de 2019, a Lei Geral de Proteção de Dados (Lei 13.709/2018), conhecida como LGPD, a qual “versa sobre o tratamento de dados pessoais de pessoas naturais, tanto em meio físico quanto digital, com a finalidade de tutelar seus direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade” (PEDROSO XAVIER, 2019, p. 490).

Ao comparar a LGPD com o RGPD, percebe-se uma convergência nos “princípios enunciados por ambas as regulamentações, no modelo *ex ante* de proteção, bem como no papel central da *accountability*” (BIONI, 2019, 805), sendo clara a influência do processo legislativo europeu na lei brasileira.

Para nortear as possibilidades de tratamento de dados, o artigo 6º LGPD, elenca alguns princípios, valendo destacar os princípios da finalidade (I), adequação (II) e necessidade (III), que correspondem aos princípios da limitação das finalidades e da minimização dos dados trazidos pelo RGPD. Destaca-se, ainda, os princípios da transparência (VI), segurança (VII) prevenção (VIII) e da não discriminação (IX), que visam prevenir os possíveis danos causados pelo tratamento de dados pessoais, valendo informar que os três últimos não têm correspondência no RGPD.

Quanto aos fundamentos de licitude para o tratamento de dados pessoais, a legislação brasileira abrange outras situações além das elencadas pelo regulamento europeu, como por exemplo o tratamento para a proteção do crédito (artigo 7º, X, L 13.709/2018).

Vale ressaltar que a lei brasileira, assim como o RGPD, apresenta o consentimento do titular e a necessidade do tratamento para execução de contrato do qual ele seja parte, como fontes distintas de licitude para realização do tratamento (artigo 7º, I e V, LGPD). Ainda, nos termos da legislação brasileira, a necessidade não pode ser considerada fundamento válido para tratamento de dados sensíveis (artigo 11, I e II, LGPD).

No que diz respeito ao tratamento automatizado de dados pessoais, o artigo 20 da Lei 13.709/2018, confere ao titular dos dados o direito de “solicitar a revisão das decisões tomadas unicamente com base no tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade”.

Percebe-se que a legislação brasileira não menciona expressamente o direito de obter intervenção humana, apenas conferindo ao titular o direito de revisão da decisão tomada com base no tratamento automatizado de dados pessoais.

Ainda, no caso de o responsável pelo tratamento se negar a fornecer informações sobre os critérios e procedimentos utilizados para a decisão automatizada, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios no tratamento automatizado³³.

O artigo 21 da LGPD, por sua vez, proíbe a utilização de dados pessoais referentes ao exercício regular de direitos pelo titular em seu prejuízo, não havendo disposição correspondente no RPDG.

Conclui-se que a LGPD foi altamente influenciada pelo RPDG, havendo correspondência de inúmeros dispositivos entre as normas. Entretanto, existem dispositivos divergentes, devendo ser levado em consideração o histórico de evolução das regulamentações e o local em que foram promulgadas.

Percebe-se que a lei brasileira permite a realização do tratamento de dados em mais situações que o RPDG, apresentando menos direitos protetórios, principalmente ao se tratar de decisões automatizadas. Pode se considerar a maior proteção conferida pelo legislador europeu como resultado da experiência com regulamentações passadas menos protetivas.

Entretanto, por ser uma legislação mais atual, a LGPD apresenta direitos que não foram abordados pelo RPDG, como os relacionados a anonimização e pseudonimização dos dados pessoais.

Conclui-se que, embora apresentem dispositivos divergentes, ambas disposições buscam proteger o titular de dados, sendo louvável o esforço dos legisladores em tal sentido, tendo em vista o aumento dos dados disponíveis e a evolução do capitalismo movido a dados.

³³ Art. 20, L 13.709/2018. 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.

CAPÍTULO 2 – CONTRATAÇÃO AUTOMATIZADA. UTILIZAÇÃO DA DEFINIÇÃO DE PERFIS PARA ESCOLHA DA CONTRAPARTE CONTRATUAL.

Um contrato é um vínculo jurídico no qual as partes contratantes acordam cláusulas que criam, extinguem ou modificam um direito ou dever, entre uma ou mais partes interessadas.

A contratação automatizada surge quando todo, ou boa parte, do processo de elaboração e conclusão contratual se dá com a utilização de um algoritmo, o qual, após analisar os dados inseridos, os organiza e cataloga, verificando, ao final, se a contratação entre as partes interessadas é possível e desejável pela empresa.

A automatização do processo de contratação tem inúmeras vantagens do ponto de vista empresarial, posto que melhora a eficiência, agilidade e segurança dos dados, facilitando as negociações, transações e contratações da empresa. Nesse sentido, há uma otimização da produtividade empresarial, com uma diminuição dos custos em comparação à contratação individual.

Entretanto, se pelo lado empresarial a contratação automatizada é altamente vantajosa, do ponto de vista da contraparte contratual, qual seja o titular de dados, tal automatização pode ser prejudicial, a depender dos dados tratados e do nível de automatização do processamento e tomada de decisão.

Conforme já exposto, a automatização do tratamento de dados pode levar a decisões e a definições de perfis injustas, que perpetuam preconceitos e discriminações existentes na sociedade, além de poder ter como resultado inferências que não correspondem com a realidade. Assim se faz necessário saber o nível de automatização do processo de contratação, para se verificar a legalidade dentro dos padrões estipulados pela lei.

Ao analisar a automatização da contratação, tem-se que ela pode se dar em diversos níveis do processo de contratação, devendo-se sempre ter em mente as proibições e permissões sobre decisões individuais automatizadas decorrentes do Regulamento Geral de Proteção de Dados (artigo 22º).

Em um primeiro momento, a automatização pode se dar na fase de definição do perfil da possível contraparte contratual. O perfil pode ser definido com base em dados fornecidos pelo titular e/ou obtidos através de “*Big Data*”, e processados com análise do maior número de dados disponíveis, incluindo dados inseridos pela empresa e dados históricos e sociais. O perfil obtido será considerado apto, ou não, a contratar com a empresa responsável pelo tratamento.

Essa contratação pode ser determinada por um gestor, ou ser automatizada, sendo que, se automatizada, deve ser possível a obtenção de intervenção humana.

Conforme já analisado, a tomada de decisões com base em perfis definidos automaticamente por algoritmos, com a utilização de diversos bancos de dados, pode conter riscos (perpetuação de discriminações e preconceitos), sendo a intervenção humana ao final uma tentativa de diminuição de tais riscos.

Ainda, pode-se considerar automatizada uma contratação quando, a partir de perfis já definidos, de formulários preenchidos pelo titular ou de dados disponíveis, e levando em consideração critérios estabelecidos pela empresa, o algoritmo automaticamente decide pela contratação do titular de dados, não sendo necessário que o perfil seja definido automaticamente.

Em tais situações, surge os problemas relacionados ao processamento automatizado de dados por algoritmos que utilizam técnicas de “*Machine Learning*”, tendo em vista que a dificuldade em rastrear todos os dados utilizados e saber o motivo da decisão. Assim, mesmo com a solicitação de intervenção humana para revisão da decisão, o encarregado pela contratação pode não conseguir informar todas os dados utilizados para a decisão.

Ressalta-se que o processamento automatizado tende a perpetuar práticas históricas da empresa, podendo conter traços de discriminações e preconceitos que não são percebidos pelo encarregado pela contratação. Nesse sentido, podem ser deixados de fora perfis que, de acordo com os dados anteriores, não teriam histórico de contratação com a empresa, mas que na realidade fática seriam parte contratual desejada.

Ainda, no caso de não serem utilizados mecanismos de definição automatizada de perfis ou algoritmos para buscar o histórico do titular, a empresa acaba por não ter uma segurança na contratação, tendo em vista a inexistência de dados para prever o comportamento do titular.

Percebe-se que a maioria dos problemas da contratação automatizada são devidos à utilização de dados provenientes de diversos bancos de dados *on-line*, dados passados ou dados desatualizados no processamento automatizado, ou da utilização de algoritmos que tornam impossível saber os fundamentos utilizados na tomada da decisão.

Assim, uma forma de obstar os problemas apontados, sem tornar a contratação arriscada para nenhuma das partes, seria a permissão da utilização apenas de bancos de dados de órgãos públicos ou estabelecidos por lei no processamento automatizado utilizado para a definição do perfil. Ainda, deveriam ser utilizados algoritmos com critérios objetivamente estabelecidos pela

empresa como desejáveis para contratação, sem a realização de inferências em dados pessoais alheios ao contrato.

Em tais casos, não seriam investigados todos os aspectos da vida pessoal do titular de dados, mas somente os necessários para a realização do contrato em espécie. Dessa forma, a empresa teria uma segurança no perfil contratado e o titular de dados não teria sua esfera privada violada, tornando possível uma decisão automatizada objetiva, com menos chances de injustiças, preconceitos e discriminações.

Assim, por diminuir os riscos inerentes à automatização da decisão ou definição de perfis, respeitando os princípios da minimização de dados e limitação das finalidades, a solução apontada seria mais adequada ao disposto no RGPD.

Salienta-se que a utilização de dados sensíveis para tomada de decisões automatizadas é, em regra, proibida pelo regulamento, de forma que os dados utilizados devem ser apenas os objetivamente necessários para o contrato em espécie.

Conclui-se que o regulamento não veda toda forma de contratação automatizada, sendo permitida a utilização de mecanismos automatizados para definição de perfis a depender do caso concreto, devendo sempre ser observado o tipo de dado utilizado e o nível de automatização da decisão.

2.1. A Utilização Da Definição De Perfis Para Escolha Da Contraparte Contratual

Conforme já mencionado, cada vez se torna mais comum e necessária a utilização de perfis definidos de forma automatizada para escolha da contraparte contratual, valendo ressaltar que o perfil obtido constitui uma previsão do comportamento e da personalidade da pessoa.

Sendo uma previsão comportamental, baseada em comportamentos passados, o perfil definido de forma automatizada cai no campo da probabilidade, não sendo uma ciência precisa.

Vale ressaltar que, ao utilizar perfis definidos automaticamente para tomar decisões de forma automatizada, são utilizados dados passados tanto do titular, quanto da empresa, realizando correlações entre características do titular e características de pessoas que já contrataram com a empresa.

Assim, o algoritmo presume que pessoas com as mesmas características irão ter o mesmo comportamento contratual, razão pela qual perfis potencialmente melhores, mas com características de perfis que tiveram algum problema com a empresa, podem sequer serem analisados, por estarem no domínio das baixas probabilidades de contratação de sucesso.

Evidente que a utilização de perfis definidos com a utilização de algoritmos para escolha da contraparte contratual gera efeitos jurídicos na esfera privada do titular de dados, adentrando no âmbito de proteção do RGPD.

2.2 Responsabilidade Civil pela Contratação Automatizada no RGPD

O RGPD estabelece sanções para o responsável pelo tratamento que não cumpra as regras estabelecidas, valendo destacar o direito de indenização e responsabilidade civil do titular de dados³⁴.

O artigo 82 do RGPD, permite a responsabilização direta dos responsáveis pelo tratamento e dos subcontratantes por danos materiais ou imateriais, causados na esfera jurídica dos titulares de dados e na decorrência de qualquer violação do RGPD (MENEZES CORDEIRO, 2019, p. 778).

A legislação portuguesa^{35, 36}, em concordância com o regulamento, também confere ao titular de dados o direito à reparação pelos danos, patrimoniais ou não, decorrentes da violação das disposições referentes à proteção dos dados pessoais.

³⁴ Artigo 82º, RGPD: Direito de indemnização e responsabilidade. 1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. 2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. 3. O responsável pelo tratamento ou o subcontratante fica isento de responsabilidade nos termos do n.º 2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos. 4. Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.ºs 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados. 5. Quando tenha pago, em conformidade com o n.º 4, uma indemnização integral pelos danos sofridos, um responsável pelo tratamento ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com as condições previstas no n.º 2. 6. Os processos judiciais para exercer o direito de receber uma indemnização são apresentados perante os tribunais competentes nos termos do direito do Estado-Membro a que se refere o artigo 79.º, n.º 2

³⁵ Artigo 33º, Lei 58/2019: Artigo 33.º Responsabilidade civil: 1 — Qualquer pessoa que tenha sofrido um dano devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições do RGPD ou da lei nacional em matéria de proteção de dados pessoais, tem o direito de obter do responsável ou subcontratante a reparação pelo dano sofrido.

³⁶ Artigo 51º, Lei 59/2019. Direito de indemnização: Qualquer pessoa que tenha sofrido danos, patrimoniais ou não patrimoniais, causados por uma violação das disposições da presente lei tem direito a receber do responsável pelo tratamento ou de qualquer outra autoridade competente uma indemnização pelos danos sofridos, nos termos do regime da responsabilidade civil extracontratual do Estado e demais entidades públicas.

Quanto ao tipo de reparação obtida, o considerando 146 do RGPD estabelece regras de aplicação do artigo 82, devendo o conceito de dano ser interpretado em sentido *lato* à luz da jurisprudência do Tribunal de Justiça da União Europeia, os objetivos do RGPD plenamente respeitados e todos os danos ressarcidos, incluídos os materiais e os imateriais.

Insta informar que os diplomas legais em análise responsabilizam tanto os responsáveis pelo tratamento, como os subcontratantes. Nesse viés, os responsáveis pelo tratamento são responsabilizados sempre que estiverem envolvidos em algum tratamento que viole o RGPD (artigo 82º, nº 2, p. 1, RGPD). Já os subcontratantes, que são aqueles que tratam os dados pessoais por conta do responsável pelo tratamento (artigo 4º, nº 8, RGPD), são responsabilizados se não cumprirem as obrigações determinadas pelo regulamento, que lhes sejam especificadamente dirigidas, ou se não tiverem seguido as instruções lícitas do responsável pelo tratamento (artigo 82º, nº 2, p. 2, RGPD).

Somente no caso de provarem que não são, de modo algum, responsáveis pelo evento que deu origem aos danos, tais partes ficam isentas de responsabilidade (artigo 82º, nº 3, RGPD; artigo 33º, 2, L 58, 2019 de 8 de agosto).

Como exemplo de possíveis danos materiais reparáveis, em matéria de definição automatizada de perfis para escolha da contraparte contratual, podem se citar: (a) não celebração de um contrato de trabalho ou despedimento na decorrência da coleta ilícita de dados pessoais, pela entidade patronal, relativos ao candidato; (b) utilização ilícita de dados pessoais por entidades financeiras, com um impacto negativo nas condições apresentadas ao titular, por exemplo, nos juros cobrados (MENEZES CORDEIRO, 2019, p. 783).

Em relação aos danos imateriais, citam-se: a exposição pública não pretendida, a ansiedade e a discriminação daí decorrentes, a objetivação do ser humano enquanto mero dado, ou a inibição do desenvolvimento da personalidade (MENEZES CORDEIRO, 2019, p. 783).

Quanto a forma de indenização e quantificação da indenização, há que ser levado em conta o disposto no regulamento e na legislação de cada país, levando em consideração a especificidade do caso em concreto.

CAPÍTULO 3 – A UTILIZAÇÃO DA DEFINIÇÃO AUTOMATIZADA DE PERFIS NOS CONTRATOS DE TRABALHO

É crescente o número de empresas que utilizam algoritmos na relação laboral. Tal utilização se dá tanto na fase pré-contratual, para seleção curricular, como nas fases de manutenção do contrato, com a utilização de algoritmos inteligentes para a vigilância de funcionários, e de término da relação empregatícia, existindo algoritmos que automaticamente dispensam um funcionário que infringiu alguma norma da empresa. No presente trabalho, será dado enfoque à utilização de algoritmos na fase pré-contratual, sendo estudada a utilização da definição de perfis para escolha do empregado.

Ao realizar uma seleção curricular, o responsável pela contratação tenta obter o maior número de informações sobre os candidatos, objetivando contratar aquele que mais se enquadra no perfil desejado pela empresa. Assim, por meio dos dados obtidos, o recrutador tenta perceber se o candidato será produtivo, se irá se encaixar no ambiente de trabalho, o motivo pelo qual ele quer aquele emprego, entre outros (TODOLI-SIGNES, 2018, p. 2).

Até há pouco tempo, todas as empresas realizavam as contratações com base, apenas, nos currículos profissionais entregues e nas entrevistas realizadas com os candidatos. Ora, se para pequenas e médias empresas tal situação é viável, ao se tratar de grandes empresas, com um massivo número de currículos enviados, o processo de contratação passava a ser demasiadamente demorado.

Com as novas tecnologias disponíveis, as “*e-recruitment practices*” (práticas de recrutamento eletrônico) vem aumentando consideravelmente, sendo utilizados algoritmos para o processamento automatizado dos currículos, a definição automatizada de perfis, a utilização de “*Big data*”, entre outros, tornando o processo de contratação mais rápido, barato e eficiente.

Assim, o empregador determina algumas características e requisitos para a obtenção de um cargo disponível na empresa e as coloca em um algoritmo. Este, por sua vez, realiza correlações entre os currículos recebidos, os dados obtidos *on-line* e dados histórico-sociais, buscando o perfil que mais adequado para a empresa..

Em regra, os dados analisados ao definir os perfis são os relativos às características socioeconômicas (ex. idade, género), motivação para procurar ou aceitar o emprego (ex. forma de procura de emprego, expectativas de pagamento), adequação ao trabalho (ex. nível de educação, habilidades, limitações de saúde, responsabilidade) e oportunidades (ex. informação

sobre o mercado de trabalho regional), sendo ainda considerado o risco de o candidato permanecer desempregado por um longo tempo. (OECD, 2018, p. 2).

A partir do resultado do processamento algorítmico, pode haver uma contratação automática do perfil escolhido, ou podem ser enviados os perfis entendidos como mais adequados para o cargo disponível para análise de um responsável.

Como já frisado acima, sempre deve ser levado em consideração que as decisões provenientes de processamentos automatizados tendem a perpetuar os dados históricos e sociais, podendo resultar em decisões discriminatórias, injustas ou preconceituosas, com base em inferências não condizentes com a realidade.

Na relação laboral, alguns exemplos de discriminação podem ser: a) não contratação de mulheres, perpetuando dados históricos de contratação apenas de homens (se poucas mulheres foram contratadas anteriormente, os dados sobre empregadas mulheres serão menos confiáveis do que os dados sobre os homens – não havendo mulheres que já atingiram um cargo alto, o algoritmo pode entender que homens se enquadrariam melhor como diretores ou funcionários de tal estabelecimento). Pela mesma razão: não contratação de pessoas que moram em determinada região conhecida por ser um local onde existe um elevado índice de criminalidade (o algoritmo pode entender que os residentes de tal bairro têm uma tendência a cometer crimes, não sendo os perfis residentes naquele local, desejados para a empresa); não contratação de pessoas de determinada idade ou de determinada opinião política, sexual ou religiosa.

Percebe-se que, quanto mais dados sensíveis forem utilizados, e quanto mais detalhado for o perfil analisado, maiores são as chances de decisões discriminatórias. Em virtude disso, o Regulamento Geral de Proteção de Dados, tem como regra a proibição da utilização de dados sensíveis quando forem tomadas decisões automatizadas com base em definição de perfis (artigo 22º, número 4).

Assim, em regra, ao analisar um currículo, devem ser levados em consideração apenas fatores determinantes no quesito profissional, tais quais formação e experiência profissional, não devendo sequer serem colhidos dados relacionados a características físicas ou ideológicas.

Entretanto, existem situações nas quais as características físicas ou ideológicas podem ser determinantes para a empresa, de forma que a análise de determinados dados sensíveis se faz necessária. Como exemplo: clínicas estéticas que atendem exclusivamente mulheres, tendo o compromisso de ter somente esteticistas do sexo feminino; ou instituições religiosas que somente contratam fiéis que seguem a própria religião.

Nesse aspecto, sempre que o tratamento de dados sensíveis for necessário, devem ser observados os princípios da limitação das finalidades e da minimização dos dados, recolhendo e tratando apenas os dados necessários para a contratação em questão, visando a diminuição da possibilidade de se terem decisões injustas.

Vale ressaltar a importância de atualização periódica dos dados e do modelo algorítmico utilizados, em busca de minimizar as chances de perpetuação de discriminações passadas.

Destaca-se, ainda, o direito à obtenção de intervenção humana sempre que existir uma decisão automatizada, incluindo as definições de perfis (artigo 22, RGPD), sendo evidente que o regulamento proíbe a substituição total da parte de recursos humanos por algoritmos. Assim, é necessário que a empresa tenha ao menos um funcionário para decidir sobre a contratação ou não dos candidatos, ou para poder prestar informações relativas à decisão.

Ademais, tendo em vista o desequilíbrio existente na relação entre o candidato à vaga de emprego e o responsável pela contratação, o regulamento apenas permite a utilização da definição automatizada de perfis se for (a) necessária para a celebração ou a execução do contrato de trabalho ou (b) se for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, desde que previstas medidas adequadas para salvaguardar direitos e liberdades e os legítimos interesses do titular de dados (artigo 22º, número 2, alíneas “a” e “b”). Isto pois, o consentimento do titular não deve ser levado em consideração nos casos em que há um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento (considerando 43, RGPD).

Ainda, ao verificar a incidência da proibição do regulamento, importa saber em quais situações a contratação vai ser considerada automatizada, devendo ser observada a necessidade do procedimento automatizado e o grau de automatização da contratação.

Assim, primeiramente deve-se observar se a pessoa responsável pela contratação tem poder para influir na decisão obtida através do processamento de dados, podendo escolher contratar, ou não, a pessoa que o algoritmo determinou como mais adequada para a empresa. Dessa forma, para que uma decisão possa ser considerada como não tomada somente por processamento automatizado de dados, a pessoa responsável deve ter a opção de contratar a pessoa escolhida pelo algoritmo ou fazer sua própria seleção dentre os currículos enviados.

Há ainda casos em que, mesmo que a decisão final seja realizada por um funcionário, o algoritmo teve um papel fundamental na mesma, sem o qual a decisão não poderia ter sido tomada. Como exemplo, tem-se as empresas multinacionais que recebem milhares de currículos. Em tais casos, a automatização do tratamento pode ser considerada necessária, posto

que uma seleção realizada por um funcionário seria inviável. Assim, o algoritmo seria utilizado para realizar uma pré-seleção dentre os currículos recebidos, remanescendo uma quantia menor de currículos para o responsável pela contratação analisar e decidir pela contratação.

Faz-se válida a discussão sobre a necessidade de informar à lógica subjacente da decisão ao titular de dados (artigos 13º, nº 2, “f” e 14, nº 2, “g”, do RGPD) que não teve seu currículo selecionado pelo algoritmo, posto que tal decisão causou efeitos em sua esfera jurídica. Em tal ponto, deve ser analisado o direito do titular de obter intervenção humana por parte do responsável, manifestar seu ponto de vista e contestar a decisão.

Para que tais direitos sejam respeitados, seria necessário que o responsável pelo tratamento tivesse conhecimento dos critérios e requisitos utilizados pelo algoritmo para eliminar determinados currículos. Ocorre que no caso de algoritmos mais complexos, a determinação de todos os critérios utilizados fica mais difícil, tendo em vista a realização de correlações que, muitas vezes, não são passíveis de serem reconhecidas.

Por conta disso, se faz necessário que o responsável pela contratação, que irá prestar as informações solicitadas pelo titular de dados, seja alguém com formação adequada a perceber se, dentre os currículos finais obtidos, há alguma semelhança ou padrão que revele uma tendência do algoritmo a ter perpetuado uma discriminação.

Ainda, se faz necessário que o candidato à vaga de emprego possa saber quais dados pessoais foram utilizados no processamento automatizado, para poder contestar caso encontre algum dado desatualizado.

Por fim, saindo da esfera pré-contratual e passando à da vigência do contrato de trabalho, insta lembrar que o RGPD confere proteção apenas às pessoas singulares titulares de dados, não conferindo qualquer tipo de proteção para uma coletividade de indivíduos. Nesse sentido, o RGPD acaba por dificultar a atuação sindical, causando um *défict* na proteção do trabalhador.

Fato é que o trabalhador e o empregador estão em níveis desiguais do contrato de trabalho, sendo que a proteção sindical tende a proporcionar certo equilíbrio à relação contratual, de forma que muitos trabalhadores precisam do sindicato para efetivarem ou negociarem seus direitos.

O problema em análise advém do fato de que os sindicatos, por advogarem para uma coletividade, não podem negociar direitos conferidos pelo regulamento.

Ainda, ao focar apenas na proteção individual, o regulamento não confere aos sindicatos o poder para monitorar coletivamente o uso de dados pelos empregadores, o que acaba por enfraquecer o direito laboral e permitir o abuso de diversos empregadores.

Dessa forma, há a necessidade dos representantes dos trabalhadores e sindicatos terem poder não apenas para o exercício de alguns direitos em nome dos trabalhadores, mas também ter a possibilidade de verificar de dentro das empresas a forma que as informações dos trabalhadores são usadas, visando assegurar que as informações utilizadas nos processos de seleção, avaliação e demissão sejam obtidas de forma legal (TODOLI-SIGNES, 2018, p. 15).

Em conclusão, ao utilizar formas automatizadas de definição de perfil ou de contratação, as empresas devem atentar para a forma de coleta de dados, para o tipo de dados coletados e a forma da decisão tomada com base em tais dados, visando não perpetuar práticas discriminatórias, e sempre dando a oportunidade de o titular dos dados obter intervenção humana e ser informado sobre a lógica subjacente da decisão.

3.1 A Utilização de Decisões Automatizadas em Contratos de Trabalho pela Legislação Portuguesa

O artigo 88 do Regulamento Geral de Proteção de Dados³⁷, prevê a possibilidade de os Estados Membros estabelecerem normas específicas para garantir os direitos dos trabalhadores no que diz respeito ao tratamento de dados.

Já o artigo 22º, número 2, “b”, RGPD, autoriza decisões automatizadas, incluindo definições de perfis, nos casos em que o Estado-Membro a que o responsável pelo tratamento estiver sujeito as autorize, desde que previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados.

³⁷ Artigo 88, RGPD: 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho.

Com base em tais dispositivos, o artigo 28º da Lei 58/2019 de 8 de agosto³⁸, dispõe sobre o tratamento de dados nas Relações Laborais em Portugal, remetendo ao Código do Trabalho português (CTP - Lei nº 7/2009) e respectiva legislação complementar a definição das finalidades e limites para que o empregador possa realizar o tratamento de dados pessoais.

Ressalta-se que o número três do artigo em análise, expressamente retira do consentimento do trabalhador o requisito de legitimidade do tratamento dos seus dados pessoais se (a) do tratamento resultar uma vantagem jurídica ou econômica para o trabalhador, ou, (b) se o tratamento for necessário para a execução do contrato.

Quanto à hipótese do nº 3, alínea “a”, do artigo 28º da Lei 58/2019, é importante mencionar que a Comissão Nacional de Proteção de Dados, em sua Deliberação 2019/494, p. 5v, entendeu ser uma “restrição não adequada, desnecessária e excessiva do direito fundamental à autodeterminação informacional ou à proteção dos dados enquanto direito ao controlo dos seus próprios dados, para lá do que é necessário à salvaguarda dos direitos e interesses dos trabalhadores”, que restringe o âmbito de aplicação da alínea “a” do nº 1 artigo 6º e da alínea “a” do nº 2 do artigo 9º do Regulamento Geral de Proteção de Dados, eliminando o livre arbítrio do trabalhador. Assim, optou por desaplicar a referida alínea.

Ressalta-se que, conforme abordado, o Regulamento Geral de Proteção de Dados determina que, no caso de decisões automatizadas, incluindo a definição de perfis, o consentimento não deve ser considerado fundamento de validade para o tratamento de dados em caso de desequilíbrio entre as partes.

Sendo certo que no contrato laboral há uma desigualdade entre as partes, somente pode haver uma automatização da decisão que utilize dados pessoais do candidato ou empregado quando houver outro fundamento que torne lícito o tratamento.

³⁸ Artigo 28.º Relações laborais 1 — O empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo. 2 — O número anterior abrange igualmente o tratamento efetuado por subcontratante ou contabilista certificado em nome do empregador, para fins de gestão das relações laborais, desde que realizado ao abrigo de um contrato de prestação de serviços e sujeito a iguais garantias de sigilo. 3 — Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou b) Se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do artigo 6.º do RGPD. 4 — As imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância, nos termos previstos no artigo 20.º do Código do Trabalho, só podem ser utilizados no âmbito do processo penal. 5 — Nos casos previstos no número anterior, as imagens gravadas e outros dados pessoais podem também ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal. 6 — O tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados.

Faz-se oportuna a análise dos dispositivos relativos à proteção dos dados dos trabalhadores inseridos no Código do Trabalho.

Primeiramente, o artigo 17º, CTP, informa os direitos dos candidatos a emprego ou trabalhadores em relação à proteção de dados pessoais no que se refere a reserva da intimidade da vida privada e à saúde ou estado de gravidez³⁹.

O número 1 do referido artigo estabelece que, via de regra, o empregador não pode exigir informações relativas à vida privada do candidato a emprego ou empregador, a não ser nos casos em que tal informação seja relevante e necessária para o contrato de trabalho em concreto. Percebe-se que a proteção conferida pelo artigo se dá não apenas aos já empregados da empresa, mas também aos candidatos à vaga de emprego.

A tutela conferida pelo CTP “se estende da proteção de dados, em sentido estrito, à recolha da informação” (REDINHA, 2015, p. 9), sendo “irrelevante o método ou o processo de recolha das informações ou o tratamento dispensado aos dados” (REDINHA, 2015, p. 9).

Ainda, tem-se em tal dispositivo a concordância com os princípios gerais da proporcionalidade, necessidade e adequação, somente podendo ser tratados os dados “necessários e relevantes” para que seja avaliada a adequação do candidato ou empregado ao trabalho no caso concreto.

Nesse passo, para poderem ser tratados, os dados devem ser apropriados, importantes e relativos às finalidades previamente estabelecidas, percebendo-se a concordância com os princípios da minimização e da finalidade dos dados pessoais, dispostos no RGPD e na legislação portuguesa.

Por sua vez, o nº 3 do art.º 17, do CTP, estabelece o direito de controle, retificação e atualização dos dados pessoais por parte do trabalhador, assim como o direito de conhecer a finalidade do tratamento, reafirmando os direitos conferidos pelo RGPD e pela LPDP. Ressalte-se que tal dispositivo permite que o trabalhador controle os dados que fornece ao empregador,

³⁹ Artigo 17.º, CTP: <rotecção de dados pessoais: 1 - O empregador não pode exigir a candidato a emprego ou a trabalhador que preste informações relativas: a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação; b) À sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação. 2 - As informações previstas na alínea b) do número anterior são prestadas a médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a actividade. 3 - O candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respectivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua rectificação e actualização. 4 - Os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à protecção de dados pessoais. 5 - Constitui contra-ordenação muito grave a violação do disposto nos n.os 1 ou 2.

podendo exigir sua retificação e atualização, reafirmando o disposto pelos artigos 13 a 17 do RGPD e da lei 59/2019.

Ainda, o Código de Trabalho trata dos dados biométricos⁴⁰ dos trabalhadores no artigo 18^{o41}, proibindo, em regra, o tratamento de tal categoria de dados.

Ressalta-se que, quando permitido, os dados biométricos somente podem ser armazenados durante a vigência do contrato de trabalho entre o trabalhador e a empresa (nº 3).

Não há no Código do Trabalho uma proteção direta contra decisões automatizadas, incluindo a definição de perfis, sendo as disposições do CTP voltadas aos tipos de dados fornecidos para o tratamento. Assim, no que diz respeito à automatização das decisões, deve-se observar o disposto no âmbito geral, indo às leis 58 e 59 de 8 de agosto de 2019, e ao Regulamento Geral de Proteção de Dados.

⁴⁰ Dados biométricos são aqueles “recolhidos através de sistemas que se baseiam na análise e mensuração de dados biológicos em comparação com uma amostra digital (template), baseados, por hipótese, em impressões digitais, da retina e íris, da geometria das mãos, voz, etc” (REDINHA, 2015, p. 14).

⁴¹ Artigo 18.º, CTP: Dados biométricos: 1 - O empregador só pode tratar dados biométricos do trabalhador após notificação à Comissão Nacional de Protecção de Dados. 2 - O tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objectivos a atingir. 3 - Os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho. 4 - A notificação a que se refere o n.º 1 deve ser acompanhada de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer. 5 - Constitui contra-ordenação grave a violação do disposto no n.º 3.

CAPÍTULO 4 – POSSÍVEIS SOLUÇÕES PARA OS PROBLEMAS APRESENTADOS

Os principais problemas relacionados ao tratamento automatizado de dados, incluindo a definição de perfis, são a propagação de discriminações e preconceitos existentes na sociedade, e a possibilidade de serem realizadas falsas inferências, levando a decisões injustas, não condizentes com a pessoa analisada, e que acabam por interferir negativamente na esfera privada do titular de dados.

Ambos os problemas resultam do fato de que os algoritmos, ao processarem os dados disponíveis, realizam uma análise estatística/probabilística, categorizando os dados de acordo com ocorrências anteriores similares.

Assim, os algoritmos trabalham com uma espécie de “probabilidade datal”, categorizando os titulares de dados com o objetivo de prever o comportamento futuro deles.

Tendo em vista que os problemas apontados decorrem das correlações realizadas entre os dados disponíveis, podem ser dadas algumas soluções para tentar minimizá-los.

Primeiramente, pode-se chamar a atenção para a atualização dos dados que serão objeto de tratamento. Para tanto, se faz necessária a atualização periódica dos dados utilizados, posto que, quanto mais atuais, menor a chance de refletirem comportamentos indesejados que ocorreram no passado. Assim, deve-se ter o cuidado de sempre atualizar o banco de dados em que realizarão as inferências, não devendo ser permitido o tratamento com base em dados antigos.

Ainda, é de suma importância observar a qualidade e o tipo dos dados analisados. Dessa forma, quando necessária a utilização de bancos de dados, deve-se atentar para a procedência dos dados disponíveis, vez que existem muitos dados falsos disponíveis *on-line*. Conforme dito anteriormente, o ideal seria a utilização apenas de bancos de dados governamentais ou de origem legal.

Quanto ao tipo dos dados analisados, o ideal é que não sejam utilizados dados sensíveis, e que, quando necessário o processamento de dados de categorias especiais, se observem os princípios da minimização de dados e limitação das finalidades.

Outro item importante para a solução dessa problemática, seria o desenvolvimento de algoritmos que deixem marcas ao realizar inferências, de forma que seja possível saber exatamente quais dados foram utilizados para chegar à decisão, tornando o princípio da transparência mais fácil de ser aplicado.

Frisa-se, ainda, a importância de o titular de dados poder fazer parte do processo de decisão automatizada, incluindo a definição de perfil. Nesse cenário, o ideal seria que, sempre que fossem utilizados dados pessoais de um indivíduo, ele fosse notificado, para que, querendo, pudesse saber quais dados foram utilizados para que determinada decisão. Dessa forma, no caso de alguma decisão ser tomada com base em dados que não foram consentidos, desatualizados, ou que não foram necessários para a decisão em concreto, o indivíduo poderia questionar a decisão, minimizando os efeitos negativos do tratamento automatizado.

Evidente que a intervenção do titular dos dados no tratamento automatizado reforça o controle que ele deve exercer sobre os seus dados, freando as vicissitudes que possibilitaram que o estágio atual da economia movida a dados se consolidasse (FRAZÃO, 2019, p. 31).

Visando uma maior proteção dos titulares de dados e diante das possíveis soluções apresentadas para os problemas expostos, não se pode descartar a possibilidade do legislativo aprimorar as normas já existentes com a criação de projetos que coadunam com as soluções específicas sugeridas no presente trabalho.

É sabido que, quanto maior a proteção legal, maiores são os entraves para os desenvolvedores de algoritmos e para as empresas que precisam utilizar dados disponíveis *on-line*.

Contudo, há de ser levado em consideração que os dados pessoais são informações que revelam a vida privada dos titulares de dados, de forma que, sempre que for necessário o tratamento de dados, deve-se atentar para os princípios da proteção da intimidade, da vida privada e da dignidade da pessoa humana, evitando que os dados que o titular não têm interesse em revelar, continuem sob sigilo, em sua esfera privada.

CONCLUSÃO

O aumento na quantidade de dados disponíveis, juntamente com o avanço tecnológico, gerou uma enorme mudança na sociedade, que passou a valorizar economicamente os dados pessoais dos cidadãos.

Com a supervalorização e comercialização dos dados pessoais, paulatinamente foram desenvolvidos algoritmos cada vez mais rápidos e eficientes, que conseguem processar automaticamente, e sem intervenção humana, uma vasta quantidade de dados provenientes não somente de informações obtidas pela empresa, mas também de diversos sítios e bancos de dados *on-line*.

Porém, esse desenvolvimento tecnológico acabou por priorizar a monetarização do tratamento de dados face aos direitos à privacidade e individualidade dos titulares, de forma que houve um enorme aumento na captura e armazenamento de dados. Assim, passaram a ser realizados tratamentos sobre todos os tipos de dados, muitas vezes sem o titular sequer ter o conhecimento de que seus dados haviam sido coletados e disponibilizados.

Ainda, percebeu-se um problema na tomada de decisões de forma automatizada. Isto pois, o processo de tomada de decisão algorítmica consiste na realização de inferências e previsões com os dados disponíveis, podendo resultar em julgamentos equivocados ou que reproduzam preconceitos, desigualdades e discriminações.

Com o aumento da utilização da definição automatizada de perfis para tomadas de decisões, passou-se a perceber que as categorias para as quais os indivíduos são “catalogados” passaram a definir quem é e quem será cada cidadão, evidenciando-se que os dados pessoais, ao mesmo tempo que representam a pessoa, servem para regulá-la (CHENEY-LIPPOLD, 2017, p. 14-19).

No que diz respeito à definição automatizada de perfis, deve ser levado em conta que as decisões decorrentes da realização do perfil tendem a determinar o destino do titular, principalmente no que diz respeito ao acesso do mesmo a direitos e oportunidades. Como exemplo, foi analisada a utilização da definição de perfis para a escolha da contraparte contratual, mormente em se tratando dos contratos de trabalhos.

Nessa análise, observou-se que os maiores problemas do tratamento automatizado de dados pessoais, incluindo a definição de perfis, residem nos seguintes pontos: a) utilização de dados antigos para a tomada de decisão ou definição do perfil (nesse ponto vale destacar que os dados antigos utilizados dizem respeito tanto aos do titular de dados quanto aos dados

histórico-sociais, ou empresariais, utilizados pelo algoritmo para realizar as inferências e predições); b) utilização de dados desnecessários para o caso em concreto (ex. Análise do estado de gravidez de uma pessoa para uma vaga que não diz respeito a tal fato); c) utilização de algoritmos que não permitem o rastreio dos dados utilizados para tomada da decisão; d) falta de transparência; e) ausência de intervenção humana; e f) ausência da possibilidade de o titular dos dados realizar a revisão da decisão ou do perfil.

Ademais, na tentativa de combater o uso indiscriminado de dados pessoais e os prejuízos causados aos titulares de dados com o tratamento deles de forma equivocada, passaram a ser desenvolvidos regulamentos e legislações com limitações e regras para a realização da colheita, armazenamento e tratamento de dados pessoais.

Foram abordadas as disposições consideradas mais importantes na questão da tomada de decisões de forma automatizada, incluindo a definição de perfis, dadas pelo Regulamento Geral de Proteção de Dados e pelas legislações nacionais portuguesa (leis 58 e 59 de 8 de agosto de 2019) e brasileira (lei 13.709 de 14 de agosto de 2018), constatando-se que as normas atuais, apesar de representarem um enorme avanço no combate da colheita e tratamento indiscriminados de dados pessoais, trazendo inúmeras disposições protetivas dos titulares de dados, deixaram de lado diversos pontos importantes, como a defesa de dados de uma coletividade, e o lapso temporal para utilização dos dados colhidos.

Certamente que quanto mais direitos são conferidos aos titulares de dados, maior a dificuldade das grandes empresas em utilizar os dados obtidos de forma a obter o desenvolvimento econômico almejado.

Todavia, o que deve ser levado em consideração é a vulnerabilidade dos titulares de dados face aos responsáveis pelo tratamento. Isto pois, são estes quem dispõem das ferramentas que irão realizar a colheita e o tratamento dos dados, podendo facilmente manipulá-los ou utilizá-los de uma forma que acabam por prejudicar os indivíduos, principalmente os que se encontram nos grupos minoritários da sociedade.

Vale frisar que a utilização prejudicial pode se dar tão somente por descuido na inserção dos dados ou pela ausência de atualização dos algorítmicos, porém, pode gerar enormes consequências na esfera jurídica do indivíduo, que pode deixar de conseguir um emprego, um financiamento ou até um plano de saúde em decorrência da utilização de seus dados pessoais de forma equivocada.

Desde modo, para que sejam minimizadas as consequências negativas do tratamento automatizado dos dados pessoais, foram apresentadas na presente dissertação, tanto aos

legisladores, quanto às empresas e aos titulares de dados, possíveis soluções na tentativa de resolver os problemas apontados.

Não há dúvidas de que os operadores do direito devem direcionar sua atenção para a tutela da privacidade, protegendo os indivíduos da coleta e tratamento indevido de seus dados pessoais.

Como dizia Rodotà (2008), citado por Frazão (2019, p. 49), “a forte proteção dos dados pessoais continuam a ser uma “utopia necessária” se se deseja garantir a natureza democrática de nossos sistemas políticos”, sendo evidente a necessidade de se assegurar a proteção dos dados pessoais para garantir a preservação de direitos inerentes à dignidade da pessoa humana.

BIBLIOGRAFIA

BIONI, BRUNO R.; MENDES, LAURA SCHERTEL (2019) – Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: Mapeando convergências na direção de um nível de equivalência. Em: FRAZÃO, ANA.; TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978-85-5321-663-5. p. 797-820.

BRKAN, MAJA (2017) - *Do algorithms rule the world? Algorithmic decision-making in the framework of the gdpr and beyond*. Maastricht: Maastricht University - Faculty of Law, 2017. [consult. 05 Out. 2020]. Disponível em: <https://ssrn.com/abstract=3124901>.

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

Orientações sobre recolha dos dados de saúde dos alunos. Comissão Nacional De Protecção De Dados. Lisboa, 19 de maio de 2020. [consult. 05 Out. 2020]. Disponível em: https://www.cnpd.pt/home/orientacoes/Orientacoes_medicao_temperatura_estabelecimentos_ensino.pdf.

CORDEIRO, A. BARRETO MENEZES (2019) - Repercussões do RGPD sobre a responsabilidade civil. Em: FRAZÃO, ANA.; TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. Thomson Reuters Brasil. São Paulo: 2019. ISBN 978-85-5321-663-5. p. 777-795.

CONSTITUIÇÃO da República Portuguesa. Diário da República n.º 86/1976, Série I de 1976-04-10. Assembleia constituinte.

DELIBERAÇÃO/2019/494. Aprovada na reunião de 3 de setembro de 2019. Comissão Nacional De Protecção De Dados (2019).

- DE STEFANO, VALERIO. (2018) - 'Negotiating the algorithm': Automation, artificial intelligence and labour protection. *Comparative Labor Law & Policy Journal*. Vol. 41. Nº. 1. [consult. 05 Out. 2020]. Disponível em: <https://ssrn.com/abstract=3178233>
- DIRETIVA 95/46/CE do Parlamento Europeu e do Conselho da União Europeia, de 24 de outubro de 1995.
- Tackling long-term unemployment through risk profiling and outreach: A discussion paper from the Employment Thematic Network. Directorate general for employment, social affairs and inclusion. Technical Dossier no. 6. European Union. 2018.
- EDWARDS, LILIAN.; VEALE, MICHAEL. (2017) - *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. *Duke Law & Technology Review* [consult. 05 Out. 2020]. Disponível em: <https://ssrn.com/abstract=2972855>.
- FRAZAO, ANA (2017) - *Dados, estatísticas e algoritmos. Perspectivas e riscos da sua crescente utilização*. Jota, 2017. [consult. 05 Out. 2020]. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017>
- FRAZÃO, ANA (2019) – Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. Em: FRAZÃO, ANA.; TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. Thomson Reuters Brasil. São Paulo: 2019. ISBN 978-85-5321-663-5. ISBN 978-85-5321-663-5. p. 23-52.
- GUIMARÃES, MARIA RAQUEL; REDINHA, MARIA REGINA - Through the Keyhole: Privacy in COVID-19 times - A Portuguese approach. Intersentia Online. 2020. [consult. 13 Out. 2020]. Disponível em: <https://www.intersentiaonline.com/publication/coronavirus-and-the-law-in-europe/720?version=v-544bf2be-8004-f72f-8088-dea754a9a0da>.

- HILDEBRANDT, MIREILLE (2008) - *Defining profiling: A new type of knowledge?*. In: HILDEBRANDT, MIREILLE; GUTWIRTH, SERGE (eds). *Profiling the European Citizen*. Dordrecht: Springer, 2008. [consult. 05 Out. 2020]. Disponível em: https://doi.org/10.1007/978-1-4020-6914-7_2.
- KAMARINOU, DIMITRA.; MILLARD, CHRISTOPHER; SINGHT, JATINDER (2016) - *Machine Learning with personal data*. Legal Studies Research Paper 247/2016. London: Queen Mary University of London, School of Law.
- KIM, PAULINE KIM (2019) - *Big Data and artificial intelligence: New challenges for workplace equality*. Vol 57. Louisville: Forthcoming University of Louisville Law Review. [consult. 05 Out. 2020]. Disponível em: <https://ssrn.com/abstract=3296521>.
- LEI 7/2009, de 12 de fevereiro. Código do Trabalho. Diário da República n.º 30/2009, Série I de 2009-02-12.
- LEI 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Edição: 157, Seção: 1, Página: 59. Publicado em: 15/08/2018. Atos do Poder Legislativo.
- LEI 58/2019, de 8 de agosto. Diário da República n.º 151/2019, Série I de 2019-08-08. Assembleia da República
- LEI 59/2019, de 8 de agosto. Diário da República n.º 151/2019, Série I de 2019-08-08. Assembleia da República
- MENDOZA, ISAK; BYGRAVE, LEE A. (2017) - *The right not to be subject to automated decisions based on profiling*. EU Internet Law: Regulation and Enforcement. Oslo: University of Oslo, Faculty of Law. Research Paper no 2017-20. [consult. 05 Out. 2020]. Disponível em: <https://ssrn.com/abstract=2964855>.

OECD (2018) - “*Profiling tools for early identification of jobseekers who need extra support*”, Policy Brief on Activation Policies. Paris: OECD Publishing.

Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. WP 248 rev.01. Grupo de trabalho do artigo 29º para a proteção de dados. Revistas e adotadas pela última vez em 4 de outubro de 2017. [consult. 05 Out. 2020]. Disponível em: https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

Orientações relativas ao consentimento na aceção do regulamento (UE) 2016/679. Grupo de trabalho do artigo 29º para a proteção de dados. WP259 rev.01. Última redação revista e adotada em 10 de abril de 2018. [consult. 05 Out. 2020]. Disponível em: https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf

Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679. Grupo de trabalho do artigo 29º para a proteção de dados. WP 250 rev. 01. [consult. 05 Out. 2020]. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

REDINHA, MARIA REGINA (2015) - *Da protecção da personalidade no Código do Trabalho*. Em: LEITE, JORGE. *Escritos Jurídico-Laborais*. Coimbra: Coimbra Editora, 2015.

REGULAMENTO (UE) 2016/679 do Parlamento e do Conselho da União Europeia, de 27 de abril de 2016.

RUCKER, DANIEL; KUGLER, TOBIAS. (2018) - *New European general data protection regulation, a practitioner's guide: ensuring compliant corporate practice*. 1st ed. Baden-Baden: Nomos Verlagsgesellschaft, 2018. ISBN 978-3-8487-3262-3.

TERRA, ALINE DE MIRANDA VALVERD; MULHOLLAND, CAITLIN (2019) - A utilização econômica de rastreadores e identificadores on-line de dados pessoais. Em: FRAZÃO, ANA.;

TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. Thomson Reuters Brasil. São Paulo: 2019. ISBN 978-85-5321-663-5. p. 601-619.

TODOLÍ-SIGNES, ADRIAN (2018) - *Algorithms, artificial intelligence and automated decisions about workers and the risks of discrimination: The necessary collective governance of data protection*. Transfer: European Review of Labour and Research, p. 25. [consult. 05 Out. 2020]. Disponível em: <http://dx.doi.org/10.2139/ssrn.3316666>

VERONESE, ALEXANDRE (2019) - Os Direitos de explicação e de oposição frente às decisões automatizadas: comparando o RGPD da união europeia com a LGPD brasileira. Em: FRAZÃO, ANA.; TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. Thomson Reuters Brasil. São Paulo: 2019. ISBN 978-85-5321-663-5. p. 385-415.

XAVIER, LUCIANA PEDROSO; XAVIER, MARÍLIA PEDROSO; SPALER, MAYARA GUIBOR (2019) - Primeiras impressões sobre o tratamento de dados pessoais nas hipóteses de interesse público e execução de contratos. Em: FRAZÃO, ANA.; TEPEDINO, GUSTAVO.; OLIVA, MILENA DONATO. *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. 1ª ed. Thomson Reuters Brasil. São Paulo: 2019. ISBN 978-85-5321-663-5. p. 485-503.