O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas

Francisca Cardoso Resende Gomes[*]

Resumo: Graças a uma evolução tecnológica galopante, vivemos num mundo computacional omnipresente potenciador de fenómenos analíticos de tratamento e processamento de dados assentes na utilização de algoritmos, como o *Big Data* e o *data mining*. O seu funcionamento permite a criação de nova informação respeitante ao perfil dos cidadãos, caracterizada por se traduzir em inferências de valor altamente imprevísivel e com uma taxa relativamente baixa de verificabilidade, num contributo para a perda de controlo de que os cidadãos atualmente padecem sobre a sua identidade e a forma como são percecionados pelos outros. Como iremos demonstrar ao longo deste artigo, o atual direito fundamental à proteção de dados emerge como um mecanismo com potencialidade para assegurar uma proteção compreensiva a nível constitucional. Impõe-se, todavia, uma reconfiguração deste direito fundamental, no sentido de enquadrar, do ponto de vista interpretativo, uma nova manifestação de tutela subjetiva, apelidada de direito a inferências razoáveis.

Palavras-chave: *direito fundamental à proteção de dados, Big Data, inferências, decisões automatizadas, direito a inferências razoáveis.*

Abstract: Due to a rampant technological evolution, we live in a ubiquitous computational world that promotes analytical phenomena of data processing based on the use of algorithms, such as Big Data and data mining. Its operation allows for the creation of new information regarding the citizens' profile, characterised by being translated into

[*] Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa (FDUL). Frequenta o *LL.M. in Commercial and Corporate Law* na *Queen Mary University of London*, onde realizou o módulo de *European Data Protection Law*. Este *paper* foi originalmente concebido como um trabalho para avaliação final à cadeira de Direitos Fundamentais sob a regência do Professor Doutor Jorge Reis Novais e orientação do Mestre Tiago Fidalgo de Freitas, a quem se agradece pelos profícuos contributos prestados.

inferences of highly unpredictable value and with a relatively low rate of verifiability, which contributes to the loss of control that citizens currently suffer over their identity and how they are perceived by others. As we will demonstrate throughout this article, the current fundamental right to data protection emerges as a mechanism with the potential to ensure a comprehensive protection at constitutional level. However, it is necessary to reconfigure this fundamental right, in order to frame, from an interpretative point of view, a new manifestation of subjective protection, known as right to reasonable inferences.

Keywords: *fundamental right to data protection, Big Data, inferences, automated decisions, right to reasonable inferences.*

Introdução

Ao consagrar o art. 35.º, a Constituição da República Portuguesa (doravante "CRP") apresentou-se como pioneira na proteção constitucional dos cidadãos perante o tratamento de dados pessoais informatizados, procedendo ao reconhecimento e garantia daquilo que a doutrina portuguesa, por inspiração germânica, veio a designar de "direito à autodeterminação informacional ou informativa"[1].

O direito à proteção de dados não foi, porém, criado num universo cibernético como o de hoje, que comporta a vivência em rede, a socialização eletrónica e a proliferação informativa em redes abertas, tendo-se assistido recentemente a uma modificação da realidade constitucional propiciada pelas novas tecnologias de informação e comunicação.

Mudou, desde logo, a envolvente em que os dados pessoais são recolhidos, processados e utilizados. Fruto de uma galopante evolução

---

[1] Entre outros, CALVÃO, Filipa Urbano, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", in *Jornadas nos quarenta anos da Constituição da República Portuguesa*, Almedina, 2017, p. 85; CANOTILHO, José Gomes e MOREIRA, Vital, *Constituição da República Portuguesa – Anotada*, Vol. I, 4.ª ed. revista, Coimbra Editora, 2007, p. 551; CASTRO, Catarina Sarmento e, «40 anos de "Utilização da Informática": O artigo 35.º da Constituição da República Portuguesa», *e-Pública*, vol. 3, n.º 3, 2016, p. 84-99. Disponível em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2183-184X2016000300004&lng=pt&nrm=iso. Acedido a: 12.10.2019; FARIA, Paula Ribeiro de, "Anotação ao Artigo 35.º da Constituição", in MIRANDA, Jorge e MEDEIROS, Rui (orgs.), *Constituição da República Portuguesa Anotada,* Tomo I, 2.ª edição, Coimbra Editora, 2010, p. 785.

tecnológica, assistiu-se ao aparecimento de instrumentos de tratamento da informação pessoal distintos dos tradicionais ficheiros eletrónicos, com destaque para as redes sociais, os sistemas de vigilância e, mais recentemente, a Internet das Coisas (fenómeno também conhecido como IoT). Tornam-se percetíveis os desafios colocados a este direito fundamental face à consideração de que, hoje, a recolha, transmissão e conservação de informação é realizada através de dispositivos eletrónicos incorporados em objetos do quotidiano, como os relógios, os automóveis, os eletrodomésticos e as televisões[2].

É graças a este mundo computacional omnipresente que se assiste à acumulação de um volume crescente e diversificado de informação, instantaneamente recolhida e partilhada, que surge como potenciadora de fenómenos como o *Big Data* e o *data mining*. Trata-se da criação de nova informação, consubstanciada em juízos de probabilidades, inferências e previsões respeitantes ao perfil e padrão de comportamento dos cidadãos, como resultado da utilização de algoritmos no relacionamento e análise dos dados pessoais recolhidos nestes novos contextos tecnológicos. A título exemplificativo, pense-se na capacidade demonstrada pelo Facebook para inferir a orientação sexual, a raça e as convicções políticas dos seus utilizadores[3]. Daqui resultam inferências assentes numa taxa relativamente baixa de verificabilidade, porque revestidas de um valor preditivo e contraintuitivo, a que acresce o seu caráter imprevisível igualmente contribuidor para a emergência das preocupações aqui tratadas relativas ao controlo e responsabilização algorítmica.

A urgência da abordagem teórico-prática desta temática é salientada pela consideração de que esta nova existência cibernética tem como pano de fundo uma mudança dos interesses públicos e privados, traduzida na afirmação de objetivos de eficiência na gestão das empresas e dos organismos públicos. Este ambiente promotor do recurso à inteligência

---

[2] Sobre esta temática, veja-se ANTUNES, Luís Filipe, "A privacidade no mundo conectado da Internet das Coisas", *Fórum de Proteção de Dados*, n.º 2, 2016, pp. 52-58. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-I.html#. Acedido a: 12.10.2019.

[3] Veja-se, a este propósito, CABANÃS, José González, CUEVAS, Ángel e CUEVAS, Rúben, "Facebook Use of Sensitive Data for Advertising in Europe", *CoRR*, 2018. Disponível em: http://arxiv.org/abs/1802.05030. Acedido a: 11.10.2019.

artificial e aos fenómenos analíticos descritos anteriormente não constitui ficção científica em Portugal, atento o recente investimento na sua implementação em vários setores da Administração Pública[4].

Neste seguimento, este artigo pretende refletir sobre a questão de saber se o conteúdo do direito à proteção de dados não deverá ser alvo de uma atualização no plano constitucional considerando as especificidades traduzidas pelas decisões automatizadas, pois como Tene/Polonetsky referem "In a big data world, what calls for scrutiny is often not the accuracy of the raw data but rather the accuracy of the inferences drawn from the data"[5].

1. Da jusfundamentalidade do direito à proteção de dados

Desde o seu texto originário, aprovado em 1976, que a CRP integra um preceito com a epígrafe "Utilização da informática", tendo sido, assim, pioneira na consagração constitucional de direitos que especificamente protegem os dados pessoais dos cidadãos em relação ao uso das novas tecnologias[6]. Ao consagrar o art. 35.º, a CRP veio conceder expressa autonomia constitucional a um direito do indivíduo à autodeterminação informativa, distinguindo-o da tutela constitucional concedida à reserva da intimidade da vida privada e familiar protegida no âmbito do art. 26.º

---

[4] cfr. Iniciativa Nacional Competências Digitais (INCoDe.2030), *AI Portugal 2030 – An innovation and growth strategy to foster Artificial Intelligence in Portugal in the European context*, 2019. Disponível em https://www.incode2030.gov.pt/sites/default/files/draft_ai_portugal_2030v_18mar2019.pdf. Acedido a: 14.10.19.

[5] TENE, Omer e POLONETSKY, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics", Northwestern Journal of Technology and Intellectual Property, Vol. XI, n.º 5, 2013, p. 270. Disponível em https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/. Acedido a: 11.10.2019.

[6] Neste sentido, LOPES, Joaquim Seabra, "O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível", *Fórum de Proteção de Dados*, n.º 2, 2016, pp. 15-49. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2016_2/files/assets/basic-html/page-I.html#. Acedido a: 9.05.2020. Porém, o Autor não deixa de referir que, embora o art. 35.º tenha sido introduzido na Constituição originária de 1976, o seu conteúdo atual resulta, em grande medida, da quarta revisão constitucional, ocorrida em 1997, e que visou compatibilizar o dispositivo com o que se preceituava na Diretiva n.º 95/46/CE.

da CRP, e à autodeterminação comunicativa protegida no contexto do art. 34.º da CRP.

Esta autonomia dogmática é ostensivamente tratada pelo Tribunal Constitucional nos Acórdãos n.º 213/2008 e n.º 403/2015, nos quais nos dá conta, em primeiro lugar, da capacidade da CRP para antecipar a imprescindibilidade de uma dicotomia protecional entre reserva da intimidade da vida privada e proteção de dados pessoais, ao promover uma proteção diferenciada, que apenas mais tarde viria a ser reconhecida pela Carta dos Direitos Fundamentais da União Europeia sob a égide dos arts. 7.º e 8.º, reiterando que "... esta proibição [do n.º 4 do art. 35.º] não impede o acesso apenas a dados íntimos de uma pessoa, mas a todos os dados a ela relativos, mesmo que em nada afetem a sua privacidade."[7]; e, em segundo lugar, da distinção entre autodeterminação comunicativa e autodeterminação informativa, afirmando que "O objeto de proteção do direito à autodeterminação comunicativa reporta-se a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo de comunicações. Naquele outro direito [direito à proteção de dados] protege-se as informações pessoais recolhidas e tratadas por entidades públicas e privadas, cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito."[8].

O direito à proteção de dados é composto pelo conjunto de direitos aos quais é reconhecida expressa dignidade constitucional nos demais números do art. 35.º da CRP, entre eles o direito de acesso aos tratamentos de dados pessoais para conhecimento dos dados que lhe pertencem, o direito à retificação dos dados, o direito à atualização dos dados, o direito a conhecer a finalidade dos tratamentos de dados (n.º 1), assim como o direito ao não tratamento de dados cujo processamento se possa revelar especialmente sensível e o direito à não divulgação de dados objeto de tratamento no sentido de proibição do acesso de dados por terceiros (n.º 3).

Neste seguimento, o conteúdo essencial do moderno direito à proteção de dados demonstra tratar-se de um direito fundamental com uma

---

[7] Acórdão do Tribunal Constitucional n.º 213/2008, *Diário da República* n.º 86/2008, Série II de 2008-05-05, p. 19994.

[8] Acórdão do Tribunal Constitucional n.º 403/2015, *Diário da República* n.º 182/2015, Série I de 2015-09-17, pp. 8254-8255. Esta distinção foi reiterada pelo Acórdão do Tribunal Constitucional n.º 464/2019, in *Diário da República* n.º 202/2019, Série I de 2019-10-21, p. 34.

dupla dimensão, positiva e negativa[9]. De facto, a sua natureza de direito, liberdade e garantia aponta, desde logo, para o seu caráter defensivo, estando em causa a tutela da reserva sobre factos cujo conhecimento por terceiros deve depender do consentimento do seu titular. Este direito de defesa e de liberdade com um conteúdo negativo (*Abwehrrecht*) fica garantido mediante a proibição de ingerência do Estado relativamente a dados informativos que pertencem ao cidadão, mas encontra-se concomitantemente dependente de uma prestação normativa por parte do Estado, traduzida na imposição legiferante concorrente para a plena realização da autodeterminação da pessoa.

Por outro lado, o mesmo direito reveste-se de uma natureza positiva, assente num feixe de faculdades e poderes de decisão e atuação relativamente aos dados pessoais, que dotam o titular dos dados de instrumentos que lhe permitem dispor e controlar os dados pessoais objeto de tratamento, seja realizado pelo setor público ou pelo setor privado, vinculando, com força económica e social equiparável, tanto entidades públicas como entidades privadas (*Drittwirkung*[10])[11].

Apesar da dignidade constitucional que lhe é atribuída, a proteção de dados exige a intervenção do legislador, cabendo à lei, conforme estabelece a letra do art. 35.º da CRP, o estabelecimento das exceções aos direitos ou condições de tratamento nele fixadas (por exemplo, exceções à proibição ao acesso a dados de terceiros, tal como consta do n.º 2), bem como a definição do conceito de dados pessoais e das condições aplicáveis ao seu tratamento, atento os termos do n.º 4 do preceito.

Desde 25 de maio de 2018, a referência à "lei e nos termos da lei" é primordialmente preenchida pela regulamentação constante do Regulamento (UE) N.º 2016/679, de 27 de abril de 2016 (doravante "RGPD"), ao revogar a anterior "Lei de Proteção de Dados Pessoais" (Lei n.º 67/98, de 26 de outubro), sendo a sua execução assegurada, no contexto da ordem jurídica nacional, pela Lei n.º 58/2019, de 8 de agosto. Enquanto ato de direito

---

[9] Neste sentido, FARIA, Paula Ribeiro de, *ob. cit.*, p. 789, e, jurisprudencialmente, o Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 35.

[10] Neste sentido, FARIA, Paula Ribeiro de, *ob. cit.*, p. 790.

[11] Para uma sistematização das faculdades e poderes de natureza positiva, veja-se o Acórdão do Tribunal Constitucional n.º 355/97, *Diário da República* n.º 131/1997, Série I-A de 1997-06-07, p. 2808.

derivado da UE de aplicabilidade direta nas ordens jurídicas nacionais dos Estados-Membros[12], o RGPD providencia, à partida, toda a regulamentação dos mecanismos através dos quais se torna possível o exercício da autodeterminação informacional constitucionalmente consagrada, ao cumprir o dever de ação legislativa constante do art. 35.º da CRP[13].

A jusfundamentalidade do direito da proteção de dados é, pois, caracterizada não só pelas faculdades constantes das normas consagradas na CRP no âmbito do art. 35.º, mas igualmente pelas faculdades constantes da medida legislativa que torna plenamente exequível as garantias aí presentes, ou seja, as faculdades constantes do RGPD. Consequentemente, importa questionar se a disciplina legislativa existente é apta para a proteção dos sujeitos face ao processamento de dados por via algorítmica.

Atendendo aos contornos do presente artigo, cumpre ainda referir que estes direitos não são absolutos, no sentido de que poderão sofrer limitações de conteúdo em determinadas situações e sob determinados pressupostos, face à relação de tensão existente com outros direitos fundamentais, tais como a liberdade de iniciativa privada[14], através de leis restritivas de direitos, liberdades e garantias. Nesta sequência, a operatividade de todo este feixe de direitos faz-se com a orientação de certos princípios que têm vindo a ser elencados pela doutrina[15] e operacionalizados pela jurisprudência constitucional e europeia, com destaque para os princípios da transparência, da especificação das finalidades, da fidelidade e de limitação da utilização.

---

[12] V. o 2.º parágrafo do n.º 2 do art. 99.º do RGPD, em junção com o 2.º parágrafo do art. 288.º do Tratado sobre o Funcionamento da União Europeia.

[13] Na medida em que é diretamente aplicável em todos os Estados-Membros, o RGPD apresenta vantagens face à Diretiva 95/46/CE, a qual estava sujeita a medidas de receção no plano do direito interno. Promove-se, assim, "a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais" (Considerando 10 do RGPD).

[14] Neste sentido, WACHTER, Sandra e MITTELSTADT, Brent, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2018, p. 5. Disponível em: https://ssrn.com/abstract=3248829. Acedido a: 13.10.2019.

[15] Para um quadro completo dos princípios em causa, v. CANOTILHO, Gomes, e MOREIRA, Vital, *ob. cit.*, p. 552.

A este respeito, cumpre referir a análise operada pelo Tribunal Constitucional no Acórdão n.º 464/2019, que vem clarificar a possibilidade de restrição expressamente prevista no n.º 4 do art. 35.º da CRP, no inciso final "salvo em casos excecionais previstos na lei", face à ausência de indicação no preceito dos seus pressupostos ou finalidades. Segundo o Tribunal Constitucional, "... a restrição terá de observar, para além da reserva de lei em sentido formal consagrada no artigo 165.º, n.º 1, alínea b), da Constituição, os limites impostos pelo artigo 18.º, n.os 2 e 3: proporcionalidade em sentido amplo; reserva de lei em sentido material; proibição de retroatividade; e inviolabilidade do conteúdo essencial."[16].

2. A problemática do controlo das decisões automatizadas

Atenta a exposição sobre o conteúdo essencial do direito fundamental à proteção de dados, encontram-se reunidas as condições para nos pronunciarmos sobre a capacidade deste direito fundamental, tal como se encontra hoje densificado, para se adaptar ao mundo da *Big Data*, considerando, em particular, a tendencialmente crescente tomada de decisões por inteligência artificial com base em algoritmos que funcionam com recurso a uma variabilidade incontrolável de dados, de onde decorre a proliferação de inferências, previsões, assunções relativas aos cidadãos.

Ao ser confrontado com este novo contexto, o Tribunal de Justiça da União Europeia (doravante "TJUE") defendeu que as inferências são parte integrante do sistema algorítmico de tomada de decisão, não consubstanciando dados pessoais passíveis de controlo pelo titular ao abrigo do direito fundamental em causa[17]. Face a este cenário de inaplicabilidade, o Tribunal Constitucional Alemão havia já ensaiado na sua jurisprudência um novo direito fundamental diverso do direito à autodeterminação informativa, denominado "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais" (*Grundrecht*

---

[16] Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 49.

[17] Acórdão do Tribunal de Justiça (2.ª seção) de 17 de julho de 2014, *YS c. Minister voor Immigratie, Integratie en Asiel* e *Minister voor Immigratie, Integratie en Asiel c. M e S,* processos apensos C-141/12 e C-372/12, ECLI:EU:C:2014:2081, pars.38-48.

auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme)[18]. Considerando que os sistemas técnico-informacionais permitiriam a criação de dados, maioritariamente produzidos autonomamente pelo sistema, sem a participação consciente do utilizador[19], o BVerfG concluiu que existia uma "lacuna de proteção" subsequente à perda do valor normativo do direito à autodeterminação informativa, atento o facto de se tratarem de realidades que dispensam a intervenção humana direta e consciente.

Todavia, cremos que esta visão que toma como objeto de proteção o sistema técnico-informacional em si não é correta, visto que propugna por uma verdadeira "objetivação" dos direitos fundamentais, deslocando a esfera de proteção para um elemento externo ao indivíduo, com a consequente crise da atual noção de "dados pessoais". A criação do direito-garantia, ao ter como objeto de proteção "sistemas", supõe na argumentação do BVerfG uma "desindividualização" do sujeito titular de dados pessoais, falecendo o recurso dogmático à ideia de autodeterminação informacional, desde logo por via de perda do valor dogmático de uma formulação construída sob o prefixo "auto"[20].

---

[18] Acórdão do BVerfG, Julgamento do Primeiro Senado de 27 de fevereiro de 2008 – 1 BvR 370/07 – pars. 1-333. Disponível em http://www.bverfg.de/e/rs20080227_1bvr037007en.html. Acedido a: 13.10.2019. Este novo direito-garantia foi mais recentemente analisado no Acórdão do BVerfG, Julgamento do Primeiro Senado de 20 de abril de 2016 – 1 BvR 966/09 – 1 BvR 1140/09 – pars. 1-360. Disponível em http://www.bverfg.de/e/rs20160420_1bvr096609en.html. Acedido a: 17.01.2019.

[19] A este respeito, impõe-se dar nota, na esteira de ALEXANDRE SOUSA PINHEIRO, que "a sacralização do consentimento constitui uma das ilusões mais correntes na história da proteção de dados e adquire características de puro logro quando aplicado à Internet, nomeadamente às redes sociais" – PINHEIRO, Alexandre Sousa, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, AAFDL Editora, 2015, p. 812.

[20] Neste sentido, LEPSIUS, Oliver, "Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft" in ROGGAN, Fredrik (org.), *Online-Durchsuchungen: Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008*, Berliner Wissenschafts-Verlag, 2008, pp. 22 e 33. Para uma perspetiva diferente, ROβNAGEL, Alexander e SCHNABELL, Cristoph, "Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationtecnhnischer Systeme und sein Einfluss auf das Privatrecht", *Neue Juristische Wochenschrift*, 49, 2008, p. 3535, segundo os quais o novo direito não protege sistemas que, pela sua técnica, impliquem a existência de dados pessoais de uma forma irrelevante para uma área da vida da pessoa afetada.

Ainda assim, a sua análise não se restringe, no que concerne à proteção do indivíduo relativamente à utilização de mecanismos de decisão automatizada e às inferências que resultam da sua operacionalização, ao recurso ao "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais", tendo numa recente decisão de 18 de dezembro de 2018, aplicado o direito fundamental à autodeterminação informativa, mas reconhecendo a necessidade de conceder uma proteção constitucional mais assertiva atento o nível de danosidade que a utilização dos mecanismos referidos pode infligir na esfera de proteção dos indivíduos.[21]

Como se verá de seguida, defendemos, de modo semelhante, a existência de espaço de manobra dentro do atual regime constitucional, partindo, porém, a nossa argumentação da consideração prévia de que as inferências são também elas dados pessoais.

2.1. As inferências como dados pessoais

Como resultado da ratificação do RGPD, a noção de dados pessoais em vigor no ordenamento jurídico português consiste na "informação relativa a uma pessoa singular identificada ou identificável"[22]. Tendo em consideração a definição apresentada, a determinação do estatuto legal dos dados inferidos levanta dificuldades, particularmente por estar em causa processos *M2M – Machine to Machine*[23]. Neste seguimento, impera o

---

[21] Acórdão do BVerfG, Julgamento do Primeiro Senado de 18 de dezembro de 2018 – 1 BvR 142/15 – par. 37. Disponível em http://www.bverfg.de/e/rs20181218_1bvr014215en.html. Acedido a: 03.02.2019. De acordo com o BVerfG, "the data in question can be aligned with data collected from other sources, allowing for diverse possibilities of use and linking. These possibilities of use and linking may yield further information and thus lead to conclusions that may result in the impairment of the constitutionally protected confidentiality interests of the person concerned as well as the subsequent interference with their freedom of conduct. Furthermore, there is particular potential for interference given the amount of data that can be processed by means of electronic data processing, which could definitely not be handled by conventional means. The increased risk associated with such technical possibilities is matched by the corresponding fundamental rights protection."

[22] V. n.º 1 do art. 4.º do RGPD.

[23] De modo semelhante, CORDEIRO, António Barreto Menezes, "Dados pessoais: conceito, extensão e limites", *Revista de Direito Civil*, A. 3, n.º 2, 2018, p. 304.

recurso ao modelo dos três passos formulado pelo Grupo de Trabalho do Artigo 29.º, que identifica três situações alternativas, em que se entende que se está perante informação relativa a pessoas. São elas o conteúdo, a finalidade ou o resultado[24].

É no âmbito deste último passo que se chega à conclusão de que este tipo de informação deve ser classificado como dados pessoais, na medida em que abrange toda a informação que não incida sobre uma pessoa (conteúdo) e que não vise avaliá-la ou influenciá-la (finalidade), mas que, em abstrato, o permita fazer (resultado). Consequentemente, ainda que se trate de informação não diretamente legível dos dados recolhidos, é dela inferida, apresentando potencial para impactar uma pessoa identificada ou identificável.

Neste sentido se pronunciou recentemente o Tribunal Constitucional, ao reiterar que "Não obstante aqueles dados [dados de tráfego que não envolvem comunicação intersubjetiva] não se reportarem a concretas e efetivas comunicações realizadas ou tentadas entre pessoas, mas apenas entre pessoas e máquinas ou até mesmo entre máquinas (*machine-to--machine communications*) proporcionadas por «agentes de software», a verdade é que podem assentar nos mesmos dados de base dos segundos e, tal como estes, possibilitar a monitorização, vigilância e controlo de movimentos de pessoas, assim como a construção de perfis de utilizadores que comportam riscos evidentes de perda de privacidade."[25]. Esta conceção pode ser ainda complementada pelo Parecer da Comissão Nacional de Proteção de Dados (daqui em diante, CNPD) n.º 38/2017, que refere que, nos dias de hoje, ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente, como sucede no caso das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes e ocorrem mesmo quando os indivíduos utilizadores dos equipamentos nada fazem.[26]

---

[24] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, WP 136, 20 de junho de 2007, p.12. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Acedido a: 14.10.2019.

[25] Acórdão do Tribunal Constitucional n.º 464/2019, *ob. cit.*, p. 42.

[26] V. Parecer da CNPD n.º 38/2017, processo n.º 8243/2017, pp. 7-10.

O facto de as inferências consistirem em assunções com elevado caráter subjetivo e não-verificável, que partem de dados já existentes sobre o titular de dados, não prejudica a classificação anteriormente operada, na medida em que a mesma não está dependente de se tratar de informação exata ou dada como provada[27]. Se assim fosse, estar-se-ia a prejudicar o objetivo último de proteção dos titulares de dados[28].

Tratando-se, portanto, de dados pessoais, as inferências, previsões e assunções beneficiam da proteção que a eles é disponibilizada no plano constitucional. Todavia, cumpre indagar se a regulamentação em vigor, ainda que recentemente alterada, surge preparada para responder aos desafios levantados, prevendo mecanismos aptos e eficientes para a proteção dos titulares de dados.

2.2. Suficiência das pretensões jurídico-subjetivas existentes?

Ao confrontar a regulamentação existente no plano constitucional, propendemos para a conclusão de que as pretensões jurídico-subjetivas expressamente consagradas são insuficientes para uma eficaz proteção do titular dos dados contra o atual contexto tecnológico, mas evidenciam um potencial de proteção aproveitável mediante a adoção de uma abordagem compreensiva.

Primeiramente, cumpre assinalar que a atual legislação adota um maior enfoque na fase do processamento referente ao *input*, comparativamente com os instrumentos de proteção e controlo que emergem referentes ao *output*. Isto é, as faculdades apresentadas estão mais direcionadas para a vigilância do modo como os dados pessoais são recolhidos e tratados, sendo relativamente incipiente a regulamentação existente quanto ao controlo das decisões alcançadas mediante a sua utilização, sobretudo tendo em consideração que as mesmas dão origem ou partem, frequentemente, de

---

[27] Article 29 Data Protection Working Party, *ob. cit.*, p. 6. No mesmo sentido, KLABUNDE, Achim, "DS-GVO Art. 4 Begriffsbestimmungen", in EHMANN, Eugen e SELMAYR, Martin (eds.), *Datenschutz-Grundverordnung*, 1.ª edição, CHBeck, 2017, pp. 7-8.

[28] Neste sentido também se pronunciou o Tribunal Constitucional – v. Acórdão do Tribunal Constitucional n.º 213/2008, in *Diário da República* n.º 86/2008, Série II de 2008-05-05, p. 19994.

inferências e assunções promovidas pelo recurso a fenómenos analíticos que se baseiam em dados não diretamente providenciados pelos sujeitos, mas que a eles dizem respeito.

Observando a legislação europeia sobre esta matéria, denota-se uma tentativa de melhor acautelamento desta segunda fase de tratamento de dados, consagrando-se aquilo a que doutrina vem designando como direito à explicação, que surge associado ao direito a contestar enunciado no 3.º parágrafo do art. 22.º do RGPD[29]. Importa, todavia, ter em consideração o cariz limitado desta nova pretensão jurídico-subjetiva, que advém da aplicação restritiva que tem vindo a ser promovida pelo TJUE. Segundo este órgão jurisdicional, são excluídas do seu escopo as situações em que se pretenda contestar o raciocínio e os parâmetros utilizados aquando da tomada de decisão, afirmando o TJUE que o conteúdo essencial deste direito fundamental não inclui a análise da precisão e correção do processo de tomada de decisão[30]. Afasta-se, assim, a possibilidade de o titular de dados pessoais ter acesso e, por sua vez, contestar o raciocínio analítico por detrás da tomada de decisão[31].

Concomitantemente, é importante deixar claro que são vários os obstáculos que este tipo de pretensão enfrenta na prática. Desde logo, importa recordar que, atualmente, estão em causa maioritariamente decisões assentes em sistemas de *machine learning*, cujo processo analítico é difícil de traduzir para linguagem percetível e inteligível pelos sujeitos, com a agravante de que esses processos estão em constante alteração em razão da aprendizagem que os caracteriza e distingue face aos sistemas algorítmicos tradicionais[32].

---

[29] Para uma visão exaustiva das posições doutrinárias existentes sobre esta temática, v. CALDAS, Gabriela, "O direito à explicação no Regulamento Geral sobre a Proteção de Dados", *Anuário do Direito da Proteção de Dados Pessoais*, 2019, pp. 40-45. Disponível em http://protecaodedadosue.cedis.fd.unl.pt/. Acedido a: 26.10.2019.

[30] Acórdão do Tribunal de Justiça, processos apensos C-141/12 e C-372/12, *YS, M e S c. Minister voor Immigratie, Integratie en Asiel, ob. cit.*, pars. 39-47.

[31] *Idem*, par. 45, e Acórdão do Tribunal de Justiça (3.ª seção) de 20 de dezembro de 2017, *Peter Nowak c. Data Protection Commissioner,* processo C-434/16, ECLI:EU:C:2017:994, pars. 51-54.

[32] Neste sentido, ANALIDE, Cesar e REBELO, Diogo Morgado, "Inteligência Artificial na era *data-driven*: a lógica *fuzzy* das aproximações *soft computing* e a proibição de sujeição a

Finalmente, não se pode deixar de relembrar que o desvendar dos parâmetros em que se alicerça o funcionamento dos autómatos, doutrinariamente conhecido como o dilema da abertura das *black boxes*[33], levanta um problema de confronto com outros interesses constitucionalmente protegidos, podendo pôr em causa a segurança, o interesse económico e comercial das empresas multimédia, os direitos de propriedade intelectual detidos pelas entidades públicas e privadas, afrontando a liberdade de iniciativa privada constitucionalmente consagrada.

Considerações finais: solução preconizada

Chegados a este ponto, reiteramos que a procura por um melhor enquadramento constitucional das novas realidades tecnológicas não passa pela consagração de um novo direito fundamental, impondo-se, sim, a reconfiguração do direito à proteção de dados, no sentido de enquadrar constitucionalmente novas manifestações de tutela subjetiva que se revelam necessárias, o que se traduz, neste âmbito das decisões automatizadas propiciadoras da proliferação de inferências de "alto risco", na implementação de uma proteção compreensiva, *ex-ante* e *ex-post*[34], enquadrada pelo princípio da limitação da utilização à finalidade.

A primeira componente de proteção, enquadrada na dimensão negativa deste direito, exige uma justificação por parte do criador e/ou utilizador dos dados pessoais inferidos relativamente à necessidade do recurso a esse tipo de dados como base do processamento automatizado de decisões, impondo-se, igualmente, a demonstração de que os dados e os métodos analíticos usados para a criação de inferências são adequados

---

decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais", *Fórum de Proteção de Dados*, n.º 6, 2019, p. 87.

[33] Trata-se de um conceito decorrente da ciência da computação utilizado para referir sistemas de que se conhece somente os dados de entrada e de saída, sem possibilidade de acesso ao seu funcionamento interno. Ao invés, quando são verosímeis ou inteligíveis os detalhes da programação de um sistema de aprendizagem, geralmente associado a aproximações de *hard computing*, dir-se-á ser *white box* a lógica que funcionaliza a extração de conclusões inferidas. – v. ANALIDE, Cesar e REBELO, Diogo Morgado, *ob. cit.*, p. 87.

[34] Igualmente, WACHTER, Sandra e MITTELSTADT, Brent, *ob. cit.*, pp. 4-5.

e estatisticamente fiáveis[35]. Neste seguimento, o titular tem direito a ser informado sobre a criação e utilização de assunções derivadas de dados pessoais a si respeitantes, cabendo ao responsável pelo tratamento de dados demonstrar a finalidade a que se destinam. Deve, por conseguinte, tratar-se de uma finalidade constitucionalmente legítima, impondo-se o recurso a um teste de proporcionalidade, no sentido de a utilização deste tipo de dados ser idónea e necessária no alcance dos benefícios e utilidade previstos. A estas exigências jurídico-constitucionais acrescem, por sua vez, o controlo da legitimidade, determinabilidade, exatidão, atualidade e limitação temporal da criação ou utilização dos dados inferidos.

Em complemento com a componente *ex-ante*, impõe-se uma segunda componente de proteção, agora *ex-post*, que visa a responsabilização algorítmica, permitindo ao sujeito contestar a decisão alcançada mediante a utilização de inferências imprecisas e irrazoáveis, não com vista a alterar o sentido da decisão tomada, mas a retificar os dados nos quais se baseia, sempre à luz da finalidade para a qual esses dados foram recolhidos.

Inspirados por Sandra Watcher/Brent Mittelstadt[36], propomos, enfim, uma nova pretensão jurídico-subjetiva: direito a inferências razoáveis ("*right to reasonable inferences*").

---

[35] Assim determina o Considerando 71 do RGPD. No mesmo sentido, Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Wp251rev.01, 6 de fevereiro de 2018, p. 26. Disponível em https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826. Acedido a: 14.10.19.

[36] Cfr. WACHTER, Sandra e MITTELSTADT, Brent, *ob. cit.*, p. 4.