# *Profiling* e algoritmos autónomos: um verdadeiro direito de não sujeição?

Afonso José Ferreira*

**Resumo:** O novo Regulamento Geral sobre a Proteção de Dados prevê um direito de não sujeição, por parte do titular de dados, às decisões que sejam baseadas no tratamento automatizado de dados ou na definição de perfis (*profiling*). A opinião do legislador europeu parece ser a de que esta forma de tratamento de dados é de alguma forma anormal, e deverá assim ser "proibida", deste modo escudando-se o particular. No presente texto, esta opinião é refutada. Em primeiro lugar, o tratamento automatizado de dados e o *profiling* são hoje considerados como formas legítimas de processamento de dados em setores como o *e-banking* ou o sistema judiciário. Em segundo lugar, seria irrazoável a exigência de que o processador de dados utilizasse apenas métodos manuais para o processamento de uma grande quantidade de dados. Em terceiro lugar, o próprio direito de não sujeição não poderá ser utilizado em situações em que o tratamento de dados pertence à base de uma relação contratual entre o titular e o processador, o que, na prática, retirará utilidade a este direito. Assim, o texto termina por propor outras soluções para os problemas que advêm do uso de algoritmos autónomos, como a responsabilidade fiduciária dos processadores.

***Palavras-chave:*** *Algoritmos autónomos; definição de perfis; direito de não sujeição; responsabilidade algorítmica.*

**Abstract:** The new General Data Protection Regulation creates a right of non-subjection, granted to the data holder, to decisions which are based on automated processing of data or on profiling. The EU legislator's opinion seems to be that this is an abnormal form of

---

* Licenciado em Direito pela Faculdade de Direito da Universidade Nova de Lisboa. Frequenta o Mestrado em Direito Europeu no Colégio da Europa. Bolseiro de Iniciação Científica no CEDIS/FDUNL. Este *paper* foi originalmente apresentado como uma comunicação no *workshop* "O novo regulamento de proteção de dados pessoais", organizado pelo Observatório de Proteção de Dados, integrado no CEDIS/FDUNL, a cujos participantes se agradece desde já pelos preciosos contributos prestados. Este trabalho é financiado por uma Bolsa da Fundação para a Ciência e Tecnologia.

data processing and that it should be thus "forbidden", thus shielding the individual. This text tries to refute this opinion. Firstly, automated processing of data and profiling are nowadays considered as legitimate ways to process data in sectors such as e-banking or the judicial system. Secondly, it would not be reasonable to demand that the responsible for data processing used solely manual methods when processing a large amount of data. Thirdly, the right of non-subjection itself may not be used in situations in which data treatment is in the basis of a contractual relationship between holder and processor, which, in practice, would deprive this right of its utility. Thus, the text will end by proposing other solutions for the problems deriving from the use of autonomous algorithms, such as fiduciary responsibility for processors.

***Keywords:*** *Autonomous algorithms; profiling; right of non-subjection; algorithmic accountability.*

**I.** A tecnologia tem vindo a evoluir a ritmos incríveis, tornando verdadeira a chamada Lei de Moore, segundo a qual o poder de processamento dos computadores pessoais duplica a cada ano. Assim, os avanços tecnológicos fazem agora parte do quotidiano das nossas vidas. Esta evolução, ligada a uma progressiva normalização da compra, e descida dos preços, dos computadores pessoais e outros mecanismos, como *smartphones* ou *tablets*, têm vindo desde os anos sessenta e setenta a tornar óbvia a necessidade da criação de métodos jurídicos de proteção de dados pessoais[1].

Estes mecanismos, que se revestem tradicionalmente, na Europa, de um caráter geral e amplo, que visa, contrariamente ao que ocorre nos EUA, regular todos os domínios em que é possível prever uma cedência de dados pessoais, têm vindo a evoluir com uma curiosa lentidão face à rapidez evolutiva dos processos tecnológicos. Tomando como exemplo a regulação na União Europeia, sobre a qual, por motivos óbvios, me debruçarei, a última versão da Diretiva de Proteção de Dados – a Diretiva 95/46/CE – data de outubro de 1995, momento em que ainda não existia sequer a Internet como a conhecemos hoje. Ora, tendo em conta este paradoxo, que opõe de forma clara uma tecnologia que evolui com velocidade extrema, e normas jurídicas

[1] Esta história pode ser apreciada, de um método geral, e circunscrevendo-se à Europa – foco principal da minha exposição – em Mayer-Schönberber, Viktor. "Generational development of data protection in Europe", *in*: Agre, Philip E. e Rotenberg (eds.). *Technology and Privacy: The New Landscape*. Cambridge: MIT Press, 1998.

que visam regular essa mesma tecnologia e que evoluem com uma lentidão igualmente extremada, é fácil perceber as críticas que a sociedade civil tem vindo a apontar ao legislador europeu quanto à inadaptação daquela Diretiva à regulação dos novos fenómenos tecnológicos.

Assumo-me, imediatamente, como um desses mesmos críticos. De facto, num campo que tem vindo a evoluir de forma tamanha, e com a quantidade de fenómenos da vida social que são diariamente eclipsados pela dimensão digital (como a saúde, o *e-banking* ou a educação, apenas para apontar os casos mais flagrantes), torna-se altamente preocupante assistir à progressiva descredibilização da Diretiva e à interpretação que o Tribunal de Justiça da União Europeia e os tribunais nacionais têm vindo a fazer da mesma, sendo um exemplo o caso *Google Spain*[2], que revela um profundo desconhecimento técnico sobre as tecnologias em causa[3]. Considerando a quantidade e profundidade dos dados pessoais em causa nas indústrias que exemplifiquei anteriormente, não se torna difícil percebermos o porquê da necessidade de um novo quadro jurídico nestas áreas.

O legislador europeu pareceu dar uma resposta aos seus críticos com a adoção do RGPD, cuja aplicação se iniciará em maio de 2018. No entanto, este Regulamento não colmata todas as falhas da teoria regulatória da União Europeia em matéria de novas tecnologias.

Uma destas falhas, que abordarei durante este *paper*, relaciona-se com o processamento de dados por algoritmos autónomos. Por algoritmos autónomos, refiro-me a métodos automáticos de processamento de dados, em que determinados dados são inseridos, direta ou indiretamente, pelo utilizador, num algoritmo que os processa para providenciar ao utilizador um resultado. O processamento de dados através de algoritmos autónomos funciona como uma *black box* – isto é, não é possível perceber o seu funcionamento interior, sendo apenas possível conhecer os *inputs* e os *outputs* da operação de processamento.

Por motivos de concorrência e inovação, estes algoritmos, e a forma como eles funcionam, são tradicionalmente secretos. Ou seja, o utilizador – e, na maior parte dos casos, as pessoas que supervisionam o funcionamento dos algoritmos – não têm acesso ao método de funcionamento do algoritmo.

---

[2] Acórdão do TJ, C-131/12, ECLI:EU:C:2014:317, *Google Spain*, de 13 de maio de 2014.

[3] Para um resumo destas críticas, v. "Google Spain SL *vs* Agencia Española de Protección de Datos", *Harvard Law Review*, vol. 128, 2014, pp. 735-742.

No entanto, a utilização de algoritmos autónomos para o processamento de dados tem-se vindo a tornar extraordinariamente comum. Desde logo, quando utilizamos um motor de busca como o Google, estamos a proceder a uma operação de processamento de dados através de um algoritmo autónomo. No entanto, são também operações de processamento de dados por algoritmos autónomos a procura, pelo Google, de publicidade especificada e personalizada em relação aos nossos históricos de pesquisa, ou de preços e promoções dos produtos que pesquisamos.

Mas estas operações são igualmente comuns em outros domínios. Por exemplo, nos Estados Unidos da América, tem-se vindo a tornar comum o uso de algoritmos para o cálculo da reincidência de criminalidade leve em tribunais de primeira instância. Por outro lado, é já perfeitamente comum a utilização por bancos e seguradoras de algoritmos que calculam as possibilidades de pagamento de empréstimos, ou a probabilidade da morte de um beneficiário no caso de um seguro de vida. Em suma, o uso de algoritmos autónomos tem vindo a tornar-se comum no quotidiano de todos, independentemente do seu contacto direto com as tecnologias. Isto leva a que, regra geral, os utilizadores finais – quer as pessoas que intervêm junto dos algoritmos, alimentando-os com dados, quer aqueles a quem o tratamento de dados ultimamente se destina – não tenham conhecimentos técnicos suficientes para perceber quais são, exatamente, as operações e "raciocínios" feitos pelos algoritmos.

**II.** Os algoritmos autónomos funcionam, de certo modo, como uma forma de *profiling* ou de definição de perfis. Por *profiling*, refiro-me ao tratamento automatizado de dados por uma entidade processadora, para perceber ou identificar determinados aspetos sobre uma pessoa. Em dadas situações – por exemplo, quando a Google identifica publicidade personalizada para alguém com base no seu histórico de pesquisa –, nem sequer é claro para o utilizador final que está a alimentar um algoritmo com dados pessoais.

Não é, assim, minimamente difícil perceber quais os problemas éticos e, potencialmente, jurídicos, que podem advir do uso de algoritmos autónomos. Identificarei brevemente um dos principais problemas que tem vindo a ser discutido pela doutrina nas ciências sociais e na engenharia informática. Este prende-se com aquilo a que Shirky chama de "autoridade algorítmica", ou, no original, *algorithmic authority*. Brevemente, este conceito refere-se à confiança implícita que a maior parte das pessoas deposita no resultado

dos algoritmos. Ou seja, tendo em conta que o algoritmo é uma máquina © e como tal, é supostamente desprovido de preconceitos ou parcialidades inerentes ao processo de decisão humano –, ser-nos-á mais fácil confiar em decisões feitas por aquele[4]. Esta confiança só tem vindo a ser aumentada através do uso de tecnologias de *machine learning* e do desenvolvimento das experiências e interfaces de utilizador, que tornam o contacto com o algoritmo normalizado e quase "humano".

Este progressivo depósito de confiança nos resultados dos algoritmos é problemático ao considerarmos que, muitas vezes, é impossível assegurar a imparcialidade dos mesmos. Devido a questões de programação e de design de interface do utilizador, os algoritmos funcionam, como referi anteriormente, como uma *black box*. Ou seja, nem o próprio programador, enquanto "monitorizador" do algoritmo, conseguirá perceber o porquê de aquele ter chegado a um determinado resultado.

Consideremos, por exemplo, uma investigação jornalística feita pelo website norte-americano ProPublica[5], que, ao analisar estatisticamente os resultados dos mecanismos algorítmicos de reincidência criminal em vários estados dos Estados Unidos da América, concluiu ser possível perceber a existência de tendências raciais desfavoráveis a pessoas de raça negra, quando comparadas com pessoas de raça branca que tenham o mesmo, ou pior, historial criminal. Colocando de lado o debate sobre o porquê destes resultados – que, embora essencial, é irrelevante na questão da autoridade algorítmica –, é inegável que é necessário garantir o correto funcionamento destes algoritmos.

Além disso, e por força da facilidade da sua utilização e resultados, é igualmente verdade que eles continuarão a ser utilizados e desenvolvidos. Assim, torna-se necessário garantir a independência e a imparcialidade dos algoritmos cujos resultados possam produzir efeitos nas esferas jurídicas dos particulares.

---

[4] Para uma discussão sobre este conceito, v. "A Speculative Post on the Idea of Algorithmic Authority", *Clay Shirky*, de 15 de novembro de 2009. Disponível em: <http://www.shirky.com/weblog/2009/11/a-speculative-post-on-the-idea-of-algorithmic-authority/> (acedido a 15/12/2017).

[5] Angwin, Julia *et al.* "Machine Bias", *ProPublica*, de 23 de maio de 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (acedido a 13/12/2017).

**III.** As áreas da regulação e do *cyberlaw* têm vindo a defender duas soluções primárias para o problema do excesso de autoridade algorítmica. Zittrain, baseando-se no direito norte-americano, propõe o conceito de *information fiduciary*, ou "fidúcia de informação[6]". Este conceito foi originalmente proposto por Balkin, constitucionalista norte-americano, especificamente para as questões de privacidade online[7]. Outra preocupação dos autores é a possibilidade de influência política dos algoritmos, como os do Facebook, que selecionam quais as notícias a que os utilizadores são expostos[8].

Para estes autores, tendo em conta que certas classes profissionais reguladas, como os médicos ou os advogados, têm, nos Estados Unidos, uma responsabilidade fiduciária para com os seus clientes no que diz respeito ao uso da sua informação, também as entidades que utilizam algoritmos autónomos para a produção de resultados deverão ser responsáveis para com os titulares dos dados quanto ao seu correto tratamento. Parece-me que esta solução poderia, em princípio, ser acolhida na tradição romano-germânica sobre as égides da responsabilidade civil e dos direitos de personalidade.

Outra solução, proposta por Pasquale[9], e mais próxima das soluções que têm vindo a ser desenvolvidas na Europa continental, refere-se a uma regulação e limitação dos dados que podem ser assimilados através do uso de algoritmos. Como notei anteriormente, algoritmos como o Google recolhem os inputs que lhes são alimentados pelos utilizadores para criar perfis sobre os mesmos. Pasquale, que chama a esta criação de perfis *runaway data* (algo como "dados em fuga") defende que é necessária regulação prévia que permita delinear com sucesso quais os dados que podem ou não ser recolhidos pelos algoritmos para a construção de perfis. Assim, e tendo em conta o caráter eminentemente privado e secreto dos algoritmos que são usados por empresas (quase como um *trade secret*), Pasquale sugere regulação administrativa nestas áreas, com fiscalização regular.

---

[6] Zittrain, Jonathan. "Facebook Could Decide an Election Without Anyone Ever Finding Out", *New Republic*, 2014. Disponível em: <https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering> (acedido a 16/11/2017).

[7] Balkin, Jack. "Information Fiduciaries and the First Amendment", *UC Davis Law Review*, vol. 49, n.º 4, 2016, pp. 1183-1234.

[8] Balkin, Jack e Zittrain, Jonathan. "A Grand Bargain to Make Tech Companies Trustworthy", *The Atlantic*, 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/> (acedido a 25/11/2017).

[9] Pasquale, Frank. *The Black Box Society*. Cambridge: Harvard University Press, 2015.

Estas duas soluções partem do pressuposto, a meu ver correto, de que o processamento automático de dados e a construção de perfis vão passar a ser o método comum de processamento de dados, e que, na nossa sociedade, adotarão um papel fulcral. No entanto, os instrumentos legislativos da União Europeia em matéria de proteção de dados não adotam esta perspetiva. Quer na Diretiva, quer no novo Regulamento, o *profiling* é visto como uma forma anormal de processamento de dados, e como uma exceção a ser evitada.

De facto, a única regulação específica que o Regulamento nos oferece no que diz respeito aos algoritmos autónomos e ao *profiling* é a previsão de um direito de não sujeição às decisões que produzam efeitos na esfera jurídica do titular dos dados e que sejam tomadas com base no resultado do tratamento automatizado de dados. Este direito é previsto pelo art. 22.º, n.º 1 do Regulamento.

**IV.** A previsão deste direito parece-me, no entanto, ser contraproducente. Em primeiro lugar, e observando-o de uma perspetiva regulatória, a previsão de um direito que permita ao particular recusar a adoção de decisões baseadas num algoritmo autónomo é irrisória. De facto, num mundo globalizado em que os algoritmos autónomos são comumente utilizados, e tendo em conta a inserção do RGPD na estratégia da Comissão Europeia de digitalização da economia europeia, a existência deste direito corresponde a um completo afastamento do progresso do comércio jurídico. A meu ver, é uma perspetiva ineficaz e ignorante da parte do legislador europeu.

Em segundo lugar, considero que esse direito não terá qualquer utilidade prática. O art. 22.º, n.º 2, alínea a) do Regulamento prevê que o titular dos dados não poderá exercer o direito de não sujeição quando o *profiling*, ou a decisão dele decorrente, sejam necessários para a celebração ou execução de um contrato entre o titular de dados e a entidade processadora dos mesmos. Ora, na criação desta exceção, o legislador europeu parece esquecer-se de que, em várias situações, o *profiling* e o processamento automatizado de dados fazem parte do objeto e da base de contratos de adesão celebrados entre o titular de dados e a entidade processadora no mero uso do algoritmo.

Na utilização de um motor de busca como o Google, por exemplo, o utilizador está a prestar tacitamente o seu consentimento para com a Política

de Privacidade e os Termos e Condições do serviço. Estes esclarecem que o titular consentirá no agrupamento dos seus dados para a definição de perfis que levem a usos publicitários ou de personalização dos resultados de pesquisa. Eles são, assim, contratos de adesão, cuja justiciabilidade tem vindo a ser afirmada várias vezes por tribunais nacionais, e que tem estado bem clara na jurisprudência norte-americana.

Na situação anteriormente referida, o processamento de dados é, assim, o objeto do contrato de adesão celebrado entre o titular dos dados e a entidade processadora. De outras vezes, no entanto, o uso do algoritmo faz apenas parte do contexto e da base do contrato. Imaginemos, por exemplo, a situação do uso de um algoritmo por um banco para o cálculo das possibilidades de pagamento de um requerente de empréstimo. Nesta situação, o contrato celebrado entre o requerente e o banco envolve o consentimento do tratamento dos dados do requerente, para que o banco possa decidir corretamente. Ora, nesta situação, permitir ao titular dos dados que se opusesse à forma como o banco processa esses dados, impedindo que eles sejam analisados automaticamente e obrigando o banco a utilizar métodos antiquados e incertos, seria fortemente irrazoável.

O titular dos dados teria o seu bolo e comê-lo-ia – embora consentisse no processamento dos dados, recusar-se-ia a que eles fossem processados de uma forma eficaz. Considerando a relevância crescente do processamento automatizado de dados no comércio jurídico, seria, em bom rigor, presumível ao titular de dados que o uso de métodos automatizados seja a forma pré-definida de agir. Assim, parece-me que seria irrazoável, e contra as bases do contrato, que o particular se pudesse opor a este processamento.

Assim, na maior parte das situações, este malogrado direito de não sujeição não terá sequer aplicação prática. De facto, a Comissão Europeia tenta proteger o particular escudando-o do progresso tecnológico – e, no caminho, falha nessa mesma proteção.

**V.** Ora, tendo em conta as questões, previamente analisadas, que são inerentes ao uso de algoritmos autónomos e que estão na base das preocupações do legislador europeu, que soluções poderiam ser propostas que não fossem anti paradigmáticas e que não perpetuassem o paradoxo da regulação tecnológica?

A primeira solução deriva da teoria da regulação, e, nomeadamente, da corrente do paternalismo justificado defendida por Sunstein[10]. Este autor defende que compete ao Estado orientar os seus cidadãos para que aqueles façam as melhores escolhas possíveis, através de mecanismos como a simplificação visual ou o aumento de informações disponíveis antes da escolha. Assim, a ideia – que é óbvia – baseia-se em tornar mais claro ao titular dos dados que tipo de processamento de dados irá ocorrer; através, por exemplo, do uso de ícones. Deste modo, não ocorreriam situações nas quais um utilizador alimenta indevidamente um algoritmo autónomo.

A segunda solução, e que se baseia nas ideias da fidúcia de informação propostas por Balkin e Zittrain, tem como base a exigência de uma "responsabilidade algorítmica" às entidades responsáveis pelo processamento dos dados. Esta responsabilidade dividir-se-ia em duas fases. Em primeiro lugar, durante a execução dos algoritmos, a sua supervisão seria garantida por entidades independentes, que avaliariam a sua imparcialidade e eficácia, utilizando os métodos técnicos disponíveis. Esta supervisão seria acompanhada de uma transparência para com esta entidade reguladora, que garantiria uma continuação da concorrência face aos rivais do criador do algoritmo. Numa segunda fase, seria permitida a responsabilidade extracontratual nas situações em que o processamento dos dados seja parcial ou incorreto, garantindo-se assim a existência de incentivos à manutenção da imparcialidade e eficácia dos algoritmos.

O uso destas soluções permitiria respeitar aquilo que o legislador europeu vê como essencial na regulação dos algoritmos autónomos – que estes sejam imparciais e eficazes, e que o seu uso não prejudique os titulares dos dados. Por outro lado, no entanto, permitiria que a regulação nesta área se aproximasse do nível de progresso tecnológico que já existe no comércio jurídico, e permitiria igualmente o contínuo desenvolvimento de uma forte economia digital na União Europeia.

---

[10] Sunstein, Cass. *Why Nudge? The Politics of Libertarian Paternalism*. New Haven: Yale University Press, 2014.