

# Os Desafios dos Consumidores na Era de *Big Data*

TAMÁRA CHELES\*

**Resumo:** Face a sociedade atual e a sua constante simbiose com a tecnologia nas mais pequenas ações diárias, bem como a implementação do Regulamento Geral de Proteção de Dados (doravante RGPD), é importante analisar a influência e dependência de *big data* (megadados) na contratação, nomeadamente na contratação com o consumidor. Questiona-se se, com a implementação do RGPD, estará agora o consumidor (verdadeiramente) protegido ou terá o legislador europeu sido ingénuo na construção do regime? Afigura-se primordial uma análise do *modus operandi* de *big data* para ser possível construir uma análise crítica e questionar em que medida o consumidor estará (des)protegido com a aplicação do RGPD.

**Palavras-chave:** *Big data, proteção de dados, consumidores, direito dos consumidores, profiling, decisões automatizadas, data brokers.*

**Abstract:** Given today's society and its constant symbiosis with technology in the smallest daily actions, as well as the implementation of the General Data Protection Regulations (henceforth GDPR), it is essential to analyse the influence and dependence of big data on contracts, namely contracts made by consumers. One must enquire, with the implementation of GDPR, is the consumer now (truly) protected or has the European legislator been ingenuous creating the regime? An analysis of the *modus operandi* of big data seems essential in order to be able to build a critical analysis and question to what extent the consumer is (un)protected with the application of the GDPR.

**Keywords:** *Big data, data protection, data brokers, consumers, profiling, automatized decisions, data brokers.*

---

\* Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa (FDUL). Frequenta o Mestrado Forense na Faculdade de Direito da Universidade Católica Portuguesa, em fase de dissertação. Este paper foi originalmente concebido como trabalho para avaliação final no âmbito da disciplina de Direito do Consumidor no Mestrado Forense.

## Introdução

A comunidade europeia está ciente da dependência e necessidade a uma escala sem precedentes à tecnologia e, conseqüentemente, da recolha de *big data* pelo que surgiu a necessidade de aprimorar o regime e a tutela dos cidadãos, com especial atenção ao consumidor – figura que estará em constante contacto com o recurso a mecanismos que possibilitem a recolha e o tratamento de dados pessoais, por parte das empresas com que contrata. Deste modo, terá de se verificar e continuar a proceder à proteção do direito fundamental à proteção de dados pessoais, devendo respeitar-se todas as regras aplicáveis à matéria.

O recurso à recolha, análise e tratamento de *big data* dos consumidores através da criação de algoritmos autónomos e de *machine learning* possibilita um controle e análise permanente acerca dos mesmos, sendo estes dados obtidos e tratados, muitas vezes, em tempo real, conservados por tempo indeterminado. A recolha destes dados poderá não deter importância evidente, mas quando recolhidos em conjunto com outros dados, poderão conduzir a uma formação de perfis detalhados sobre cada consumidor, possibilitando a integração dos variados consumidores em perfis específicos de acordo com os seus dados pessoais e comportamentos.

A adoção do RGPD foi a resposta aos críticos face às dificuldades de regulação jurídica e aos avanços tecnológicos sem resposta imediata do legislador. Porém, o regulamento não veio colmatar todas as falhas de regulação em matéria de tecnologias. Com efeito, o legislador absteve-se de regulamentar a atividade praticada por *data brokers*, isto é, a compra e venda de dados pessoais, sendo este um mercado que parece estar a emergir nos meios digitais.

Diariamente, os consumidores envolvem-se em inúmeras transações comerciais tanto *offline* como *online*. Tais interações, em particular as *online*, compreendem a partilha dos dados pessoais dos consumidores para com quem contratam e, porventura, com terceiros. Destarte, destas inúmeras interações poderão surgir vários desafios perante os consumidores que fará sentido tratar e analisar.

## Considerações iniciais

Começamos por assinalar a influência e a dependência cada vez superior de *big data* (megadados) na contratação, particularmente, na contratação com o consumidor. É possível definir o conceito de *big data* como a “rápida recolha, armazenamento e tratamento automatizado de um conjunto enorme e variado de dados e que permite uma maior personalização da oferta de bens e serviços”<sup>1</sup>. A principal proveniência desta informação que possibilita a recolha de dados é a *internet*. Tais dados são gerados pelos utilizadores da *internet*, seja pela utilização de aplicações, pela navegação em *browsers*, interações em redes sociais, histórico das páginas de *internet* que frequentou, entre outras ações ou omissões quando o utilizador se encontra em rede.

A matriz central do tratamento de *big data* reconduz-se ao facto de ser totalmente automatizado, sendo que a automatização constitui uma característica central do tratamento. O tratamento é concretizado através de modelos de análise construídos por algoritmos e assentes em técnicas de inteligência artificial, nomeadamente, *machine learning*. Entende-se por *machine learning*, a elaboração de conclusões e decisões sem intervenção humana, isto é, os computadores não necessitam de ingerência humana, conseguindo aprender através de outros computadores da rede, sendo, assim, uma técnica substancialmente caracterizada pela autonomia e automatização.<sup>2-3</sup> Ao recorrer às técnicas enunciadas, a inteligência artificial consegue gerar uma análise preditiva de comportamento<sup>4</sup>, sendo este o modelo predominantemente empregue no tratamento

---

<sup>1</sup> V. MORAIS CARVALHO, Jorge, *Manual de Direito do Consumo*, 6ª edição, Almedina, 2019, p. 51.

<sup>2</sup> Veja-se, a título de exemplo, a decisão de colocar um determinado e-mail recebido na pasta ‘spam’ ou na pasta ‘recebido’. O computador irá analisar o respetivo *e-mail* e irá determinar, sem intervenção humana, o destino do *e-mail*.

<sup>3</sup> Sobre esta temática, confira-se FLACH, Peter, *Machine Learning, The Art and Science of Algorithms that Make Sense of Data*, Cambridge University Press, 2012.

<sup>4</sup> Tome-se como exemplo de *predictive analytics* a operação de, através de uma simples análise do histórico da navegação pelos diversos *browsers* e *sites* na *internet* e a data de nascimento do consumidor, é possível personalizar um produto específico para determinado consumidor como, por exemplo, uma camisola desportiva com a sua data de nascimento para a qual o consumidor será imediatamente atraído.

de *big data*. Como refere Ana Alves Leal, este modelo corresponde ao processo de identificação de padrões a partir dos dados recolhidos de modo a possibilitar a previsão de determinados comportamentos ou tendências no futuro<sup>5</sup>. Podemos concluir que a aprendizagem automática é uma tecnologia que se constrói a si mesma sem necessidade de auxílio externo ou de *inputs* dos programadores tendo como característica própria ser uma aprendizagem autónoma de ingerências humanas – o oposto da programação manual onde será preciso *educar* o computador na tarefa que terá de realizar. Um algoritmo de aprendizagem aprende a partir dos dados que lhe forem fornecidos e aprende simulando o raciocínio por analogia, sem ter de recorrer a uma prévia instrução do seu programador<sup>6</sup>.

### **1. *Modus operandi* do tratamento de *big data***

A evolução da tecnologia apresenta variadíssimas vantagens, não obstante, ostenta também desvantagens e assim também o é quanto ao tratamento de dados pessoais. É inegável que para qualquer empresa o recurso ao tratamento de *big data* e, conseqüentemente, o acesso aos resultados obtidos através do tratamento de dados pessoais, apresenta inúmeros benefícios na medida em que, com base nos resultados do tratamento, a empresa toma conhecimento de como angariar potenciais novos clientes e ainda como conservar os atuais, inserindo-os em diversos perfis consoante os seus dados pessoais – perfis esses produzidos através do tratamento de *big data*. Com a angariação de dados e com a inserção dos clientes (potenciais ou atuais) em determinados perfis, a inteligência artificial efetua um *profiling*. Com *profiling* entende-se a técnica de “utilizar esses dados pessoais 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, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização

---

<sup>5</sup> ALVES LEAL, Ana, “Big data e proteção de dados pessoais – desafios à luz do Regulamento Geral de Proteção de Dados”, *Vida Judiciária*, n.º 207, maio/junho, 2018, pp. 18-19.

<sup>6</sup> Neste sentido, DOMINGOS, Pedro, *A revolução do algoritmo mestre: como a aprendizagem automática está a mudar o mundo*, Letras & Diálogos, 2017.

ou deslocações”<sup>7</sup>. Assim, as empresas ao recolherem e analisarem os diferentes dados pessoais, agrupando a diferente informação por grupos, terão a capacidade de identificar padrões, comportamentos e preferências de uma determinada pessoa, possibilitando a introdução dos diversos clientes em determinados perfis adequados aos seus dados pessoais<sup>8</sup>. Ao possibilitar a criação de perfis de clientes, o recurso ao tratamento de *big data* fomenta uma maior taxa de sucesso na angariação de novos clientes sendo que as empresas, conforme os resultados do tratamento de dados, ajustam a sua estratégia de *marketing* e a sua oferta ao seu público-alvo, bem como aumentam a sua capacidade de preservar os seus atuais clientes.

Com o desenvolvimento do comércio eletrónico, a personalização automatizada tornou-se imprescindível. Indo mais longe, na sociedade contemporânea onde a dependência tecnológica é colossal, é possível afirmar que a dependência da quantidade e qualidade dos algoritmos de aprendizagem que as empresas detenham, está diretamente ligado ao sucesso ou fracasso das empresas.

Como refere Ana Alves Leal, o *modus operandi* de *big data* é marcadamente indutivo: parte-se de conjuntos de dados para identificar padrões e associá-los a futuros comportamentos, produzindo-se conclusões sem anterior formulação de hipóteses e sem posterior experimentação<sup>9</sup>. Uma análise de todos os dados existentes é verdadeiramente impossível pelo que terá de haver uma prévia seleção e determinação de quais os dados selecionados sendo que a referida escolha ficará sempre sujeita e condicionada à vontade humana que irá direcionar a sua escolha tendo em conta as finalidades pretendidas. Destarte, as conclusões a que se

---

<sup>7</sup> Este processo, nos termos do RGPD, traduz-se no tratamento de dados, estipulado no seu art. 4.º, n.º 4.

<sup>8</sup> Expondo um simples e atual exemplo de *profiling*: as plataformas de *streaming* (como a *Netflix* ou a *HBO*) possuem um variado e diverso conteúdo armazenado, todavia, se os consumidores não souberem procurar o que pretendem assistir, a plataforma irá recomendar certo conteúdo com base no perfil do consumidor – perfil esse que é criado tendo como base várias características do consumidor, nomeadamente, idade, género, preferências, de conteúdo, últimos filmes ou séries visualizadas, entre outros. Tal torna-se exequível porque a empresa utiliza um algoritmo de aprendizagem que identifica as preferências do consumidor através das suas pesquisas e visualizações e, ao tratar esses mesmos dados fornecidos por aquele específico consumidor, recomenda determinado conteúdo.

<sup>9</sup> ALVES LEAL, Ana, *op.cit.*, pp. 18-19.

chegam através da análise de *big data* estarão sempre inevitavelmente refutáveis e condicionadas, tendo as mesmas partido de uma escolha arbitrária por parte do programador. Ora, tal limitação de dados terá um forte impacto quando são tomadas decisões tendo por base esses resultados. Consideremos, tendo as conclusões sido geradas através de dados fornecidos que foram selecionados e, por isso, não englobando a totalidade de dados, as conclusões recairão em premissas refutáveis, não verdadeiras e sem a devida neutralidade. Com efeito, o consumidor poderá vir a ser excluído de variados produtos e serviços que pretenda ter acesso se a conclusão gerada pela análise preditiva for desfavorável a este pelo facto de o tratamento de dados tiver sido precedido de uma análise arbitrária e com inexistência da devida neutralidade exigida. Pelo facto de não haver uma intervenção humana na análise de dados, gera-se o iminente risco de se bloquearem certos consumidores apenas e tão-só pelo resultado da análise dos seus dados, análise esta que foi somente realizada por um computador<sup>10</sup>.

## **2. *Data brokers*: um novo mercado económico?**

Podemos entender *data brokers* como entidades que colecionam informações através da recolha de dados por via da utilização, por parte dos consumidores, de *aplicações*, programas, navegação na *Internet*, compra e venda de produtos, entre outros, e que, posteriormente, vendem esses mesmos dados a outros *data brokers*, empresas ou indivíduos privados<sup>11</sup>.

É possível distinguir três categorias de atuação de *data brokers*: (1) recolha de dados pessoais que os consumidores preenchem sobre si mesmos de forma a completar alguma transação que pretendam – por exemplo, a finalização de um contrato de compra e venda de bens onde é exigido ao consumidor preencher vários dados pessoais (número de identificação fiscal, morada, número de telemóvel, entre outros); (2) foco maioritário em marketing, recolhendo dados para procederem à aplicação dos mesmos na publicidade da empresa com o objetivo de angariar novos

---

<sup>10</sup> Igualmente, MORAIS CARVALHO, Jorge, *op. cit.*, p. 52.

<sup>11</sup> Neste sentido, “Data Brokers: A Call for Transparency and Accountability”, *Federal Trade Commission*, 2014, pp. 1-110.

clientes ou até mesmo para aperfeiçoar o seu público-alvo<sup>12</sup>; (3) oferta de serviços para verificar identidades e dados pessoais com o objetivo de detetar fraudes.

Exposto brevemente o conceito e atuação de *data brokers*, importará referir que os *data brokers*, na maioria das vezes, não têm uma relação direta com os consumidores pelo que estes não estão cientes de que a sua informação está a ser tratada por terceiros (*data brokers*) e, posteriormente, alienada a outros terceiros. Todavia, para cessar o desconhecimento do utilizador ou consumidor acerca do tratamento dos seus dados, o RGPD veio impor às empresas a obrigação de informar o utilizador acerca da cedência e tratamento dos seus dados a terceiros, contudo, não incluiu a (nova) temática da atuação económica dos *data brokers* no regulamento.

Em suma, os *data brokers* têm como núcleo de negócio a alienação ou a cedência de dados pessoais de utilizadores ou consumidores, criando assim uma verdadeira comercialização de dados pessoais. Com a criação de um novo produto transacionável, gerou-se a criação de um novo mercado económico: a venda de dados pessoais<sup>13</sup>. A referida nova realidade jurídica e económica levanta várias questões. Tendo em conta este novo mercado económico questionamos se será lícito a comercialização de dados pessoais e se sim, se poderão terceiros vender dados pessoais de indivíduos ou só o portador dos mesmos poderá aliená-los? Todavia, não nos ocuparemos de responder a estas questões nesta exposição<sup>14</sup>.

---

<sup>12</sup> Nesta categoria, é frequente os consumidores serem colocados em categorias baseadas nas suas informações, tais como, idades, nomes, *e-mails*, interesses, entre outros. O objetivo é direcionar os consumidores para ofertas específicas e dirigidas apenas para aquele perfil de consumidor particular.

<sup>13</sup> Um possível exemplo deste novo mercado seria a compra e venda de um produto onde o consumidor, ao invés de cumprir o seu sinalagma através do pagamento numa quantia pecuniária, pagaria o respetivo valor através do fornecimento de dados pessoais. Muitas empresas alegam distribuir produtos grátis a consumidores sendo que, para tal, o consumidor *apenas* terá de fornecer os seus dados pessoais para receber o bem. É evidente que se tratará de uma estratégia onde a empresa beneficiará, de que forma for, com a aquisição de dados pessoais de diversos consumidores.

<sup>14</sup> Para uma melhor compreensão sobre esta (nova) temática, vide MORAIS CARVALHO, Jorge, *op. cit.*, pp. 56-60. Confira-se ainda a Proposta de Diretiva do Parlamento Europeu e do Conselho sobre certos aspetos relativos aos contratos de fornecimento de conteúdos digitais e ainda o considerando 23 e 24 da Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019.

De forma alguma temos a pretensão de arguir uma sociedade livre da evolução e dependência tecnológica, sendo claro que não poderíamos recuar a uma era obsoleta em matéria tecnológica. Contudo, a recente apresentação de uma nova realidade e do novo conceito de “comercialização de dados pessoais” é um tema que deveria criar uma maior sensibilização junto dos legisladores, nomeadamente ao legislador nacional e europeu, e de se exigir dos mesmos grande ponderação e cautela tendo em conta que se lida com informação sensível, passível de ser alienada por agentes que não o próprio detentor dos dados.

### **3. *Big data* e a proteção de dados pessoais à luz do RGPD**

O RGPD foi “especialmente pensado para a proteção dos cidadãos face ao tratamento de dados pessoais em larga escala, por grandes empresas e serviços da sociedade de informação [...] o paradigma que esteve subjacente [...] foi o das grandes multinacionais que gerem redes sociais [...] envolvendo a recolha e utilização intensivas de dados pessoais”<sup>15</sup>. No entanto, o regulamento não institui um regime especial para o tratamento de *big data*. Este tratamento tem a verificação em alguns pontos concretos do regime, tais como a obrigatoriedade de realização da avaliação de impacto sobre a proteção de dados, disposto no n.º 1 e 3 do art. 35º; notificação da violação de dados pessoais à autoridade de controlo, nos termos do art. 33º; prestação de informações relativas à lógica subjacente dos algoritmos e às consequências desse tratamento para o titular dos dados, por força da alínea f) do n.º 2 do art. 13º; entre outros.

O RGPD não compreende uma regulação específica para o tratamento de *big data*, sendo que poderão surgir sérias e ponderadas críticas tendo em conta que todo o regulamento tem como exigências nucleares do seu regime a transparência (art. 12.º), o consentimento [alínea a), n.º 1 do artigo 6.º e ainda art. 7.º], a limitação das finalidades e a minimização de dados [alínea c), n.º 1 do artigo 5.º]. O facto de ter sido omissivo quanto a uma temática que, a nosso ver, é fundamental na sociedade contemporânea, parece não estar em harmonia com os pilares do RGPD.

---

<sup>15</sup> Cf. Presidência do Conselho de Ministros, 2018, *Proposta de Lei n.º 120/XIII*, Lisboa.



Como consta do regulamento, a proteção das pessoas singulares relativamente ao tratamento de dados pessoais consiste num direito fundamental, nos termos do n.º 1 do art. 8.º da Carta dos Direitos Fundamentais da União Europeia e do art. 16.º do Tratado do Funcionamento da União Europeia, bem como do art. 26.º e 35.º da Constituição da República Portuguesa, a nível nacional. Importante dizer que, a nível nacional, ficam adstritos ao respeito pelo referido direito fundamental não só o Estado e as demais entidades públicas, como também é destinatário direto as variadas entidades privadas que detenham dados pessoais.

Para que o tratamento de dados seja lícito, terá de se verificar uma das situações subsumíveis a, pelo menos, uma das alíneas do n.º 1 do art. 6.º, especificamente: a) o consentimento ter sido dado pelo cidadão; b) o tratamento ser necessário para se realizar um contrato do qual o titular dos dados é parte; c) ser necessário o tratamento dos dados para se cumprir uma obrigação jurídica; d) ser necessário o tratamento para a defesa de interesses vitais tanto do titular como de outro indivíduo; e) o tratamento ser necessário para o exercício de funções de interesse público ou ainda para exercício de autoridades públicas; e, por fim, f) caso estejam em causa interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros (com a salvaguarda de os direitos e liberdades fundamentais do titular prevalecerem, em especial, caso o titular seja uma criança).

Quanto ao consentimento, este deverá ser dado mediante um ato positivo, claro e que indique uma manifestação livre de vontade, bem como a manifestação da sua vontade ser informada e inequívoca de que o titular consente no tratamento dos seus dados. Não obstante, o consumidor a qualquer altura poderá opor-se ao tratamento dos seus dados notificando, para tal, a pessoa coletiva em questão.

Para que o consentimento de tratamento de dados pessoais do consumidor seja válido não bastará que este preencha um *certo* na caixa que declara que este pretende receber *e-mails* com promoções e campanhas, por exemplo. Para que o consentimento seja eficaz e validamente constituído é indispensável que o consumidor preencha a caixa que declara que concorda que os seus dados pessoais sejam armazenados e/ou reutilizados para tal. Mais ainda, para que o consentimento seja livre e esclarecido, tal como exige o regulamento, o consumidor deverá ser informado acerca da

empresa que irá processar os seus dados pessoais, o objetivo do tratamento dos dados, porquanto tempo irá a empresa encarregar de tratar os dados detê-los, os seus direitos quanto aos mesmos e, também, informações da empresa subcontratante que irá receber e analisá-los.

Quanto à exigência do tratamento de dados em situações de realização de contratos, este será indispensável, atualmente, na maioria dos contratos, particularmente nos contratos celebrados à distância, máxime, *online*. Porém, para que o tratamento seja lícito nos termos desta alínea, o mesmo terá de ser necessário para que o contrato se concretize e não apenas ser conveniente (por razões económicas, práticas ou temporais) para as partes<sup>16</sup>.

#### **4. Questões por resolver**

Pelo que abordámos até então, cremos ser relevante algumas questões face à problemática de tratamento de dados pessoais, *big data* e a sua relação com os consumidores.

##### ***4.1. Da exigibilidade de diligência imposta ao consumidor-médio***

A figura do homem-médio (diligente, fiel ao direito, *bonus pater familias*) é conhecida no panorama jurídico, recorrendo-se em variadas ocasiões à mesma para determinar um nível-padrão para a exigência do grau de atuação de um indivíduo. Estando perante um direito que tem como sede principal o direito civil<sup>17</sup>, cremos que a transposição desta figura para uma figura adequada no Direito do Consumo é legítima, podendo, assim, referirmo-nos à figura de “consumidor-médio”: um consumidor diligente e fiel ao direito, onde seja possível aferir o nível-padrão de exigência de atuação por parte dos consumidores.

---

<sup>16</sup> BARRETO MENEZES CORDEIRO, António, “Artigo 6.º – Anotação”, in BARRETO MENEZES CORDEIRO, António, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, 2021, p. 113.

<sup>17</sup> Neste sentido, MORAIS CARVALHO, Jorge, *op.cit.*, p. 44.

A partir da imagem de consumidor-médio, tentar-se-á apurar se, colocado perante o facto em apreço, que *quantum* de diligência se exigirá ao mesmo aquando a leitura dos termos e condições sempre que o individuo pretenda adquirir um bem ou contratar um serviço. Chegados aqui, caberá questionar se se poderá exigir do consumidor-médio a leitura na íntegra dos termos e condições para adquirir a consciência do tratamento dos seus dados pessoais e, assim, exigindo-se do consumidor uma atitude pró-ativa e diligente quanto à partilha dos seus dados ou se haverá a necessidade de implementar normas paternalistas protegendo, então, o consumidor da sua própria inatividade.

Realizando o exercício de concretizar uma simples compra *online*, apercebemo-nos que para o consumidor se tornar consciente de todas as informações a que tem direito, terá de despende uma quantidade substancial de tempo. Mais, mesmo que a empresa (com que o consumidor pretenda contratar) refira as consequências do tratamento e com que terceiros partilha os dados pessoais do sujeito, o consumidor dificilmente ficará inteiramente esclarecido sobre os efeitos do tratamento nem quem são os referidos terceiros nem que fins visam estes com o tratamento de dados.<sup>18</sup>

É da nossa opinião que a ordem jurídica não deverá promover um consumidor negligente. Não obstante, a ordem jurídica tem de deter uma posição atualista e consciente das evoluções tecnológicas, bem como da sociedade em que se insere, não podendo alienar-se de tal exercício. Atualmente, o tempo é considerado um bem essencial e escasso e é fundamental geri-lo de uma forma adequada e racional. Deste modo, somos da opinião que o Direito deverá estabelecer mecanismos legais para que o consumidor alcance a possibilidade de se informar diligentemente, mas num período de tempo que não extravase o extraordinário face a celebração do contrato em causa. Será razoável esperar do consumidor-médio a leitura dos termos e condições, mas possivelmente já não será exigível uma leitura e análise aprofundada dos mesmos em certos contratos menos onerosos pelos motivos relativos ao período temporal que demandaria do consumidor, como supramencionado.

---

<sup>18</sup> Também assim, BARRETO MENEZES CORDEIRO, António, “Artigo 6.º – Anotação”, *op.cit.*, p. 111.

Deste modo, quanto mais oneroso e mais obrigações adviessem do contrato para o consumidor, mais tempo iria ser necessário para este despendar para se informar; para a situação contrária, no caso de as obrigações serem poucas e a onerosidade advinda do contrato ser diminuta, menos tempo deveria ser necessário para o consumidor se informar.

Mantendo o mesmo nível-padrão de exigência para todos os tipos de contratos a celebrar pelo consumidor, independentemente das obrigações e consequências adjacentes aos mesmos, cria-se a eventualidade de o consumidor se afastar da sua devida diligência de tomar conhecimento dos termos e condições adjacentes à celebração de contratos. A figura de consumidor-médio terá de se adaptar aos tempos modernos, tendo o direito de tomar em consideração e acompanhar o desenvolvimento da sociedade.

Em suma, para cada grau de oneração adjacente aos diferentes tipos de contratos, os termos e condições deveriam alinhar-se consoante esse referido grau. Destarte, um contrato de mútuo bancário exigirá, certamente, um consumidor muito mais alerta e diligente ao ler os termos e condições de adesão ao mesmo; em contraste, não se deverá exigir a mesma exigência do consumidor para celebrar um simples contrato de compra e venda de uma peça de vestuário por via online. Exposto isto, a figura de consumidor-médio irá, imperativamente, variar consoante a onerosidade e obrigações adjacentes aos diferentes contratos que o consumidor pretenda concluir.

Mais ainda, para que o tratamento de dados possa ser licitamente realizado, o consumidor terá de consentir com o mesmo o que parece trazer à colação a ideia de que este detém o controlo sobre o tratamento dos seus dados, tendo a possibilidade de não consentir. Contudo, somos do entender que este consentimento acaba por fornecer uma falsa sensação de controlo ao consumidor não sendo nada mais do que uma ficção jurídica. Ora, não consentindo com o tratamento de dados, os consumidores poderão ver afastadas as suas pretensões de contratar e aceder a variados serviços e bens<sup>19</sup>.

---

<sup>19</sup> Também mencionando as críticas subjacentes ao consentimento, BARRETO MENEZES CORDEIRO, António, “Artigo 6.º – Anotação”, *op. cit.*, p. 111.

#### **4.2. RGPD e a relação com os data brokers: uma real proteção dos consumidores?**

A atividade de *data brokers* consiste tão-só na compra e venda de dados pessoais, lucrando com a sua posterior venda a outras partes – sejam empresas, outros data brokers ou indivíduos particulares. Com a possibilidade do tratamento de dados pessoais e com o recurso à inteligência artificial, fomentou-se um novo mercado económico: venda de dados pessoais. Alvo deste novo mercado, em larga escala, encontram-se os consumidores que, muitas vezes, partilham os seus dados pessoais e consentem o tratamento dos mesmos de uma forma inconsciente ou, pelo menos, de uma forma não inteiramente conscientes das possíveis consequências do mesmo. Em outras situações o consumidor vê-se forçado a partilhar os dados e a consentir com o tratamento alegando que, para concluir a transação pretendida, o consumidor terá obrigatoriamente de partilhar os seus dados ou, num outro espectro, impondo, efetivamente, a partilha dos dados sem a qual o consumidor fica incapaz para celebrar o contrato pretendido. Tais circunstâncias fomentam e possibilitam a atuação indevida de data brokers.

Exposto isto, julgamos que mesmo com a implementação do RGPD, os consumidores não estão verdadeiramente protegidos de *data brokers*. Tal como foi suprarreferido, o RGPD não instituiu um regime especial para o tratamento de *big data* nem para a realidade de *data brokers*, não conferindo, assim, proteção para a atuação dos mesmos. Deste modo, os dados pessoais do consumidor – independentemente do grau de sensibilidade dos mesmos – poderão ser alienados e adquiridos por transações comerciais com o fim último de lucro. Mais ainda, a transposição do regulamento para o ordenamento jurídico nacional não tem como consequência direta e imediata que os consumidores estejam cientes dos direitos e garantias que lhe assistem sobre os seus dados pessoais, criando a abertura necessária para que a venda de dados pessoais de consumidores se torne uma realidade.

É verdade que o RGPD protege o consumidor: o silêncio e a inatividade deixam de ser considerados consentimentos válidos, sendo necessária uma verdadeira ação (afirmativa) por parte do consumidor para manifestar o seu consentimento ao tratamento dos seus dados. Todavia, uma ação por parte do consumidor estará longe de albergar todas as devidas proteções

no âmbito da proteção de dados, em particular em proteger o consumidor das potenciais consequências negativas acima mencionadas.

Parece-nos, então, que o consentimento do consumidor é falacioso pois apenas produz uma mera ilusão no sentido de que estes se encontram devidamente protegidos. Em variadas transações comerciais, é imposto ao consumidor que este consinta com o tratamento dos seus dados para que possa concluir a transação desejada (*vide* contratos de compra e venda de bens *online*) apesar de lhe ser garantido o direito de oposição, consagrado no art. 21.º RGPD. Exposto isto, o RGPD é, decididamente, um passo na direção certa para a proteção do consumidor, todavia, não podemos afirmar na sua totalidade que o consumidor se encontre verdadeiramente protegido, nem mesmo com a implementação do RGPD.

#### **4.3. Da (in)existência do direito ao esquecimento**

O RGPD determina o direito ao esquecimento no seu art. 17.º, sendo uma das justificações para tal a ocasião em que o consumidor revoga o seu consentimento para o tratamento dos seus dados. Da leitura do referido artigo parece resultar um breve e claro comando que confere ao indivíduo a garantia que os seus dados serão removidos e eliminados da base de dados de quem realize o tratamento dos mesmos. Porém, a conjuntura deste artigo insere-se numa realidade bem mais complexa do que aparenta ser.

Em primeiro lugar, o artigo em análise apresenta, desde logo, alguma controvérsia face à epígrafe do preceito sendo que apresenta duas terminologias distintas: direito ao apagamento e direito a ser esquecido. Contudo, como bem ensina Vítor Palmela Fidalgo, o art. 17.º subdivide-se em dois direitos: o direito ao apagamento *stricto sensu*, previsto no n.º 1 do preceito e o direito a ser esquecido, estabelecido no n.º 2<sup>20</sup>.

---

<sup>20</sup> PALMELA FIDALGO, Vítor “Artigo 17.º – Anotação”, in BARRETO MENEZES CORDEIRO, António, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Almedina, 2021, p. 189.

Do art. 17.<sup>o</sup> retira-se uma obrigação de resultado: a empresa a quem os dados pessoais foram fornecidos terá que eliminá-los<sup>21</sup>. Questão que se levanta com tal concerne à possibilidade de a empresa ter partilhado, anteriormente à execução pelo consumidor do seu direito ao esquecimento, os dados pessoais com terceiros.

Apesar do art.17.<sup>o</sup> ser de âmbito geral, isto é, ser dirigido a todos aqueles que procedam ao tratamento de dados pessoais, o direito ao apagamento de dados está configurado como um meio de tutela contra os perigos subjacentes ao tratamento de dados na internet<sup>22</sup>. Assim, desta nova garantia e proteção conferida aos consumidores questionamos se será real a possibilidade de um esquecimento eficaz ou será apenas uma ficção jurídica onde o legislador quis proteger o consumidor e legislar com esse fim sem tomar em consideração a realidade virtual adjacente.

Atentemos, a base de dados onde se encontram os dados pessoais que o cidadão pretende que sejam eliminados poderá partilhá-los com outras bases de dados. Deste modo, verificamos duas objeções face a esta obrigação de eliminar os dados pessoais do consumidor: i) da verdadeira possibilidade de deteção do efetivo paradeiro dos dados e a conseqüente impossibilidade de os eliminar: o legislador parece ter sido absorto à realidade quanto ao mundo digital e quanto à virtualidade dos dados pessoais; ii) a efetiva (im)possibilidade de apagar por completo os dados num espaço virtual sem fim<sup>23</sup>.

O mundo virtual é uma realidade ilimitada, pelo que a deteção do efetivo paradeiro dos dados pessoais vai para além da simples pesquisa e eliminação dos mesmos da base de dados das empresas. Consequentemente, pela característica própria da *internet*, questionamos se haverá uma verdadeira possibilidade de apagar de forma integral os dados numa realidade onde o infinito impera.

---

<sup>21</sup> Também no sentido de o art.17.<sup>o</sup> constituir uma obrigação de resultado, MEIRELES, Isa “O Direito a ser esquecido no Novo Regulamento Geral de Proteção de Dados: Uma utopia na (im)possibilidade de controlo do paradeiro dos dados pessoais ou uma possível destruição efetiva da base de dados?”, *Vida Judiciária*, n.º 207, maio/junho, 2018, pp. 28-29 e ainda PALMELA FIDALGO, Vítor, *op. cit.*, p.189 ao referir a “obrigação subjacente de apagar os dados.

<sup>22</sup> Também assim, PALMELA FIDALGO, Vítor, *op. cit.*, p. 189.

<sup>23</sup> Elencando também estes obstáculos face à obrigação de apagar os dados pessoais nos termos do artigo 17.<sup>o</sup> RGPD, MEIRELES, Isa, *op. cit.*, pp. 28-29.

Para além do exposto, na hipótese de as empresas serem obrigadas a eliminar os dados pessoais de um consumidor e assim o conseguirem, tal não obsta a que os dados desse mesmo consumidor já não tenham sido alienados a terceiros e, assumindo essa possibilidade como fática, como se verificará a aplicabilidade efetiva do art. 17.º RGPD? Se do art. 17.º nasce uma verdadeira obrigação de resultado (direito do cidadão em obter “o apagamento dos seus dados pessoais”) parece-nos, com o devido respeito pela opinião contrária, existir uma total inaplicabilidade prática do referido direito pois parece ser impraticável exigir de um terceiro – não tendo sido a parte contratante com o consumidor – que este elimine os dados pessoais. Verdade é que o próprio RGPD não obriga a que este terceiro os elimine, como fica expresso no n.º 2 do citado artigo, havendo apenas um dever de “informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento”. Porém, cremos que é aqui que se centra a pedra de toque da inaplicabilidade do direito ao esquecimento em sentido amplo tutelado pelo art.17.º.

O legislador teve o primor de garantir que o cidadão, *in casu*, o consumidor, teria controlo sobre os seus dados pessoais e teria à sua disponibilidade, verificadas os motivos elencados pelo n.º 1 do mesmo artigo, a exigência que se eliminasse os seus dados, contudo, não logrou estender este direito a terceiros que detenham dados pessoais do consumidor. Assim, parece-nos, salvo melhor opinião, que a proteção dos dados pessoais fica aquém do expectável e do desejado. Se o consumidor pretende que os seus dados pessoais sejam eliminados, certamente ambicionará que esta eliminação vise qualquer detentor dos mesmos e não apenas o detentor num primeiro plano.

Com todo o respeito pelas opiniões em sentido contrário, não cremos que a aplicabilidade do art. 17.º RGPD seja efetiva pela impossibilidade factual e prática de asseverar que esta garantia seja passível de execução. Ao legislador não cabe somente legislar e impor sanções, mas caberá também compreender a realidade sobre a qual irá legislar para aferir da sua (possível) aplicabilidade. O Direito não se poderá extrair do mundo real tencionando proteger os indivíduos somente na teoria se, em termos práticos, daí não advenha uma efetiva proteção. Se de tal não resultar uma verdadeira e eficaz proteção, tratar-se-á, tão-somente, de uma ficção jurídica – como aparenta ser o caso do art. 17.º RGPD pelos motivos elencados.



#### 4.4. Do direito de oposição ao *profiling*

Como foi supra exposto, os consumidores têm o direito de se oporem a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, incluindo a criação de perfis com base nos seus dados. Importante referir que o responsável pelo tratamento cessará o mesmo, excluindo situações em que apresente razões imperiosas e legítimas para esse tratamento, prevalecendo, assim, os interesses do responsável pelos dados, sobre os interesses, direitos e liberdades do titular dos dados.

O art. 22.º RGPD consagra o direito e garantia que o consumidor detém em 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. Porém, o n.º 2 do art. 22.º determina que o direito consagrado no seu n.º 1 não se aplicará no caso de ser necessária para a celebração ou a execução de um contrato entre o consumidor e o responsável pelo tratamento consagrando, aqui, o prevalecimento dos interesses do responsável pelos dados. Tragamos à colação, a título de exemplo (sendo um exemplo atual e que se verifica frequentemente nos contratos celebrados entre consumidores e instituições bancárias), o uso de um algoritmo por uma entidade bancária para o cálculo das possibilidades para a cessão de crédito bancário e tendo o consumidor dado o seu consentimento para que o banco tratasse os seus dados para que este conseguisse decidir de forma correta. Nesta situação, caso o titular se opusesse à forma como o banco processa esses dados (tendo, efetivamente, esse direito), impedindo que eles fossem analisados de uma forma automática, isto é, recorrendo a *machine learning*, o efeito prático seria que a instituição bancária, para decidir sobre a aceitação ou rejeição do crédito, seria forçada a recorrer a métodos antiquados e incertos, o que seria irrazoável.

Ora, coloca-se a interessante questão de confronto entre a necessidade de recorrer a técnicas de *machine learning* e de *profiling* para concluir contratos<sup>24</sup> e as variadas legislações que proíbem e sancionam a discriminação. Referimos discriminação porque, compreendendo que os algoritmos agem

---

<sup>24</sup> Pense-se em contratos de seguros, contratos de concessão de crédito, entre outros.

por si só e concebem conclusões pelos dados que lhe foram fornecidos, é possível que os resultados extraídos do algoritmo possam culminar em resultados discriminatórios face ao sexo, etnia, idade, doença, entre outros possíveis fatores discriminatórios. Com efeito, o conjunto de dados fornecidos ao computador é da competência e decisão de indivíduos. O conjunto de dados fornecidos ao computador sofre, imperativamente, uma limitação na medida em que seria impossível, dado a imensidade de dados existentes, “alimentar” o computador com a totalidade de dados existentes. Esta restrição dos dados fornecidos poderá ser realizada de forma deliberada a deixar de fora certos dados ou mesmo de uma forma não intencional. Não obstante, é certo que a conclusão a que o computador irá chegar no final, da análise dos dados poderá encontrar-se tendenciosa e não ter sido atingida com a devida neutralidade e imparcialidade, culminando em conclusões falaciosas. Destarte, poder-se-ia verificar a situação de ser negado a um consumidor a cessão de crédito porque o resultado das variadas técnicas a que a inteligência artificial poderá recorrer, não ser satisfatório para que o banco lhe assegurasse o crédito, tendo tido, porventura, dados como doenças, sexo, etnia, entre outros<sup>25</sup>.

Tendo o ordenamento jurídico consagrado a proibição de discriminação, tanto na Constituição da República Portuguesa, no seu art. 26.º, como em legislação avulsa<sup>26</sup>, não será invulgar que as decisões com recursos a algoritmos poderão ofender as variadas normas legais. Com efeito, a discriminação poderá ser direta ou indireta, consagrando a Constituição da República Portuguesa a proteção dos cidadãos contra ambas as vias discriminatórias. Neste sentido, um comportamento discriminatório direto seria aquele que, com base em qualquer das características elencadas no n.º 2 do art. 13.º da Constituição, discriminasse o indivíduo. Quanto à discriminação indireta, esta consubstanciaria em situações em que, apesar de não haver um apelo direto às diversas características inatas do indivíduo (como as elencadas no supracitado artigo), acabam por concluir com base nessas características<sup>27</sup>. Chegados aqui, é possível avaliarmos que ambas as situações são passíveis de ocorrerem nos contratos acima identificados.

---

<sup>25</sup> Igualmente, MORAIS CARVALHO, Jorge, *op. cit.*, p. 52.

<sup>26</sup> Tal como a Lei n.º 14/2008, Lei n.º 93/2017 e Lei n.º 46/2006.

<sup>27</sup> Cf. MOREIRA, Vital e GOMES CANOTILHO, José, *Constituição da República Portuguesa – Anotada*, Vol. I, 4ª edição revista, Coimbra Editora, 2007, p. 470.

Assim, mais uma vez indagamos a efetiva aplicabilidade e proteção conferida aos consumidores pelo RGPD, no sentido em que o mesmo confere o direito de oposição a decisões automatizadas, no entanto, contemporaneamente, em variadas situações é inconcebível exigir isso das partes contratantes pelos motivos supra expostos.

Julgamos, com o devido respeito, ter existido uma certa ingenuidade do legislador europeu na criação do RGPD, nomeadamente na criação do art. 22.º sendo que parece ser fictícia a devida aplicação do direito à não sujeição a tomadas de decisões baseadas em algoritmos autónomos pelos motivos acima elencados. Atualmente, vários são os contratos que recorrem imprescindivelmente ao recurso de *profiling* ou que este faz parte do objeto do contrato de adesão pelo que a alínea a), n.º 2 do art. 22.º parece não trazer qualquer utilidade na prática aos indivíduos, em especial, ao consumidor<sup>28</sup>.

É certo que é necessária uma autêntica proteção à parte mais fraca – *in casu*, o consumidor –, por outro lado, não se poderá obstar ao desenvolvimento tecnológico de tal forma que se paralelize transações jurídicas e económicas. Chegados a este ponto, torna-se imprescindível encontrar uma exequível solução quanto à temática abordada.

Uma primeira solução poderia comportar numa solução paternalista por parte do Estado, defendida por Sunstein<sup>29</sup>. Esta solução passaria por competir ao Estado orientar os seus cidadãos para que, no momento da contratação, estes possam fazer as melhores escolhas. Para tal, competiria ao Estado a criação de técnicas de simplificação para que o consumidor aprimorasse as suas escolhas no âmbito do consumo.

Uma outra solução, que julgamos ser a mais idónea para atingir os resultados pretendidos, seria a que se baseia nas ideias da fidúcia de informação propostas por Balkin<sup>30</sup> que tem como base a exigência de uma “responsabilidade algorítmica” às entidades responsáveis pelo processamento dos dados. Na lógica do autor, a figura de fiduciário poderá ser definida como um indivíduo que detém obrigações especiais

---

<sup>28</sup> Também assim, JOSÉ FERREIRA, Afonso, “*Profiling* e algoritmos autónomos: um verdadeiro direito de não sujeição?”, *Anuário da Proteção de Dados*, CEDIS, 2019, pp. 35-43.

<sup>29</sup> Neste sentido, *idem, ibidem*, p. 43.

<sup>30</sup> V. BALKIN, Jack “Information Fiduciaries and the First Amendment”, *UC Davis Law Review*, vol. 49, no. 4, 2016.

de lealdade e confiança perante um outro, agindo sempre e de acordo com a boa-fé. Balkin concebe um paralelismo com a figura tradicional de fiduciário, criando uma figura paralela face a era digital que vivemos: o fiduciário de informações. Por usufruirmos de diversas plataformas *online*, a quem confiamos os nossos dados pessoais e sensíveis, alguns serviços online estão subjulgados aos deveres dos fiduciários. Certamente tais deveres não são iguais aos deveres clássicos da figura de fiduciário, todavia, têm similitudes.

No geral, os deveres do fiduciário incluem o dever de não usar informações obtida através da sua atuação enquanto fiduciário de forma a poder prejudicar ou ganhar vantagem sobre o beneficiário. Para tal, Balkin chama à colação as atuações profissionais de médicos e advogados que, no seu desempenho profissional, se deparam com informações sensíveis e confidenciais, estando estes sobre um dever de sigilo próprio dos ofícios mencionados. Dito de outra forma, os profissionais como médicos e advogados comportam obrigações fiduciárias que lhes conferem deveres especiais de respeito para com as informações pessoais que obtêm através do exercício das suas profissões. Assim, o citado autor cria um paralelismo entre a figura tradicional de fiduciários e os seus deveres, com uma nova figura: o fiduciário de informações.<sup>31</sup> Concluindo, um fiduciário de informações é uma pessoa (singular ou coletiva) que, pela sua relação com uma outra, obteve informações sensíveis sobre esta, detendo, conseqüentemente, um dever especial de respeito pelas informações. A lógica da figura de fiduciário de informações é que este utilize as informações obtidas para privilégio do beneficiário e não para gerar danos para o mesmo.

Da mesma forma que se aceita a figura de fiduciário de informações em certas profissões, tais como as acima mencionadas, na era da informação, segundo Neil Richards, devemos expandir o conceito de fiduciário de informações a todos os serviços que o consumidor recorre e onde partilha dados sensíveis e pessoais, tais como lojas, sistemas de navegação, redes sociais e motores de busca<sup>32</sup>.

---

<sup>31</sup> V. BALKIN, Jack, *op. cit.*, pp. 1205-1209.

<sup>32</sup> Cf. RICHARDS, Neil “Intellectual Privacy: Rethinking civil Liberties in the Digital Age”, Oxford University Press in BALKIN, Jack, *op. cit.*, pp. 1221.

Esta responsabilidade algorítmica dividir-se-ia em dois momentos. Num primeiro estágio, durante a concretização dos algoritmos, a supervisão dos mesmos deveria ficar a cargo de entidades independentes que teriam como objetivo avaliar a imparcialidade e eficácia dos métodos de *profiling*: impedindo, assim, que os mesmos se concretizassem em resultados discriminatórios e arbitrários, afastando os consumidores de realizarem os contratos pretendidos. Num segundo estágio, nas situações em que ocorresse, efetivamente, um tratamento arbitrário, parcial ou incorreto dos dados pessoais, seria permitido o recurso a uma responsabilidade extracontratual. Como bem refere António José Ferreira, com o recurso a esta solução lograva-se a criação e existência de incentivos a uma manutenção constante da imparcialidade e eficácia dos algoritmos utilizados pelos operadores.

Optando por esta solução, a diversa legislação nacional quanto à proibição de discriminação seria respeitada e a pretensão do legislador europeu na ambição da imparcialidade, não discriminação e eficácia dos algoritmos autónomos, de forma a não prejudicar os titulares dos dados, seria alcançada. Como previamente expressámos, a ordem jurídica não poderá imiscuir-se de compreender e aceitar a evolução tecnológica adjacente à sociedade, devendo compreender a relação de simbiose existente. Caberá ao legislador criar legislação passível de concretização, não produzindo tão-só uma utopia e ficção jurídica.

## Considerações finais

Chegados até aqui, é incontestável que a proteção de dados terá um impacto expressivo a um compasso veloz no Direito. Ao Direito cabe regular e harmonizar a evolução da tecnologia e, simultaneamente, proteger os indivíduos. Face ao tratamento de dados pessoais, compreendendo que os algoritmos atuam com autonomia (veja-se o caso dos algoritmos autónomos e da técnica de *profiling*), torna-se evidente que por várias ocasiões as decisões resultantes de técnicas autónomas, irão traduzir-se em potenciais conflitos para com legislações que tutelam os consumidores.

Para além do exposto, a realidade dos *data brokers* e este (novo) mercado económico aparenta ser algo ainda algo desconhecido para o legislador europeu, não tendo este legislado sobre a matéria, nomeadamente, o

RGPD não veio tutelar a atuação destes atores. Consequentemente, nesta matéria, não se conseguiu lograr uma efetiva proteção do consumidor, ficando este desprotegido em vários flancos.

Quanto à não regulação no RGPD quanto à existência de um novo mercado económico (*data brokers*), mesmo com a nova regulamentação não se conseguiu lograr uma efetiva proteção do consumidor, ficando este desprotegido da comercialização dos seus dados pessoais por terceiros que obtêm rendimento e lucro através da alienação dos mesmos. Mesmo que o consentimento seja livre e esclarecido por parte do consumidor, tal não obstará à atuação de *data brokers*, sendo este um novo mercado económico que os legisladores, tanto nacional como europeu, têm de estar vigilantes e diligentes nas medidas a serem tomadas.

Consideramos que um dos principais problemas reside na circunstância de os consumidores não estarem conscientes no que consiste o tratamento dos seus dados e, conjectura potencialmente mais perigosa ainda, não compreenderem a extensão das consequências que poderão advir desse mesmo tratamento. A generalidade dos indivíduos não percebe a quantidade de dados que são diariamente recolhidos a seu respeito – nem o potencial lucro e benefícios envolvidos para terceiros.

É certo que o RGPD veio regular de forma ampla e definida o que anteriormente se encontrava regulado de uma forma mais frágil, no entanto, este pressupõe que o consumidor irá ser diligente e irá deter um satisfatório conhecimento sobre a matéria para que possa decidir de forma esclarecida e livre sobre a partilha dos seus dados.

Creemos, em conclusão, que nos encontramos longe de alcançar uma sociedade de consumidores informada e diligente, contudo, é do no nosso entendimento que, para uma apropriada proteção dos consumidores, não bastará a regulação. É crucial a devida educação dos consumidores para tais aspetos – falamos aqui de um direito fundamental do consumidor no tratamento de tais dados, por vezes, dados esses muito sensíveis (e mesmo que não consistam em dados sensíveis, terão sempre teor pessoal), pelo que deverá estar plenamente ciente dos seus direitos e garantias. O crescimento tecnológico é exponencial sendo que cada vez mais os algoritmos de aprendizagem terão impactos potencialmente gravosos para o consumidor, nomeadamente, estes determinarão a quem poderá ou não ser concedido crédito, quem poderá ou não realizar um contrato de compra e venda, entre outras inúmeras transações.