ANUÁRIO
DA PROTEÇÃO DE DADOS
2021

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio https://protecaodedadosue.cedis.fd.unl.pt, que pretende divulgar estudos doutrinários sobre o direito da proteção de dados pessoais. O Anuário é editado desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da NOVA School of Law. Aberto a qualquer interessado, o Observatório integra atualmente onze investigadores (três doutorados) oriundos de faculdades de direito (professores e doutorandos), de empresas e do setor público.

Os seis artigos publicados na edição de 2021 do Anuário resultam de uma chamada lançada em setembro de 2020 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram depois sujeitos a um processo de blind peer review e posteriormente revistos pelos coordenadores do Anuário.

ANUÁRIO DA PROTEÇÃO DE DADOS 2021

JURIS NOVA
DataporEU
FOCUS MATTERS. ADVOGADOS
FUTURA
CEDIS CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO
DA PROTEÇÃO DE DADOS
2021

ANUÁRIO DA PROTEÇÃO DE DADOS

2021

COORDENAÇÃO
FRANCISCO PEREIRA COUTINHO
GRAÇA CANTO MONIZ

CEDIS
CENTRO DE I&D SOBRE DIREITO E SOCIEDADE

ANUÁRIO DA PROTEÇÃO DE DADOS 2021

COORDENAÇÃO

Francisco Pereira Coutinho
Graça Canto Moniz

SECRETÁRIO EXECUTIVO

João Marques de Azevedo

EDIÇÃO

Universidade Nova de Lisboa. Faculdade de Direito.
CEDIS, Centro de I & D sobre Direito e Sociedade
Campus de Campolide, 1099-032 Lisboa, Portugal

SUPORTE: ELETRÓNICO

Junho, 2021

ISSN 2184-5468

CATALOGAÇÃO NA PUBLICAÇÃO
Pereira Coutinho, Francisco e Canto Moniz, Graça (coord.).
Anuário da Proteção de Dados 2020. Lisboa: CEDIS, 2021

Nota introdutória

O Anuário da Proteção de Dados é uma revista jurídica de livre acesso, disponível em linha no sítio <https://protecaodedadosue.cedis.fd.unl.pt>, que pretende divulgar estudos sobre o direito da proteção de dados pessoais. A revista é editada desde 2018 pelo Observatório da Proteção de Dados Pessoais, um grupo de investigação criado em 2016 no CEDIS – Centro de I & D sobre Direito e Sociedade da NOVA School of Law.

Os seis artigos publicados na edição de 2021 do Anuário resultam de uma chamada lançada em setembro de 2020 no sítio da internet do Observatório da Proteção de Dados Pessoais. Os textos foram depois sujeitos a um processo de *blind peer review* e posteriormente revistos pelos coordenadores do Anuário.

O Anuário inicia-se com um texto da autoria de Catarina Silva sobre a utilização de *cookies* e o consentimento, seguindo-se um artigo de Patrick de Pitta Simões que trata o tema da responsabilidade pelo tratamento de dados gerados pelo *Whistleblowing*. Os algoritmos são novamente abordados no Anuário em dois textos: um, da autoria de Sandra Barbosa e de Sara Félix, focado no artigo 22.º do Regulamento Geral de Proteção de Dados e, num outro texto, de Lucas Cortizo, sobre os efeitos da discriminação algorítmica. De seguida, Diogo Alves debruça-se sobre o papel da Cibersegurança na proteção de dados pessoais e, por fim, Tamára Cheles, escreve sobre os desafios dos consumidores na era de *big data*.

Esta obra não teria sido possível sem o patrocínio da SRS Advogados e da FUTURA, a quem agradecemos, nas pessoas do Luís Neto Galvão (SRS Advogados) e do Rodrigo Adão da Fonseca (FUTURA), o apoio que têm prestado desde a primeira hora a este projeto. Igualmente devidos são agradecimentos aos revisores deste número, ao André Inácio, ao Domingos Farinho, ao Eduardo Magrani, ao Fabrizio Esposito, à Inês

Oliveira, ao João Traça, à Laura Mendes, ao Luís Neto Galvão, ao Luís Terrinha, à Magda Cocco, ao Matheus Passos Silva, à Mariana Melo Egídio, ao Pedro Lomba, ao Ricardo Rodrigues de Oliveira, ao Sebastião Barros Vale, ao Tiago Fidalgo Freitas. Por fim, agradecemos ao João Marques de Azevedo o auxílio prestado na edição do Anuário, bem como a todos os autores que participam nesta edição.

Lisboa, 20 de maio de 2021

Francisco Pereira Coutinho
Graça Canto Moniz
Coordenadores do Observatório da Proteção de Dados

Índice Sumário

A utilização de *cookies* e a (in)suficiência dos requisitos aplicáveis ao consentimento

Catarina Silva[*]

Resumo: Nos dias de hoje, a nossa pegada digital é utilizada para obter dados pessoais acerca de cada um de nós, sendo esta informação recolhida frequentemente através do armazenamento de *cookies*. Ora, sendo a perda de privacidade um tópico que se vem tornando progressivamente mais premente, importa averiguar se, do ponto de vista normativo, serão suficientes os requisitos aplicáveis ao consentimento prestado para o armazenamento de *cookies* ou se, conforme melhor veremos no presente artigo, deverão os mesmos ser concretizados e adaptados às práticas dos operadores de *websites*.

***Palavras-chave**: Diretiva 2002/58/CE; Regulamento Geral de Proteção de Dados; cookies; privacidade; consentimento.*

Abstract: Nowadays, our digital footprint is used to obtain personal data about each one of us, and this information is often collected through the storage of cookies. As the loss of privacy is a topic that has become progressively more pressing, it is important to ascertain whether, from a normative point of view, the requirements applicable to the consent given for the storage of cookies are sufficient or whether, as we will verify in this article, they should be implemented and adapted to the practices of website operators.

***Keywords:** Directive 2002/58/EC; General Data Protection Regulation; cookies; privacy; consent.*

[*] Advogada. Licenciada em Direito pela NOVA School of Law. Frequenta o II Curso de Pós-Graduação Avançada em Proteção de Dados, na Faculdade de Direito da Universidade de Lisboa.

1. Afinal, o que são *cookies*?

Numa era cada vez mais digital, tem-se tornado usual comparar, de forma metafórica, a perda de privacidade ao "Big Brother", a personificação de um governo totalitário omnipresente retratada na obra "1984" de George Orwell, ou ainda ao "O Processo", de Franz Kafka, em que o personagem Joseph K. é informado de que está preso, não chegando, contudo, a descobrir, ao longo do desenrolar da história, os motivos por detrás da sua detenção, muito embora tais fundamentos pareçam ser conhecidos de várias pessoas, exceto dele próprio.

A verdade é que ambas estas analogias (embora distintas) parecem, cada vez mais, corresponder a uma realidade e não já apenas a uma mera ficção.

Nos dias de hoje, qualquer utilizador de Internet deixa, ainda que inconscientemente, um rasto de informações e de dados à mercê dos operadores de *websites*, os quais são recolhidos, na maioria dos casos, através do armazenamento de *cookies* nos dispositivos que, cada um de nós, utiliza diariamente.

Mas afinal o que são *cookies*?

De acordo com o Comité Europeu para a Proteção de Dados, "um cookie é um pequeno ficheiro de texto que um sítio Web instala no computador ou dispositivo móvel do utilizador"[1], sendo o mesmo processado e armazenado no *browser* do utilizador.

De uma forma geral, os *cookies* podem ser classificados em função da sua duração, proveniência e finalidades:

1. A respeito da duração, é comum distinguir entre *cookies* de sessão, os quais são temporários e expiram quando o utilizador fecha o *browser*, e os *cookies* persistentes, que permanecem armazenados no *browser* do utilizador até que sejam apagados.
2. A nível da proveniência, poder-se-á distinguir entre *cookies* primários, os quais são armazenados diretamente pelo *website* que o utilizador está a visitar, e *cookies* de terceiros, os quais são armazenados por um terceiro.

---

[1] Disponível em <https://edpb.europa.eu/cookies_pt>, acedido a 18 de novembro de 2020.

3. Relativamente às finalidades, existem essencialmente quatro tipos de *cookies*:

   a. *Cookies* estritamente necessários, os quais são essenciais para que o utilizador possa navegar no *website* e utilizar determinadas funcionalidades do mesmo.
   b. *Cookies* de funcionalidade, os quais guardam as preferências do utilizador relativamente à utilização do *website*, não sendo necessário que o utilizador volte a configurar o *website* cada vez que o visita.
   c. *Cookies* de desempenho, os quais recolhem informações sobre a utilização do *website*, com vista à criação e análise de estatísticas e ao melhoramento do funcionamento do mesmo.
   d. *Cookies* de publicidade, os quais rastreiam a atividade do utilizador, de modo a direcionar a publicidade em função dos seus interesses.

A proliferação das notificações de *cookies* (ou *cookie notices*), habitualmente sob a forma de janelas *pop-up*, constituiu um resultado da Diretiva 2009/136/CE da União, a qual alterou o artigo 5.º, n.º 3 da Diretiva 2002/58/CE (Diretiva *ePrivacy*)[2].

Com efeito, o referido artigo passou a prever que o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador depende da prévia obtenção de consentimento por parte do mesmo, prestado com base em "informações claras e completas [...] sobre os objectivos do processamento", excetuando-se, designadamente, as situações em que tal seja estritamente necessário. A título de exemplo, os *cookies* utilizados para adicionar artigos ao carrinho de compras numa loja *online* ou destinados a assegurar que o conteúdo de uma página carrega rápida e eficazmente são considerados estritamente necessários, pelo que a sua utilização não exige o consentimento prévio do utilizador.

---

[2] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

A 25 de Maio de 2018, entrou em vigor o Regulamento (UE) 2016/679[3] ("RGPD"), relativo à proteção de pessoas singulares no que diz respeito ao tratamento e à livre circulação de dados pessoais.

De uma análise comparativa entre ambos os diplomas, conclui-se que o RGPD constitui *lex generalis*, na medida em que regula a proteção de dados pessoais no espaço da União Europeia (sem prejuízo do seu âmbito extraterritorial), enquanto a Diretiva *ePrivacy* se aplica especificamente ao setor das comunicações eletrónicas. Posto isto, em matéria de *cookies*, a Diretiva *ePrivacy* complementa o regime geral previsto no RGPD.

A respeito da relação entre a Diretiva *ePrivacy* e o RGPD, o Comité Europeu para a Proteção de Dados emitiu a Opinião 5/2019[4], na qual esclareceu que existem múltiplas matérias que se inserem no escopo de aplicação de ambos os diplomas legais. Assim, estando em causa o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador, as provisões do RGPD, em especial os requisitos aplicáveis ao consentimento, serão subsidiariamente aplicáveis sempre que as informações armazenadas no dispositivo do utilizador constituam dados pessoais, aplicando-se, a título de regime-regra, o disposto no já mencionado artigo 5.º, n.º 3 da Diretiva *ePrivacy*. Com efeito, sendo exigida a prestação de consentimento por parte do utilizador ao abrigo do referido artigo, não é admissível que a utilização e armazenamento de *cookies* de que resulte o tratamento de dados pessoais tenha por base qualquer outro fundamento de licitude previsto no artigo 6.º do RGPD.

Atento o exposto, de modo a cumprir as disposições normativas do RGPD e da Diretiva *ePrivacy*, os operadores de *websites* devem:

a. Recolher o consentimento dos utilizadores antes de utilizar e armazenar quaisquer *cookies*, salvo nos casos legalmente previstos.

---

[3] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[4] EDPB. Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, de 12 de março de 2019.

b. Fornecer informação precisa, específica e em linguagem simples sobre os dados que cada *cookie* rastreia e a sua finalidade, antes da recolha do consentimento.
c. Documentar e armazenar o consentimento recebido por parte dos utilizadores.
d. Permitir aos utilizadores o acesso ao serviço, mesmo que estes se recusem a autorizar a utilização de determinados *cookies*.
e. Adotar mecanismos que assegurem aos utilizadores ser tão fácil retirar o seu consentimento como foi dá-lo em primeiro lugar.

2. O Acórdão Planet49

No dia 1 de Outubro de 2019, foi proferido pelo Tribunal de Justiça da União Europeia ("TJUE") o Acórdão Planet49[5], em resultado de um pedido de decisão prejudicial suscitado pelo Supremo Tribunal Federal alemão no âmbito de um litígio que opunha a Federação alemã das organizações e associações de consumidores (de ora em diante, "Federação") à Planet49 GmbH (de ora em diante, "Planet49").

2.1. Enquadramento fáctico

A 24 de Setembro de 2013, a Planet49, uma empresa alemã de jogos *online*, organizou um jogo promocional no *site* www.dein-macbook.de.

Ingressando no referido *site*, e em ordem a participar no sorteio, os interessados eram obrigados a fornecer o respetivo código postal, mediante o que eram reencaminhados para uma página Web em que deviam inscrever os respetivos nomes e endereços.

Sob os campos de preenchimento do seu endereço, foram dadas aos utilizadores duas declarações descritivas juntamente com quadrículas de seleção.

---

[5] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801

A primeira quadrícula de seleção, que se encontrava desmarcada, exigia que os utilizadores dessem o seu consentimento aos patrocinadores e parceiros da Planet49 para o envio de informações promocionais via correio, telefone, email ou SMS.

Por sua vez, a segunda quadrícula de seleção, que foi pré-selecionada, exigia que os utilizadores autorizassem a utilização de *cookies* pela Planet49 por meio de uma empresa designada Remintrex que se ocuparia da recolha de dados pessoais cruciais para fins publicitários.

Sucede que os termos e condições aplicáveis ao jogo promocional supramencionado determinavam que os utilizadores só podiam participar se, pelo menos, a primeira quadrícula de seleção fosse assinalada. A este respeito, cumpre referir que os utilizadores podiam optar por não autorizar a utilização de *cookies*, desde que desmarcassem manualmente a segunda quadrícula de seleção.

2.2. Entendimento adotado pelo TJUE e principais conclusões

De acordo com o Acórdão sob análise, "[...] um consentimento dado através de uma opção pré-validada não implica um comportamento cativo por parte do utilizador de um sítio Internet"[6] e, por esse motivo, não consubstancia um consentimento suscetível de ser utilizado como fundamento de licitude do tratamento de dados pessoais.

Ora, o artigo 2.º, alínea h), da Diretiva 95/46/CE[7] do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, aplicável *ex vi* artigo 5.º, n.º 3, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002 ("Diretiva *ePrivacy*") define "consentimento da pessoa em causa" como "qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento". Por conseguinte, e no

---

[6] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 52.

[7] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

seguimento das conclusões do Advogado-Geral[8], o TJUE afirmou que a exigência de uma manifestação de vontade da pessoa em causa aponta, evidentemente, para um comportamento ativo, e não passivo[9]. Neste sentido, um consentimento dado através de uma opção pré-selecionada – e que o utilizador deverá desmarcar em ordem a recusar o seu consentimento – não implica, em qualquer circunstância, um comportamento cativo por parte do utilizador, pelo que não se poderá considerar que o mesmo tenha sido validamente obtido[10].

De sublinhar que a interpretação adotada nos termos acima referidos é imposta igualmente por força do RGPD, em especial à luz do Considerando 32, segundo o qual:

> "O consentimento do titular dos dados deverá ser dado mediante um acto positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato electrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, seleccionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. [...]".

A este respeito, o Tribunal esclareceu ainda que o consentimento prestado pelo utilizador, na aceção da alínea h) do artigo 2.º da Diretiva 95/46, deve ser específico, na medida em que deve incidir precisamente sobre o tratamento de dados pessoais em causa e não poderá, por conseguinte, ser deduzido de uma manifestação de vontade que tem um objeto distinto. Tal significa que – e com referência ao caso *sub judice* – o simples facto de um utilizador ativar o botão de participação num jogo

---

[8] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17.

[9] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 52.

[10] *Idem*, para. 57.

promocional não poderá ser considerado suficiente para concluir que o mesmo deu validamente o seu consentimento ao armazenamento de *cookies* ou à divulgação dos seus dados a quaisquer terceiros[11].

Ademais, o Tribunal considerou que a duração do funcionamento dos *cookies* e a possibilidade de terceiros terem ou não acesso aos mesmos se encontram abrangidas pelo leque de "informações claras e completas" que devem ser fornecidas ao utilizador por força do disposto no n.º 3 do artigo 5.º da Diretiva *ePrivacy*, constituindo, aliás, requisito de validade do consentimento prestado[12].

Ora, de acordo com as conclusões do Advogado-Geral, "as informações claras e completas devem permitir ao utilizador determinar facilmente as consequências do consentimento que possa vir a dar e garantir que esse consentimento seja dado com pleno conhecimento de causa", sendo que "essas informações devem ser compreensíveis e suficientemente pormenorizadas para permitir ao utilizador compreender o funcionamento dos cookies utilizados"[13].

Estatisticamente falando, o Relatório elaborado pelo Grupo de Trabalho do Artigo 29[14], datado de 2015, elucida-nos quanto à importância destas informações para o pleno esclarecimento do utilizador aquando da prestação do seu consentimento à utilização e armazenamento de *cookies*.

Ora, com base nos 478 *websites* analisados, apurou-se a existência de três *cookies* primários (em inglês, *first-party cookies*) com uma duração de 7985 anos, expirando a 31/12/9999 às 23:59, e de 17 *cookies* primários em 15 diferentes *websites* com uma duração superior a 100 anos. Cumpre sublinhar que a duração média de *cookies* primários utilizados pelos *sites* analisados é de 14.34 anos.

Em contraposição, os *cookies* de terceiros (em inglês, *third-party cookies*) apresentam uma duração substancialmente menor: em média, reduz-se para 1.77 anos.

---

[11] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, paras. 58 a 60.

[12] Idem, paras. 72 a 81.

[13] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17.

[14] Grupo de Trabalho do Artigo 29. *Cookie Sweep Combined Analysis – Report*", de 3 de fevereiro de 2015.

É, pois, evidente que a duração da utilização dos *cookies* (que, em muitos casos, considerar-se-á excessiva) apresenta, em especial, extrema relevância para a prestação de um consentimento devidamente esclarecido, sendo determinante para a completa compreensão da extensão da utilização desses *cookies*.

Uma vez mais, esta interpretação é igualmente sustentada pela alínea a) do n.º 2 do artigo 13.º do RGPD, segundo a qual o responsável pelo tratamento deve facultar ao titular dos dados informação sobre, nomeadamente, o prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo, de modo a garantir um tratamento equitativo e transparente.

Além disso, e em conformidade com o disposto na alínea e) do n.º 1 do artigo 13.º do RGPD, deverá igualmente ser prestada ao titular dos dados informação relativa aos destinatários ou às categorias de destinatários dos dados, em que se integra, portanto, a possibilidade de terceiros terem ou não acesso aos *cookies*.

Mais: de acordo com o entendimento sufragado pelo TJUE[15], as obrigações legalmente impostas em matéria de *cookies* e consentimento são aplicáveis independentemente de estarem ou não em causa dados pessoais. Para o efeito, o Tribunal baseou-se no facto de o n.º 3 do artigo 5.º da Diretiva *ePrivacy* fazer referência tão-somente ao "armazenamento de informações" e à "possibilidade de acesso a informações já armazenadas", sem, todavia, qualificar essas informações como dados pessoais.

Tal decorre também das conclusões do Advogado-Geral, segundo o qual a disposição legal *supra* mencionada se destina "a proteger os utilizadores de qualquer intromissão na sua esfera privada, independentemente da questão de saber se essa intromissão envolve dados pessoais ou outros dados"[16].

Sem prejuízo do referido, no nosso entendimento, tal resultaria, desde logo, do próprio espírito da Diretiva *ePrivacy*, cujo âmbito de aplicação se distingue do do RGPD, muito embora ambos se cruzem quando esteja

---

[15] Acórdão do Tribunal Geral de 1 de outubro de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH*, C-673/17, ECLI:EU:C:2019:801, para. 66 a 71.

[16] Conclusões do Advogado-Geral Maciej Szpunar, de 21 de março de 2019, Processo C-673/17, para. 107.

em causa o armazenamento de informação ou o acesso a informação armazenada no dispositivo de um utilizador que constitua um dado pessoal. Posto isto, quando isoladamente considerados, verifica-se que o RGPD visa, em traços gerais, assegurar a proteção dos dados pessoais, enquanto a Diretiva *ePrivacy* procura preservar a esfera privada individual, a qual pode ou não incluir, em si mesma, dados pessoais. A este respeito, o considerando 2 da Diretiva *ePrivacy* esclarece que a mesma "visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Europeia. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.º [referente ao respeito pela vida privada e familiar] e 8.º [referente à proteção de dados pessoais] da citada carta.". O considerando 24 da Diretiva *ePrivacy* acrescenta que "o equipamento terminal dos utilizadores de redes de comunicações electrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais", confirmando, assim, que a Diretiva *ePrivacy* visa salvaguardar, em primeira linha, a esfera privada de cada indivíduo face a qualquer intromissão externa, independentemente de estar ou não em causa a proteção de dados pessoais.

Em suma, e pese embora o caso sob análise anteceda a entrada em vigor do RGPD, a decisão foi tomada à luz dos padrões impostos pela referida norma, concluindo-se que:

a. As quadrículas de seleção pré-assinaladas mediante as quais a utilização de *cookies* e tecnologias semelhantes é autorizada não constituem consentimento válido ao abrigo da Diretiva *ePrivacy*.
b. Nos casos em que é exigida a obtenção de consentimento para a utilização de *cookies* nos termos da Diretiva *ePrivacy*, são aplicáveis os requisitos previstos em matéria de consentimento pelo RGPD.
c. A circunstância de os *cookies* constituírem ou não dados pessoais não é relevante, porquanto o n.º 3 do artigo 5.º da Diretiva *ePrivacy* é aplicável a qualquer informação instalada ou acedida a partir do dispositivo de um indivíduo.

d. Devem ser fornecidas aos utilizadores de um *website* informações acerca da duração da utilização dos *cookies* e da possibilidade de terceiros terem ou não acesso aos mesmos.

Na verdade, numa era pós-RGPD e pré-Regulamento *ePrivacy*, o Acórdão sob análise não parece acrescentar particulares novidades em matéria de *cookies*. Ainda assim, a presente decisão assume especial relevância na medida em que vem reforçar que a utilização de *cookies* exige um consentimento expresso, livre, informado e específico. Ademais, o Acórdão Planet49 elimina quaisquer dúvidas existentes a respeito das regras aplicáveis ao consentimento para a utilização de *cookies*, alertando para as práticas que deverão ser evitadas e encorajando os operadores de *websites* a seguir a orientação adotada pelo TJUE por forma a garantir o adequado cumprimento das regras e obrigações que lhes são impostas pelo RGPD.

Ainda assim, o Tribunal não se pronunciou acerca de outras questões relevantes a respeito deste tema, em especial relativamente à admissibilidade das chamadas *cookie walls*, que condicionam o acesso do utilizador a um *website* ou a alguns serviços ou conteúdos ao seu prévio consentimento à utilização de *cookies*, deixando, por isso, algumas dúvidas em aberto.

Não obstante, o Comité Europeu para a Proteção de Dados já se pronunciou no sentido de reconhecer que o consentimento obtido através das referidas *cookie walls* não é livre, acolhendo, assim, a posição maioritariamente adotada pelas autoridades de proteção de dados nacionais. Mas deverá mesmo ser essa a orientação a adotar? A resposta a tal questão, conforme veremos adiante, não é clara.

3. Orientação do Comité Europeu para a Proteção de Dados

A 4 de Maio de 2020, na esteira do entendimento adotado pelo TJUE no âmbito do Acórdão Planet49, o Comité Europeu para a Proteção de Dados adotou uma orientação[17] onde esclarece o que constitui um consentimento válido para o tratamento de dados pessoais ao abrigo do RGPD.

---

[17] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679*, de 4 de maio de 2020, disponível em <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, acedido em 14 de novembro de 2020.

Esta orientação, que atualiza as diretrizes do Grupo de Trabalho do Artigo 29º em matéria de consentimento[18], cimenta uma aplicação unificada do RGPD, sendo que, muito embora não tenha carácter vinculativo, é utilizada pelas autoridades nacionais de cada Estado-Membro na interpretação e aplicação do RGPD.

Assim, para que um consentimento seja considerado válido, nos termos previstos no RGPD, é necessário que seja:

a. Livre;
b. Específico;
c. Informado;
d. Inequívoco.

O Comité Europeu para a Proteção de Dados esclarece que "uma indicação inequívoca do consentimento do utilizador" implica uma ação clara e afirmativa por parte do utilizador. A este respeito, e num dos exemplos dados pelo Comité Europeu para a Proteção de Dados, as ações de um utilizador como o mero percorrer ou navegar de um *website* ou qualquer atividade similar constitui, em bom rigor, um consentimento implícito, não cumprindo, por conseguinte, os requisitos de validade do consentimento exigidos pelo RGPD, em especial a existência de uma ação clara e afirmativa. Posto isto, deixa de ser admissível que as notificações de *cookies* afirmem que a navegação contínua num determinado *website* vale como consentimento para a utilização de *cookies* que processam dados pessoais.

Alternativamente, as referidas notificações devem ser configuráveis e o *website* está impedido de utilizar ou armazenar quaisquer *cookies* sem a obtenção do consentimento prévio por parte do utilizador.

A este respeito, o Grupo de Trabalho do Artigo 29.º considerou que a exigência de "consentimento prévio" resulta diretamente do elemento literal do n.º 1 do artigo 6.º do RGPD "tiver dado"[19]. Neste sentido, decorre logicamente do referido artigo que se exige a existência de um fundamento

---

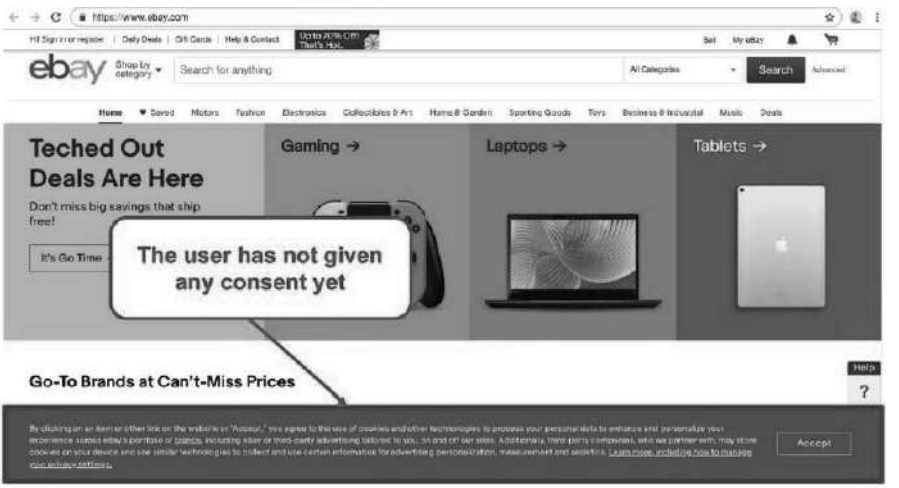
[18] Grupo de Trabalho do Artigo 29º. *Opinion 15/2011 on the definition of consent (WP 187)*, de 13 de julho de 2011.

[19] Grupo de Trabalho do Artigo 29º. *Opinion 15/2011 on the definition of consent (WP 187)*, de 13 de julho de 2011.

legal válido antes de se iniciar um qualquer tratamento de dados. De outro modo, o tratamento de dados desenvolvido desde o momento em que o referido tratamento teve início até ao momento em que o consentimento foi obtido é ilícito em virtude da inexistência de base legal.

Num estudo desenvolvido por Santos et al.[20], verificou-se que o requisito do consentimento prévio ao armazenamento de *cookies* é, muitas vezes, olvidado pelos operadores de *websites*. A título de exemplo, vejamos a Figura 1 e 2 abaixo:

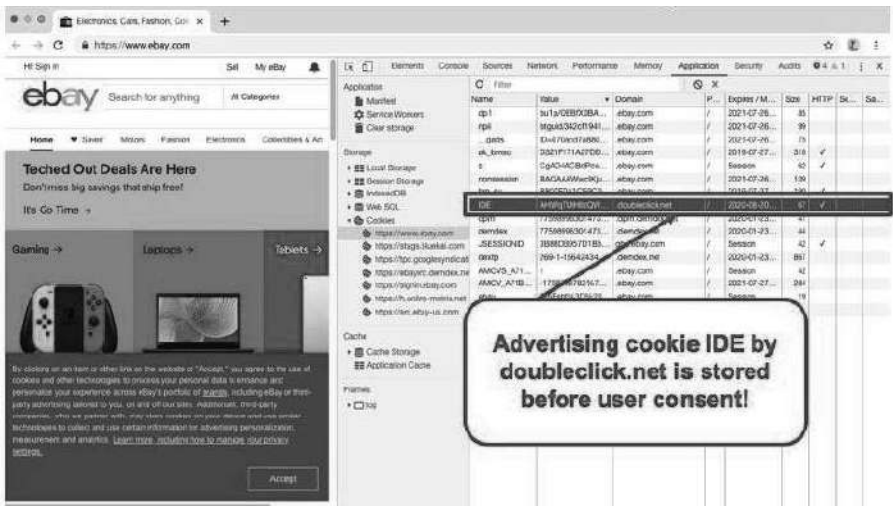
Figura 1 – Acesso ao website <www.ebay.com> em 27 de julho de 2019.
Ao aceder ao referido website, surge uma notificação relativa à utilização de *cookies*.



Fonte: Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

[20] Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

Figura 2 – Violação do requisito de obtenção de consentimento prévio ao tratamento de dados pessoais. Antes de o utilizador prestar o seu consentimento ao tratamento de dados pessoais, é instalado um *cookie* de publicidade, designado "IDE", que armazena um identificador de utilizadores no seu *browser*.



Fonte: Santos, Cristina; Bielova, Nataliia; Matte, Célestin. "Are cookie banners indeed compliant with the law?: Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners." *Technology and Regulation*, dezembro, 2020, pp. 91-135.

Sucede, no entanto, que, na prática, a identificação de situações de incumprimento deste requisito pelos operadores de *websites* constitui uma tarefa bastante complexa e de difícil execução.

Na mesma ordem de raciocínio, o Comité Europeu para a Proteção de Dados esclareceu que a utilização de quadrículas de seleção pré-assinaladas não cumpre com os requisitos impostos pelo RGPD, porquanto não se verifica igualmente a existência de uma "ação clara e afirmativa".

O Comité Europeu para a Proteção de Dados acrescenta ainda que as chamadas co*okie walls* não constituem uma forma legítima de obter consentimento do utilizador por parte dos operadores de *websites*.

Em termos genéricos, as *cookie walls* condicionam o acesso a um website à obtenção de consentimento do utilizador para o tratamento dos seus dados pessoais, pelo que esse mesmo consentimento, a existir, não é

livre. Isto porque as *cookie walls* forçam o consentimento do utilizador a armazenar *cookies* ou a aceder a *cookies* já armazenados em troca do acesso a determinados serviços e funcionalidades, sendo que não existe uma escolha genuína em sentido estrito.

O entendimento suprarreferido a respeito das *cookie walls* veio, portanto, harmonizar as diferentes posições adotadas pelas autoridades de proteção de dados nacionais.

Pese embora a orientação maioritária das autoridades de proteção de dados nacionais fosse já a de que as *cookie walls* não são permitidas ao abrigo do RGPD[21], esta não era, até agora, consensual.

A este respeito, a ICO, autoridade de proteção de dados do Reino Unido, defende que o consentimento que é prestado através de uma *cookie wall* é, com grande probabilidade, inválido[22]. Ainda assim, salienta a importância de conjugar o RGPD com outros direitos fundamentais, nomeadamente a liberdade de expressão e a liberdade de empresa, deixando, desta forma, margem para a possibilidade de, em determinados casos, se considerar válido o consentimento prestado através de uma *cookie wall*.

---

[21] A este respeito, *vide* a orientação da CNIL (*in* "Guidelines on cookies and other trackers", (2019) <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337), bem como da autoridade de protecção de dados *grega* (*in* "Guidelines on Cookies and Trackers" (2020)<http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223>), *irlandesa* (*in* "Guidance note on the use of cookies and other tracking technologies" (2020) <https://www.dataprotection.ie/sites/default/files/uploads/2020-), *holandesa* (*in* "Cookies"(2029) <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#mag-ik-als- organisatie-een--cookiewall-gebruiken-7111> and "Many websites incorrectly request permission to place tracking cookies" (2019) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op- onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies>), *belga* (*in* "Guidance Materials and FAQs on Cookies and Other Tracking Technologies", <https://www.autoriteprotectiondonnees.be/recueillir- valablement-le-consentement-des-personnes--concernees), *alemã* (*in* "On the use of cookies and cookie banners – what must be done with consent (ECJ ruling "Planet49")?" (2019) <www.baden- wuerttemberg.datenschutz.de/zum-einsatz-von-cookies-und-cookie-bannern-was-gilt-es-bei- einwilligungen-zu-tun-eugh--urteil-planet49/>,) e *dinamarquesa* (*in* "Guide on consent" (2019) <www.datatilsynet.dk/media/6562/samtykke.pdf>).

[22] ICO, *Guidance on the rules on use of cookies and similar technologies*, Privacy and Electronic Communications Regulations, 2019.

Por sua vez, a autoridade de proteção de dados austríaca, a 30 de Novembro de 2018, emitiu uma decisão[23] na qual considerou que o consentimento obtido através de uma *cookie wall* utilizada pelo jornal austríaco *Der Standard* foi prestado livremente pelo utilizador. A este propósito, apurou que o referido jornal deu aos utilizadores a opção de: i) aceitar a utilização de *cookies*, dando-lhes acesso total ao *website*; ii) recusar a utilização de *cookies*, o que lhes permitiria um acesso limitado ao *website*; ou iii) pagar uma taxa por uma subscrição mensal sem aceitar a utilização de *cookies*. Como fundamento da sua decisão, a autoridade de proteção de dados austríaca argumentou que, no caso concreto, a *cookie wall* não era proibida, uma vez que as próprias configurações do jornal conferiam ao utilizador diferentes graus de escolha. Posto isto, concluiu que:

1. O jornal apenas procedia ao armazenamento de *cookies* depois de o utilizador prestar o seu consentimento, com base numa decisão plenamente informada;
2. Ao utilizador foi dada a opção de não prestar o seu consentimento, quer através do pagamento de uma subscrição mensal, quer saindo do website do Der Standard. Além disso, considerou ainda aquela autoridade que os preços praticados pelo jornal relativamente à subscrição mensal não eram excessivamente elevados e que, ao prestar consentimento à utilização de *cookies*, o utilizador obtém para si um resultado positivo, que se traduz num acesso ilimitado aos artigos do jornal.

Na mesma senda, a autoridade de proteção de dados espanhola reconhece que o bloqueio do acesso a um determinado *website* constitui uma prática válida se um utilizador não prestar o seu consentimento ao tratamento de dados pessoais. De acordo com esta autoridade:

> "Em certos casos, a não aceitação da utilização de cookies implica ser total ou parcialmente impedido de utilizar o serviço; os utilizadores devem ser devidamente informados desta situação. No entanto, o acesso aos serviços não

[23] Autoridade de protecção de dados austríaca, *Decision on the validity of consent*, 2018.

> pode ser negado devido à recusa de utilização de cookies nos casos em que tal recusa impeça o utilizador de exercer um direito legalmente reconhecido, sendo o website o único meio disponível para o exercício de tais direitos" (tradução livre)[24].

Pese embora a orientação emitida pelo Comité Europeu para a Proteção de Dados tenha deixado claro que as *cookie walls* não são permitidas, poder-se-á concluir que existem ainda algumas zonas cinzentas nesta matéria, designadamente, a título de exemplo, nos casos em que se verifiquem práticas idênticas à adotada pelo jornal austríaco *Der Standard* e descrita *supra*.

Na nossa opinião, ainda que as *cookie walls*, em regra, não constituam uma forma legítima de obter um consentimento verdadeiramente livre do utilizador, cremos que a sua licitude deverá ser analisada caso a caso.

Ora, a este respeito, cumpre notar que a proibição inexorável da utilização de *cookie walls* poderá ser considerada contrária à Diretiva (UE) 2019/2161[25], a qual introduz, no artigo 3.º da Diretiva 2011/83/UE[26], o número 1.º-A, de acordo com o qual: "A presente diretiva [Diretiva 2011/83/UE] aplica-se igualmente caso o profissional forneça ou se comprometa a fornecer conteúdos digitais[27] que não sejam fornecidos num suporte material ou um serviço digital ao consumidor e o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para o fornecimento de conteúdos digitais que

---

[24] Autoridade de protecção de dados espanhola, *Guide on the use of cookies*, 2019, disponível em www.aepd.es/media/guias/guia-cookies.pdf.

[25] Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores.

[26] Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, que altera a Diretiva 93/13/CEE do Conselho e a Diretiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Diretiva 85/577/CEE do Conselho e a Diretiva 97/7/CE do Parlamento Europeu e do Conselho.

[27] O conceito de "conteúdo digital" deve ser interpretado de acordo com o disposto no artigo 2.º, n.º 1, da Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho.

não sejam fornecidos num suporte material ou de um serviço digital, nos termos da presente diretiva, ou para que o profissional cumpra os requisitos legais a que o profissional esteja sujeito, e o profissional não proceda ao tratamento desses dados para quaisquer outros fins.".

Ao abrigo da atual redação da Diretiva 2011/83/UE, o prestador de serviços poderá, em certos casos, e desde que observados os requisitos aplicáveis ao consentimento por força do RGPD, fazer depender o acesso a um determinado conteúdo digital do fornecimento de dados pessoais por parte do consumidor.

A tendência poderá, pois, paulatinamente aproximar-se da prática já adotada pelo jornal austríaco *Der Standard*.

Em face do que antecede, cumpre perguntar: serão as exigências até agora reconhecidas suficientes para assegurar um consentimento livre, informado e esclarecido, em especial face aos mecanismos utilizados pelos operadores de *websites*?

4. Breve análise das práticas utilizadas pelos *websites*

Num estudo levado a cabo por Utz et al.[28], foram reunidas 5 087 notificações de *cookies*, de entre as quais foram aleatoriamente selecionadas 1 000 para formar uma subamostra dos diferentes mecanismos utilizados pelos vários *websites*.

Os resultados, descritos, em termos genéricos, na Tabela 1 *infra*, foram deveras surpreendentes.

---

[28] Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Tabela 1 – Variáveis da interface gráfica das notificações de *cookies* numa subamostra de 1.000 de 5.087 notificações de *cookies* recolhidas em *websites* populares da União Europeia em agosto de 2018.

Position		**Choices (visible)**		**Choices (hidden)**		**Blocking**		**Nudging**	
top	27.0 %	no option	27.8 %	no option	26.3 %	yes	7.0 %	yes	57.4 %
bottom	57.9 %	confirmation	68.0 %	confirmation	59.9 %	no	93.0 %	no	14.8 %
top right	0.2 %	binary	3.2 %	binary	4.0 %			n/a[a]	27.8 %
bottom right	3.0 %	categories	1.0 %	slider	0.2 %				
top left	0 %	vendors	0 %	categories	8.1 %				
bottom left	3.7 %			vendors	1.1 %				
center	7.8 %			other	0.4 %				
other	0.4 %								
Link to privacy policy		**Text: Collection**		**Text: Processor**		**Text: Purposes**			
yes	92.3 %	"cookies"	94.8 %	unspecified	75.5 %	generic	45.5 %		
no	6.6 %	"data"	1.4 %	first party	0.7 %	specific	38.6 %		
other	1.1 %	both	1.6 %	third party	2.6 &	none	16.9 %		
		none	0.9 %	both	21.1 %				
		other	1.3 %	other	0.1 %				

[a] Nudging is not available for "no option" notices.

Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Neste sentido, os autores apuraram que as referidas notificações variavam em larga escala com base em múltiplos fatores, de entre os quais se têm por mais relevantes os seguintes:

- Posição: as notificações de *cookies* são, geralmente, exibidas em sete posições distintas: num dos quatro cantos do browser (6,9 %), no topo (27,0 %), na parte inferior (57,9 %) ou no centro (7,8%).
- Bloqueio (*cookie walls*): Algumas notificações (7,0 %) impedem os utilizadores de entrar e aceder à página enquanto não prestarem o seu consentimento.
- Opções:

    i. Nenhuma opção é dada ao utilizador (27,8%, quando visível, e 26,3%, quando não visível), limitando-se este a ser informado de que o *website* utiliza *cookies*. Por norma, nestes casos, o facto de o utilizador continuar a utilizar esse website é interpretado como um acordo tácito – cfr. Figura 3 abaixo.

ii. Apenas é apresentada a opção de clicar em "OK" ou "Concordo" (são, em bom rigor, notificações de mera confirmação) – cfr. Figura 4 abaixo.
iii. O utilizador pode optar entre aceitar ou recusar a utilização de *cookies* pelo *website* (3,2%, quando visível, e 4,0%, quando não visível) – cfr. Figura 5 abaixo.
iv. O utilizador pode permitir ou não a utilização de *cookies* relativamente a uma determinada categoria individual (1,0%, quando visível, e 8,1%, quando não visível) – cfr. Figura 6 abaixo.

Figura 3

Figura 4

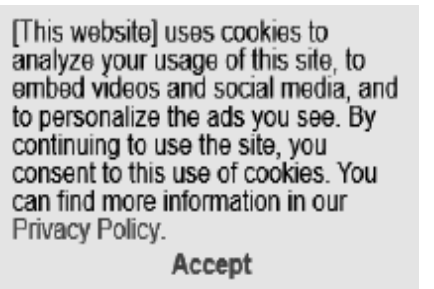
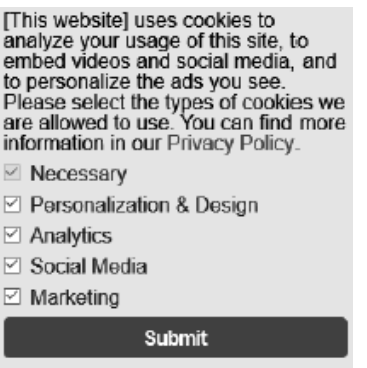


Figura 5

Figura 6



Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

- Texto: por definição, as notificações de *cookies* devem informar o utilizador do *website* de que o mesmo utiliza *cookies* ou tecnologia semelhante, bem como fornecer outras informações relevantes (tais como as finalidades da recolha de dados, o período de duração do armazenamento dos mesmos, entre outros). Ora curiosamente, o utilizador apresenta maior probabilidade de prestar o seu consentimento quando a informação facultada refere meramente a "utilização de *cookies*" (94,8%) do que quando mencionada explicitamente a recolha dos seus dados pessoais (1,4%). Ademais, verifica-se igualmente que nos casos em que as finalidades da utilização de *cookies* são especificadas (a título de exemplo, para publicidade direcionada) existe menor propensão para o utilizador prestar o seu consentimento (38,6%), comparativamente com os casos em que essas finalidades são apresentadas de forma genérica (a título de exemplo, para melhorar a experiência do utilizador) (45,5%).
- Cores e outros elementos manipuladores: frequentemente (e pelo menos em 57,4% dos websites analisados no estudo acima mencionado), as notificações referentes à utilização de *cookies* utilizam cores e outros elementos que estimulam o consentimento – na maior parte das vezes inconsciente – do utilizador. Ora, nas conclusões do Advogado-Geral apresentadas a 21 de Março de 2019, distingue-se entre a atividade que um utilizador prossegue na Internet e o consentimento prestado à utilização de *cookies*, esclarecendo que, sendo situações autónomas e independentes, "ambas as acções devem, oticamente em especial, ser apresentadas em igualdade de condições"[29]. O mesmo se deverá aplicar, por analogia, às situações em que é dada ao utilizador a opção de aceitar ou de recusar a utilização de *cookies*, não devendo ser admitidos mecanismos que induzam o utilizador a selecionar uma determinada opção. De acordo com Gray et al.[30], as técnicas utilizadas poderão consistir

[29] Conclusões do Advogado-Geral Szpunar no caso Planet49, de 21 de março de 2019, para. 66.

[30] Gray, Colin M.; Kou, Yubo; Battles, Bryan; Hoggatt, Joseph e Toombs, Austin L. "The Dark (Patterns) Side of UX Design" (Proceedings of the CHI Conference on Human Factors in Computing Systems ACM, New York, USA, 2018).

em "Falsa Hierarquia" ou em "Manipulação Estética": a "Falsa Hierarquia" espelha uma certa relação de ordenação (visual ou interativa) hierárquica entre uma ou mais opções por referência a outras; por sua vez, a "Manipulação Estética" incita o utilizador a clicar no botão "aceitar" em vez do botão "recusar". De notar que as orientações de algumas autoridades nacionais de proteção de dados reconhecem já a existência deste tipo de mecanismo. Neste sentido, a CNIL[31] designa estes mecanismos que chamam a atenção do utilizador para um determinado ponto do *website* para a desviar de outros pontos relevantes como "Desvio de Atenção". É o caso paradigmático da utilização de um botão verde na opção "Aceitar" ou "Continuar" e na utilização de cores cinzentas ou de tamanhos mais pequenos na opção "Configurações" ou "Ver Mais", levando o utilizador a, inadvertidamente, escolher aquela primeira por lhe parecer, em termos estéticos, preferível.

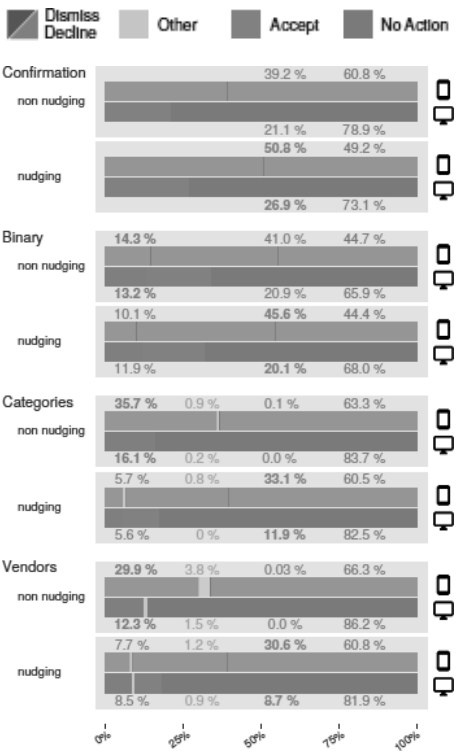
Um estudo igualmente levado a cabo por Utz et al.[32] relativamente a um *website* alemão tornou claro o forte impacto que o recurso a estes mecanismos manipuladores produz na escolha dos utilizadores. A título de exemplo, e com base no Gráfico 1 *infra*, a respeito das notificações que solicitaram apenas a confirmação da utilização de *cookies* em que se adotaram alguns dos referidos elementos de manipulação estética ("*nudging*"), verificou-se uma maior percentagem (50,8% no dispositivo móvel, 26,9% no computador) de utilizadores a clicar em "Aceitar". Em contraposição, apurou-se que, em relação a essas mesmas notificações, não havendo recurso a mecanismos de manipulação, a percentagem de utilizadores a clicar em "Aceitar" diminui, no dispositivo móvel, para 39,2% e, no computador, para 21,1%.

---

[31] CNIL. *Shaping Choices in the Digital World, From dark patterns to data protection: the influence of UX/UIdesign on user empowerment*, 2019, disponível em: <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world>.pdf, consultado em 13 de novembro de 2020.

[32] Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

Gráfico 1 – Escolhas dos utilizadores relativamente à utilização de cookies num website alemão.



Fonte: Utz, Christine; Degeling, Martin; Fahl, Sascha; Schaub, Florian; Holz, Thorsten. "(Un)informed Consent: Studying GDPR Consent Notices in the Field", in *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications* Security, novembro 2019, pp. 973–990.

É, pois, indubitável que o destaque da cor do botão correspondente à aceitação da utilização de *cookies* e as demais técnicas utilizadas pelos operadores de *websites* suscitam algumas dúvidas quanto à prestação de um consentimento devido e totalmente esclarecido pelo utilizador.

No âmbito do artigo acima referido, e com base nos dados constantes da Tabela 1, os autores concluíram que a maioria das notificações de consentimento para a utilização e armazenamento de *cookies* são colocadas na parte inferior do ecrã (58%); não bloqueiam o acesso ao website (93%);

não oferecem outras opções para além de um botão de confirmação (68%); e tentam induzir os utilizadores a consentir na utilização de *cookies* (57%).

Ademais, verificaram que, quanto maior o número de opções oferecidas ao utilizador nas notificações de *cookies*, maior a probabilidade de que estes recusem a utilização de *cookies*.

Em suma, os autores concluem que se os operadores de *websites* cumprissem na íntegra os princípios de proteção de dados consagrados no RGPD e a exigência de um consentimento informado, prestado com base em informação explícita relativa às finalidades do tratamento de dados pessoais, menos de 0,1% dos utilizadores consentiriam na utilização de *cookies* de terceiros.

5. Regulamento *ePrivacy*: uma nova realidade?

A proposta de Regulamento *ePrivacy*[33], apresentada pela primeira vez em 2017, pretende substituir a atual Diretiva *ePrivacy*. Embora inicialmente estivesse programado que a entrada em vigor do Regulamento *ePrivacy* coincidisse com a do RGPD, cedo se percebeu que a divergência verificada entre as posições adotadas pelos Estados-Membros não permitiria dar cumprimento a essa expectativa.

Nesta senda, um relatório de progresso emitido pelo Conselho (doc. 14054/19 da Presidência finlandesa de 18 de Novembro de 2019[34]) esclareceu que o Regulamento continua a dividir os Estados-Membros, e que múltiplas alterações foram sugeridas e debatidas até agora, não tendo sido ainda encontrado um compromisso.

No dia 21 Fevereiro de 2020 foi publicada uma versão revista[35] do Regulamento *ePrivacy*, verificando-se uma alteração substancial a nível do regime aplicável à utilização de *cookies*.

---

[33] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações electrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações electrónicas).

[34] Documento do Conselho da União Europeia n.º 14054/19, de 18 de novembro de 2019, disponível em https://data.consilium.europa.eu/doc/document/ST-14068-2019-INIT/en/pdf, acedido a 14 de novembro de 2020.

[35] Documento do Conselho da União Europeia n.º 14068/19 + COR 1, de 21 de fevereiro de 2020, disponível em <https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf>, acedido a 14 de novembro de 2020.

Destarte, na sua versão inicial, o artigo 8.º da proposta de Regulamento *ePrivacy* estabelecia, como regime-regra, a proibição de utilização de *cookies*, exceto:

a. Se forem necessários exclusivamente para assegurar a transmissão de uma comunicação eletrónica através de uma rede de comunicações eletrónicas; ou
b. Se o utilizador final tiver dado o seu consentimento; ou
c. Se forem necessários para prestar um serviço solicitado pelo utilizador final; ou
d. Se forem necessários para a medição de audiência, desde que tal medição seja efetuada pelo prestador do serviço da sociedade de informação solicitado pelo utilizador final.

Ora, a versão revista vem introduzir as seguintes modificações:

1. A respeito dos *cookies* necessários para a medição de audiência, prevê-se que tal medição pode ser efetuada igualmente por terceiros, ou por terceiros conjuntamente, em nome de um ou mais fornecedores do serviço da sociedade da informação, desde que cumpridos os requisitos previstos no artigo 28º, ou do artigo 26.º, quando aplicável, do RGPD.
2. Foram acrescentados dois novos fundamentos que legitimam o armazenamento de *cookies*:

    a. comunicação de uma emergência;
    b. interesses legítimos prosseguidos por um prestador de serviços, excepto quando tal interesse seja anulado pelos interesses ou direitos e liberdades fundamentais do utilizador. A este respeito, considera-se que os interesses do utilizador final se sobrepõem aos interesses do prestador de serviços quando: i) o utilizador final é uma criança ou (ii) quando o prestador de serviços processa, armazena ou recolhe dados para determinar a natureza e as características do utilizador final ou para construir um perfil individual do utilizador final ou (iii) para o processamento, armazenamento ou recolha de dados subsumíveis a categorias especiais de dados pessoais, nos termos do nº 1 do artigo 9º do RGPD.

Em especial, relativamente ao consentimento, a proposta inicial do Regulamento *ePrivacy* previa já a aplicação das condições previstas no artigo 4.º, n.º 11, e no artigo 7.º do RGPD.

Contudo, e conforme fora reconhecido pelo Comité Europeu para a Proteção de Dados[36], "o conceito de consentimento, tal como utilizado na Diretiva 95/46/EC e na Diretiva *ePrivacy* até à data, tem evoluído" (tradução livre), sendo que "no que diz respeito à Diretiva *ePrivacy* em vigor, o Comité Europeu para a Proteção de Dados sublinha que as referências à Diretiva 95/46/CE, revogada, devem ser interpretadas como referências ao RGPD" (tradução livre), o que "também se aplica a referências ao consentimento na atual Diretiva 2002/58/CE (...)" (tradução livre).

Sucede que tal já resultava do próprio RGPD: o artigo 94.º prevê expressamente que as remissões para a diretiva revogada são consideradas remissões para o RGPD.

Neste sentido, ao consentimento para a utilização e armazenamento de *cookies* já eram aplicáveis, previamente à apresentação da proposta do Regulamento *ePrivacy*, os requisitos e exigências previstos no RGPD[37].

A este respeito, Degeling et al.[38] realizaram um estudo comparando a informação apresentada aos utilizadores de 6.500 websites da UE antes e depois da entrada em vigor do RGPD, tendo observado um aumento de 6% na adoção de notificações de *cookies* por parte dos *websites* analisados.

A verdade é que os requisitos concretamente aplicáveis ao consentimento e ao armazenamento de *cookies* não se encontram especificamente concretizados, não tendo ainda o TJUE tido oportunidade de explicitamente se pronunciar a respeito das muitas práticas que ainda são adotadas pelos operadores de *websites* e que suscitam dúvidas quanto à validade do consentimento prestado pelo utilizador.

---

[36] EDPB. *Guidelines 05/2020 on consent under Regulation 2016/679,* de 4 de maio de 2020, disponível em <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, acedido em 14 de novembro de 2020.

[37] Cumpre referir que, ao abrigo do disposto no n.º 11 do artigo 4.º do RGPD, consentimento é a "manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento".

[38] Degeling, Martin; Utz, Christine; Lentzsch, Christopher; Hosseini, Henry; Schaub, Florian; e Holz, Thorsten, *We value your privacy ... now take some cookies: Measuring the GDPR's impact on web privacy, in* NDSS, 2019.

Conclusão

Em face do exposto, é manifesto que existe ainda um longo caminho a trilhar.

Ora, são vários os cenários em que resulta evidente que, em virtude da multiplicidade de técnicas utilizadas pelos operadores de *websites* – em muitos casos verdadeiramente manipuladoras –, o consentimento para o armazenamento de *cookies* não é totalmente livre, informado e esclarecido.

A título de exemplo, a mera remissão para uma Política de Privacidade ou para os Termos e Condições aplicáveis a determinado *website* não cumpre o requisito de fornecimento de informação, em linguagem clara e simples, compreensível a um utilizador normal.

Como vimos, também a indução do utilizador a autorizar a utilização ou armazenamento de *cookies* não consubstancia um consentimento totalmente livre e esclarecido. Em especial, é indubitável que a hierarquização e a distinção, designadamente com recurso a diferentes cores, entre as opções que correspondem à aceitação ou não da utilização de *cookies* produz um grande impacto na tomada de decisão (em muitos casos inconsciente) por parte dos utilizadores.

Ainda assim, têm sido dados passos relevantes nesta matéria, em especial com o reconhecimento de que as conhecidas *cookie walls* e as quadrículas de seleção pré-preenchidas não consubstanciam um consentimento válido à luz do RGPD, salvos os casos expressamente referidos *supra*.

Contudo, não existe uma forma legalmente prevista aplicável ao pedido de consentimento. O considerando 17 da Diretiva *ePrivacy* estabelece que o consentimento de um utilizador pode ser dado por qualquer método apropriado. Neste sentido, os operadores de *websites* são livres de utilizar ou desenvolver mecanismos de recolha de consentimento que se lhes afigurem mais apropriados, devendo, no entanto, observar um requisito: o consentimento tem de ser considerado válido ao abrigo da legislação da UE. O que, na verdade, tem sido pouco respeitado.

Indubitavelmente, muitas das práticas adotadas pelos operadores de *websites* suscitam dúvidas quanto à validade do consentimento prestado pelo utilizador à luz das regras impostas pelo RGPD.

Contudo, conforme as conclusões do estudo levado a cabo por Utz et al., *supra* citado, verificou-se que se os operadores de *websites* cumprissem

escrupulosamente os princípios e regras em matéria de proteção de dados consagrados no RGPD, menos de 0,1% dos utilizadores consentiriam a utilização de *cookies* de terceiros, o que, naturalmente, teria grande impacto na atividade destes terceiros, nomeadamente ao nível da publicidade e marketing digital e, em particular, dos mecanismos de *tracking*, *retargeting* e marketing de comportamento (*behavorial marketing*), os quais, hoje em dia, são da maior relevância para o sector de *e-commerce*.

Neste sentido, impõe-se estabelecer um equilíbrio (necessário) entre os princípios da proteção de dados pessoais e os interesses económicos das empresas, sob pena de que a excessiva proteção, quer de um, quer de outro, implique, *à la longue*, a limitação de outros direitos fundamentais. Aliás, a introdução dos interesses legítimos do prestador de serviços como fundamento para o armazenamento de *cookies* na nova versão do Regulamento *ePrivacy*, publicada no dia 21 de fevereiro de 2020, parece já caminhar nessa direção.

O responsável pelo tratamento de dados (pessoais) gerados pelo *Whistleblowing*

Patrick de Pitta Simões[*]

Resumo: Nas últimas décadas tem sido recorrente a divulgação pública de casos de erros graves, má administração, ilegalidades ou de corrupção. De modo a salvaguardar-se a proteção dos dados pessoais dos indivíduos envolvidos e a imagem das organizações a que pertencem, tem-se implementado por todo o mundo o *Whistleblowing*. O nosso país não é exceção, seja por existir previsão geral na Lei n.º 19/2008, de 21 de janeiro, e em leis setoriais (nomeadamente comercial, bancário-financeira, seguradora ou na área da saúde), seja pela Deliberação n.º 765/2009, de 21 de setembro (Linhas de Ética), da Comissão Nacional de Proteção de Dados. Não obstante, a União Europeia estabeleceu, através da Diretiva 2019/1937, de 23 de outubro, normas mínimas comuns para a proteção dos denunciantes de violações do direito da União. Este texto pretende fazer um sucinto enquadramento sobre o *Whistleblowing* nacional, indagando, à data, quem poderá ser responsável pelo tratamento de dados pessoais gerados pelo *Whistleblowing.*

Palavras-chave: *Divulgação pública, Whistleblowing, Portugal, Diretiva 2019/1937, responsável pelo tratamento de dados.*

---

[*] Investigador pelo Centro de Investigação e Desenvolvimento sobre Direito e Sociedade (CEDIS), Árbitro (área administrativa) e Formador Certificado. Doutorando em Direito e Segurança pela Nova *School of Law*, Mestre em Auditoria pelo Instituto Politécnico de Lisboa, Pós-graduado em áreas do Direito Público do Instituto de Ciências Jurídico-Políticas, Especialista em Direito Administrativo e Licenciado em Direito pela Universidade de Lisboa, Licenciado em Geografia e Planeamento Regional pela Universidade Nova de Lisboa. Este texto é uma adaptação, atualização e aditamento, de excertos de subcapítulos da dissertação de mestrado do autor (Os limites da Auditoria Interna – o perfil do Auditor e o *Whistleblowing*). Foi empregue o Novo Acordo Ortográfico, determinado pela Resolução n.º 8/2011 do Conselho de Ministros, publicada no Diário da República, 1.ª série, de 25 de janeiro de 2011, à exceção das transcrições de legislação ou textos anteriores àquele, ou de autores que não tenham aderido ao mesmo.

Abstract: During the last decades, the public disclosure of serious errors, illegalities, wrongdoings, or corruption cases, has been more frequent. To safeguard the protection of the personal data from those involved and the corporate image of organisations to which they belong, Whistleblowing has been implemented all over the world. Portugal is no exception, either because there is a general prediction in Law No. 19/2008, of 21 January, and in sectoral laws (namely commercial, banking-financial, insurance or in the area of health), or by Resolution No. 765 / 2009, of 21 September (Ethics Lines), of the National Data Protection Commission. Nevertheless, the European Union established, through Directive 2019/1937, of 23 October, common minimum standards for the protection of whistleblowers reporting violations of European Union law. This text aims to provide a framework of Whistleblowing, at the national level, and, considering its implementation has not yet been massively verified (which is indicated to happen), to boldly inquire, who may be the responsible for the processing of personal data generated by Whistleblowing.

Keywords: *Public disclosure, Whistleblowing, Portugal, Directive 2019/1937, responsible for handling reports.*

Enquadramento geral

Numa Sociedade de Risco[1] e informação (de *fake news*[2] e infodemia também), tem-se regularmente conhecimento, através de divulgações públicas, de casos suspeitos de malversação ou de corrupção e infrações conexas.

Como forma de mitigar o julgamento público e os danos reputacionais adjacentes incrementou-se, nos Estados Unidos da América (EUA), o *Whistleblowing* (canais específicos para a comunicação de irregularidades que permitem a proteção de denunciantes), que por sua vez, através da influência dos seus mercados bolsistas, tem sido fomentado um pouco por todo o mundo.

Em Portugal, a Comissão do Mercado de Valores Mobiliários (CMVM), através da sua Recomendação 10-A, de novembro de 2005, designada por Comunicação de Irregularidades, incentivou as sociedades empresariais

---

[1] Como descrita e desenvolvida por Beck, Ulrick, *Sociedade de risco mundial: em busca da segurança perdida*, Edições 70 (Grupo Almedina), 2015.

[2] Tradução livre do autor: distorção da informação (realidade), notícias falsas, ou simplesmente, desinformação.

a adotarem uma política de comunicação de irregularidades que mencionasse os meios internos através dos quais as comunicações podiam ser feitas, bem como se identificasse as pessoas com legitimidade para aceitá-las.

Por sua vez, a União Europeia (UE) criou um grupo de trabalho, composto pelas Autoridades Nacionais de Proteção de Dados que, no seu Parecer n.º 1/2006, de 1 de fevereiro, referindo a sua falta de competência e as diferenças histórico-culturais e sociojurídicas de cada Estado-Membro, elaborou um parecer sobre a aplicabilidade do *Whistleblowing*, limitando-o a áreas económico-financeiras e excluindo o direito laboral e penal.

Posteriormente, através da Lei n.º 19/2008, de 21 de abril, o legislador nacional aprovou medidas de combate à corrupção que estabelecem garantias para os trabalhadores que denunciem o cometimento de infrações de que tiverem conhecimento no exercício das suas funções.

No art. 4.º desta Lei estabeleceram-se garantias que se aplicavam, inicialmente, aos trabalhadores da Administração Pública e de empresas do sector empresarial do Estado, e que a partir de 2015 foram alargadas para os trabalhadores do setor privado, com as alterações introduzidas pela Lei n.º 30/2015, de 24 de abril (que procedeu à trigésima quinta alteração ao Código Penal; sexta alteração à Lei n.º 34/87, de 16 de julho; primeira alteração à Lei n.º 20/2008, de 21 de abril; primeira alteração à Lei n.º 50/2007, de 31 de agosto; e primeira alteração à Lei n.º 19/2008, de 21 de abril, no sentido de dar cumprimento às recomendações dirigidas a Portugal em matéria de corrupção pelo Grupo de Estados do Conselho da Europa contra a Corrupção, pelas Nações Unidas e pela Organização para a Cooperação e Desenvolvimento Económico).

No encadeamento de políticas de *compliance*[3] e do normativo *soft law*, a Comissão Nacional de Proteção de Dados (CNPD), em consequência do elevado número de notificações de tratamento de dados pessoais

[3] Há quem lhe intitule política antifraude, linhas de alerta, comunicação de irregularidades ou canais de reporte. Para mais desenvolvimentos *vide* Pitta Simões, Patrick, *Os limites da Auditoria Interna – O perfil do Auditor e o Whistleblowing*, dissertação de mestrado defendida no Instituto Superior de Contabilidade e Administração de Lisboa (ISCAL), 2017, p. 67. Disponível em: <http://hdl.handle.net/10400.21/8921>.

gerados pelas comunicações internas de atos de gestão financeira irregular[4], deliberou princípios orientadores (Linhas de Ética – cf. designa a Deliberação n.º 765/2009, aprovada a 21 de setembro, de ora avante Deliberação) aplicáveis a este tipo de tratamento, de modo a salvaguardar a privacidade dos intervenientes.

Com a Deliberação, além da previsibilidade de garantias aos denunciantes, passa a haver regras sobre direitos e limites para o tratamento de dados pessoais com aquela finalidade.

Estabelecem-se limites específicos de âmbito objetivo (o sistema de denúncia restringe-se aos domínios dos controlos internos, da contabilidade, da auditoria, do crime bancário e financeiro e da luta contra a corrupção), subjetivo (apenas as pessoas relacionadas com os tais domínios, que pratiquem atos de gestão, podem ser alvo de denúncia), procedimental (a sua natureza deve ser subsidiária à atividade regular da entidade) e de autonomia da vontade (obrigatoriedade da denúncia só nos casos em que a lei penal e processual penal o determina).

Antes do Regulamento Geral de Proteção de Dados (RGPD), a CNPD tinha um poder de controlo prévio deste tipo de tratamento de dados, pelo que as organizações que queriam implementar um sistema de *Whistleblowing*, tinham de pedir autorização à CNPD para criarem o mecanismo (cf. alínea a) do n.º 1 do art. 28.º, *ex vi*, n.º 2 do art. 8.º da Lei n.º 67/98, de 26 de outubro).

Por último, face à grande influência dos mercados financeiros e bolsa de valores dos EUA, com o surgimento de mais *Leaks* (comunicação ou divulgação não autorizada de informação sensível – comprometedora) a envolverem organizações e cidadãos europeus[5], com a maior sensibilização

---

[4] Debatendo este tipo de denominação, Rebelo de Sousa; Marcelo, e Salgado de Matos, André, *Direito Administrativo Geral – Actividade Administrativa*, Tomo III, 2ª edição, Publicações Dom Quixote, 2010, p. 55, explicam que "[a] irregularidade [será] a consequência reservada pela ordem jurídica para os actos que padeçam de ilegalidades pouco graves [,] (...) insusceptíveis de afectar de forma essencial a produção de efeitos estáveis pelos actos viciados em causa (...)". Prosseguem dizendo que poderão ser vícios competenciais e formais, mas nunca materiais ou funcionais.

[5] Como, por exemplo, o *Luxemburgo Leaks* (*Lux Leaks*), em que se soube, em novembro de 2014, detalhes de operações secretas de grandes empresas multinacionais para evitar o pagamento de tributos.

social[6] e consciencialização política, a UE publicou a 26 de novembro de 2019, no seu Jornal Oficial, a Diretiva 2019/1937, de 23 de outubro, do Parlamento Europeu e do Conselho, relativa à proteção das pessoas que denunciem violações do direito da União (Diretiva *Whistleblowing*, de ora em diante, designada apenas por Diretiva). Esta visa reforçar a aplicação do direito e das políticas da União em domínios específicos, estabelecendo normas mínimas comuns para um nível elevado de proteção dos denunciantes (cf. art. 1.º).

Com este texto traça-se, num primeiro momento um conceito amplo e complexo de *Whistleblowing* e *Whistleblower*, tal como é o assunto e podem ser os seus sujeitos, bem como se procurará, simplificar a sua dialética.

Num segundo momento, pensando na dificuldade que as organizações, públicas e privadas, terão na implementação efetiva do sistema de denúncias, abordar-se-á quem poderá ser responsável por este cumprimento normativo e, consequentemente, dos dados pessoais a tratar.

Em seguida, dar-se-á conta de algumas das características das entidades que pediram autorização à CNPD para a implementarem o *Whistleblowing*, tal como da existência deste em quatro das maiores empresas de auditoria. Refira-se que este texto reflete uma síntese do estudo, mais vasto, realizado para a defesa da dissertação de mestrado do autor, que aborda os limites da auditoria (interna).

Numa quarta fase enunciam-se deveres implícitos: aos cidadãos (ainda que numa ótica de providência de cautelas); aos intervenientes no procedimento e processo de *Whistleblowing* (duas componentes distintas), como destaque para o responsável pelo tratamento daquele (e as suas entidades); e aos Estados.

Por fim, tecem-se algumas considerações finais quanto aos desafios eminentes com que o legislador nacional se depara(rá), concluindo que há ainda questões cruciais por refletir e encontrar soluções.

---

[6] Tais como a Movemos a Europa (*WeMoveEurope*) que organizou uma petição internacional para a existência de uma lei a nível da UE que protegesse os denunciantes; ou a *Transparency International* uma associação com várias filiais, entre elas, uma portuguesa que tem como missão deter a corrupção e promover a transparência, a responsabilidade e a integridade da sociedade.

1. O conceito de *Whistleblowing* e *Whistleblower*

O que será afinal, no espectro nacional, o *Whistleblowing*? A Deliberação diz-nos que é um sistema que se traduz na criação, nas empresas, de condições para a denúncia de comportamentos, fraudulentos ou irregulares, capazes de afetar seriamente a sua atividade. Estas condições são normalmente designadas por canais (de denúncia), comunicação ou reporte (de irregularidades).

Esse sistema, também designado alternadamente pela Deliberação de mecanismo ou dispositivo, tem como objetivo estabelecer direitos e deveres laborais para os denunciantes, denunciados e indiretamente para os responsáveis pelo tratamento das denúncias que, em última instância, são os mais interessados na descoberta e/ou apuramento de factos, que muito provavelmente de outro modo não iriam saber.

O enquadramento de aplicação da Diretiva é bastante claro: informações sobre violações em contexto profissional [este é definido na alínea 9) do art. 5.º da Diretiva].

Os responsáveis pelo tratamento das denúncias estão incumbidos da receção e seguimento: análise, decisão e conservação daquelas, se for caso disso. O seguimento é definido na alínea 12) do art. 5.º da Diretiva, que se passa a transcrever: "qualquer medida tomada por quem recebe uma denúncia ou por uma autoridade competente, para aferir da exatidão das alegações constantes da denúncia e, se for caso disso, para resolver a violação denunciada, inclusive através de medidas como um inquérito interno, uma investigação, a ação penal, uma medida de recuperação de fundos ou o arquivamento".

Deste modo, podemos, desde já, perceber que o responsável pelo tratamento é também responsável pelo seguimento da denúncia. Assim sendo, pode ser denominado como responsável pelo seguimento da comunicação da informação sobre violações [que, por seu turno, está definida na alínea 2) do art. 5.º da Diretiva].

Tenha-se em conta que o considerando 57 enuncia que o seguimento poderá incluir, por exemplo, o encaminhamento para outros canais ou procedimentos no caso de denúncias que afetam exclusivamente os direitos individuais do denunciante, o arquivamento por insuficiência de elementos de prova ou por outros motivos, a abertura de um inquérito interno e, eventualmente, as conclusões deste e as eventuais medidas

tomadas para resolver o problema identificado, o encaminhamento para uma autoridade competente para investigação mais aprofundada, na medida em que essas informações não prejudiquem o inquérito interno ou a investigação, nem afetem os direitos da pessoa visada. Deverá ser possível solicitar ao denunciante que preste mais informações, no decurso da investigação, embora não deva ser obrigatório prestar essas informações (vide o considerando 66).

Da conjugação da Deliberação e da Diretiva, sem se abordar outros diplomas legais, tais como os mencionados na Diretiva, além de poder ser confundido com o ato ou a ação em si de denunciar (*blow the whistle*) ao abrigo de uma proteção legal, por *Whistleblowing* deve entender-se um sistema[7] que possibilita, de forma voluntária e não obrigatória, a existência (ou suscetibilidade) de denúncias[8] internas[9], nas organizações públicas e privadas[10], ou de denúncias externas, para as autoridades competentes[11] (incluindo em último recurso a divulgação pública)[12], de condutas[13] irregulares ou violações ao Direito[14], num contexto

---

[7] Conjunto de meios (vias possíveis de denunciar), tais como caixas físicas (simples de depósito ou correio postal), correio eletrónico (vulgo *email*), telefone ou outros sistemas de mensagem de voz e, a pedido do denunciante, reunião presencial (cf. considerando 53; n.º 2 do art. 9.º; n.º 2 do art. 12.º; alínea b) do art. 13.º ou art. 18.º da Diretiva). Em sistemas, que se crê poderem designar-se por *Whistleblowing* 2.0 (segunda geração), poderão ser concebidos formulários eletrónicos disponibilizados em *intranet* (dentro da organização) ou na *internet* (*online* – que permite o acesso a não trabalhadores), e por isso também acessíveis via telemóvel, ou ainda como uma opção de uma aplicação (vulgo *app*) de telemóvel inteligente (também conhecidos por *smart phone*).

[8] Ou comunicações de informações, cf. alínea 3) do art. 5.º da Diretiva. Esta expressão tem uma conotação, político-cultural, mais neutra.

[9] Preferencialmente (cf. n.º 2 do art. 7.º da Diretiva).

[10] Com 50 ou mais trabalhadores, cf. se depreende do considerando 48 conjugado com o n.º 2 do art. 26.º, com a ressalva dos casos mencionados no considerando 50 da Diretiva.

[11] Cf. definido na alínea 14) do art. 5.º e com as competências prevista no art. 11.º da Diretiva.

[12] Cumpridos os pressupostos de tentativa de recurso aos meios internos e, ou, às autoridades competentes, cf. art. 15.º da Diretiva.

[13] Comportamento por ação ou omissão, doloso ou negligente.

[14] Cf. terminologia usada pela Deliberação, mas também por duas vezes referida na Diretiva, considerando 75 (denúncia de irregularidades) e 89 (denunciar irregularidades). Será discutível se a palavra irregularidades não quererá dizer na prática infrações (disciplinares, ainda que geradoras de uma simples admoestação ou repreensão escrita, ou mesmo

profissional[15]; assegurando o direito à defesa do denunciante[16], de boa fé[17] ou convicto de tal (na procura de um interesse coletivo da organização ou interesse público), de pessoas colaterais a este[18] e do denunciado[19]; bem

---

contraordenacionais), ver-se-á o que prática, jurisprudência, dirá sobre este conceito, aparentemente, indeterminado. A palavra irregularidade é usada pela Deliberação, enquanto que a palavra violação é usada pela Diretiva, mas ambas convergem para o significado de atos ou procedimentos errados, incorretos, ilegais ou ilícitos. *Cum grano salis*, entende-se que, numa definição, fará sentido que as irregularidades ou violações sejam ao Direito (num todo) e não a domínios (específicos, ainda que mencionados) tanto na Deliberação, como na Diretiva. Havendo a possibilidade de cada Estado-Membro alargar os domínios de aplicação da Diretiva, que são mais amplos que os da Deliberação (cf. arts. 2.º e 3.º da Diretiva), bem como algumas matérias não serem afetadas pela Diretiva, não se considera prudente delimitar ou especificá-los numa definição.

[15] Relação laboral ou relação comercial (quanto a esta vide, entre outros, o considerando 59 da Diretiva), ocasional ou duradoura; passada, presente ou futura (cf. se depreende do proémio do n.º 1, n.º 2 e proémio do n.º 3 do art. 4.º e, também, da alínea 9) do art. 5.º da Diretiva).

[16] Interno ou externo, atual ou ex-colaborador da organização visada que é alvo de denúncia (a que pertence ou pertencia o denunciado, pessoa singular referida na denúncia como autora da violação ou que a esta esteja associada, cf. alínea 10) do art. 5.º da Diretiva – repare-se que nem a Deliberação, nem a Diretiva mencionam este aspeto temporal relativamente ao denunciado –, ou mesmo a pessoa coletiva, num todo, numa lógica de responsabilidade objetiva), que no decurso da sua atividade profissional ou por causa desta descobre irregularidades ou violações ao direito da União.

[17] Tenha-se em conta que há diplomas legais da UE, relativos à segurança dos transportes que preveem também a proteção dos trabalhadores que denunciem erros por si cometidos de boa-fé contra atos de retaliação ("cultura justa"). Vide considerando 9 da Diretiva.

[18] A Diretiva introduz "figuras jurídicas colaterais", designadamente o facilitador (pessoa que auxilie – uma testemunha ou "coautor mitigado" – definido na alínea 8) do art. 5.º da Diretiva) ou o terceiro [tais como um colega ou um familiar do denunciante, cf. alínea b) do art. 4.º, ou testemunha, cf. considerando 76 e alínea a) do n.º 1 do art. 9.º da Diretiva] que sabe da denúncia por intermédio daquele ou sofre alguma represália (ato ou omissão), independentemente do seu grau de envolvimento na denúncia ou de conhecimento (o caso claro das entidades jurídicas – cf. identificadas na alínea c) do n. 4 do art. 4.º da Diretiva), por ter algum tipo de relação, pessoal ou profissional com o denunciante. Admitindo que haja prova testemunhal, com diferentes níveis de envolvimento (conhecimento) da testemunha com a denúncia, ou diversas fases em que possa intervir no *Whistleblowing*, não será tão clara a fronteira com as figuras de terceiro, de facilitador ou mesmo de denunciante em coautoria.

[19] "Pessoa visada" que, cf. designado pela alínea 10) do art. 5.º, se define por ser: uma pessoa singular ou coletiva referida na denúncia, ou na divulgação pública, como autora da violação ou que a esta seja associada.

como estabelece regras[20] ao responsável pelo tratamento da denúncia, que não deverá ser o visado dos factos[21], direta ou indiretamente, constantes na denúncia[22].

De forma mais simples, o *Whistleblowing* é um conjunto de canais (interno e externo) de reporte ou comunicação (de informações ou de denúncias), que sinalizam ou alertam (chamam atenção) para irregularidades ou violações a regras[23] ou ao Direito da União Europeia (cf. art. 2.º da Diretiva) e de cada Estado-Membro, que pode ser diferente dos demais, cf. n.º 2 do art. 2.º e art. 3.º da Diretiva (*hard law*).

O *Whistleblowing* deve ser também encarado como um dispositivo instrumental (com canais internos e externos) e procedimental (de direitos, deveres e garantias). É no fundo um conjunto de meios técnicos (tendencialmente eletrónicos e informatizados) e jurídicos, proporcionados num ambiente profissional, que devem visar a proteção dos seus intervenientes (denunciantes, denunciados e também pessoal responsável pelo tratamento da denúncia, tais como a confidencialidade e um procedimento e processo equitativo e justo – entende-se, como melhor se verá no capítulo 4, que procedimento e processo serão duas fases distintas do sistema de *Whistleblowing*).

E quem será afinal *Whistleblower*? Curiosamente a Diretiva na sua redação em inglês apenas refere esta palavra nos seus considerandos, usando a expressão *reporting person* para aquilo que nós, na versão portuguesa, lemos na alínea 7) do art. 5.º: denunciante.

---

[20] Processuais (nomeadamente, imparcialidade, justiça e rigor) e procedimentais (designadamente, prazos de retorno de informação e de conservação).

[21] Reais (passados ou presentes) ou potenciais, cf. alínea 2) do art. 5.º da Diretiva.

[22] De acordo com alínea 3) do art. 5.º da Diretiva, entende-se por denúncia ou comunicação de informações, denunciar ou comunicar informações: a comunicação verbal ou escrita de informações sobre violações. Os ingleses utilizam a palavra *report*, os espanhóis, *denuncia* ou *denunciar*; os franceses *signalement* ou *signaler*; os italianos *segnalazione* ou *segnalare*; e os romenos *raportare* (cf. alínea 3) do art. 5.º da Diretiva, em cada respetivo idioma). Daqui se observa que não é uniforme a utilização de uma palavra, se se fizer uma tradução, *ipsis verbis*, de cada língua para o português (e destas, se excluirmos o inglês, a família linguística românica, também conhecida por línguas latinas).

[23] Diretrizes (*guidelines*), linhas gerais, linhas estratégicas, padrões ou estruturas de enquadramento (*framework*), melhores práticas do setor (guias de boas práticas) ou, ainda, códigos de conduta. Todos estes instrumentos normativos fazem parte de um leque de autorregulação (*soft law*) que tem sido usado pelas organizações.

Dito isto, recorrendo à definição incita nesta alínea, denunciante é uma pessoa singular que comunica ou divulga publicamente informações sobre violações obtidas no âmbito das suas atividades profissionais.

Podem ser denunciantes: funcionários públicos[24], não assalariados, titulares de participações sociais e pessoas pertencentes a órgãos de administração, de gestão ou de supervisão de empresas (incluindo membros não executivos), assim como voluntários e estagiários, remunerados ou não remunerados, ou quaisquer pessoas que trabalhem sob a supervisão e a direção de contratantes, subcontratantes e fornecedores (cf. n.º 1 do art. 4.º, que deve ser conjugado com os arts. 45.º, relativo à circulação de trabalhadores, e 49.º referente à liberdade de estabelecimento, do Tratado de Funcionamento da UE, bem como o capítulo VI – medidas de proteção – da referida Diretiva).

Assim, repara-se que os denunciantes podem denunciar a qualquer momento, antes, durante ou depois da relação profissional ter sido estabelecida, não estando previsto nenhum regime de caducidade ou prescrição para a comunicação (denúncia) ou divulgação da informação.

2. Quem pode ser responsável pelo tratamento do *Whistleblowing*?

Por mais informatizado e auto mecanizado que venha a ser o sistema de *Whistleblowing*, e por isso se defende que estamos já perante uma segunda geração face aos meios mais convencionais já mencionados, este dispositivo que visa garantir a integridade e transparência das entidades, carece que haja uma intervenção humana para organizar e decidir: o responsável pelo mecanismo.

Feito este enquadramento, normativo e conceptual, procurar-se-á agora identificar quem será o responsável pelo tratamento de dados pessoais gerados pelo *Whistleblowing*, isto é, quem deverá manusear e geri-lo.

Para o efeito, recorrer-se-á à Deliberação e à Diretiva do *Whistleblowing*, com algumas abordagens ao RGPD, dando por fim, no capítulo seguinte,

---

[24] Terminologia usada pelo art. 386.º do Código Penal português, mas que já não é usada na Lei Geral do Trabalho em Funções Públicas (LGTFP), aprovada pela Lei n.º 35/2014, de 20 de junho e as suas sucessivas alterações. A LGTFP utiliza, simplesmente, o termo trabalhador (em funções públicas). Não obstante, vide considerando 38 da Diretiva, que justifica a *ratio* da utilização da expressão funcionário público.

conta de como eram as entidades autorizadas pela CNPD a implementarem o *Whistleblowing* e como se organizavam, a este respeito, 4 das 5 maiores empresas de auditoria em Portugal.

Antes de mais, convém referir quais são os dados pessoais genericamente sujeitos a tratamento no decurso de uma denúncia em contexto profissional. A Deliberação refere que "(...) [c]onsiderando a finalidade do tratamento em apreço, mostram-se necessárias para o tratamento as seguintes categorias de dados: [i]dentidade e categoria profissional do denunciante; [i]dentidade e categoria profissional do denunciado; [i]dentidade e funções das pessoas que intervêm na recolha e no tratamento; [o]s factos denunciados passíveis de integrarem actividades consideradas suspeitas (...); [o]s elementos de facto recolhidos no âmbito da averiguação; [d]estino da denúncia (...)".

A Diretiva não detalha como aquela, mas refere, no seu considerando 14, que o respeito pela privacidade e a proteção dos dados pessoais, que são consagrados como direitos fundamentais nos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da UE, constituem por si só um dos domínios do âmbito material da Diretiva [previsto na subalínea x), da alínea a), do n.º 1, do art. 2.º, que deve ser conjugada com o ponto J da Parte I do Anexo, do qual destacamos a alínea ii) relativa à possibilidade de denunciar violações ao RGPD; vide ainda considerando 76, 83, 97, 105, 109, art. 13.º e 17.º da Diretiva].

Os Estados-Membros da UE devem assegurar que a identidade do denunciante não seja divulgada a ninguém, além do pessoal autorizado competente para receber as denúncias ou dar seguimento a estas, sem o consentimento explícito do denunciante. O mesmo se aplica a quaisquer outras informações que permitam deduzir, direta ou indiretamente, a identidade do denunciante (cf. n.º 1 do art. 16.º da Diretiva).

A identidade do denunciante, e quaisquer outras informações que permitam identificá-lo, apenas podem ser divulgadas se tal for uma obrigação necessária e proporcional imposta pelo direito da UE ou nacional no contexto de uma investigação por autoridades nacionais ou de processos judiciais, inclusive com vista a salvaguardar os direitos de defesa da pessoa visada (cf. n.º 2 do art. 16.º da Diretiva).

A divulgação efetuada está sujeita a salvaguardas adequadas nos termos das regras da UE e nacionais. Em especial, os denunciantes devem ser informados antes da divulgação da sua identidade, salvo se tal informação

comprometer as investigações ou processos judiciais relacionados. Ao informar os denunciantes, a autoridade competente deve enviar-lhes uma comunicação por escrito explicando os motivos da divulgação dos dados confidenciais em causa (cf. n.º 3 do art. 16.º da Diretiva).

Recorrendo à definição de dados pessoais do RGPD, ficamos a saber que estes são a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)[25], isto é, para a análise em apreço, qualquer informação que identifique as pessoas intervenientes numa situação concreta de *Whistleblowing*.

Como já se referiu, a Deliberação estabeleceu direitos para o denunciante[26] e para o denunciado[27], bem como limites de âmbito subjetivo[28], procedimental[29], de autonomia da vontade[30] e específicos quanto à entidade responsável pela apreciação das denúncias[31].

---

[25] É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (cf alínea 1) do art. 4.º do RGPD).

[26] Nomeadamente informação sobre a identidade da entidade responsável; a finalidade prosseguida; os domínios abrangidos pela denúncia; o carácter facultativo do dispositivo; a inexistência de consequência pela não utilização do dispositivo; os destinatários da denúncia, a eventual transferência de dados para Estado exterior à UE; a existência de um direito de acesso e de retificação por parte das pessoas identificadas; e a não divulgação da sua identidade ao denunciado.

[27] Designadamente, informação sobre a identidade da entidade responsável; os factos denunciados; a finalidade do tratamento; o direito de acesso aos seus dados pessoais; o direito de requerer a retificação ou supressão dos dados se forem inexatos, incompletos ou equívocos; a confidencialidade no tratamento dos dados que lhe respeitem; a defesa do seu bom nome e privacidade; e o direito de apresentar queixa crime de denúncia caluniosa, nos termos previstos e punidos no Código Penal.

[28] Quem pode ser alvo de denúncia.

[29] O *Whistleblowing* deve ser um mecanismo complementar da atividade regular das organizações.

[30] Deve defender-se um regime de voluntariedade, limitado apenas pela obrigatoriedade de denúncia nos casos em que a lei penal e processual penal determine.

[31] "(...) [A] gestão e a apreciação preliminar das denúncias apresentadas deve ser adstrita a entidades de auditoria, independentes (...)". Repare-se que podemos entender o responsável pelo tratamento das denúncias, como um gestor das denúncias.

Circunscreveu ainda que não se afigura adequado "o estabelecimento de uma linha de denúncia interna, cuja gestão e apreciação compete aos eventuais denunciados". Estes podem ser "(...) pessoas que pratiquem atos de gestão relacionados com os domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro (...)" – cf. os limites de âmbito subjetivo que prevê.

Tal gerava a dúvida de saber se o *Whistleblowing* poderia ser praticado pelo auditor (no sentido de serem denunciantes ou denunciados) que, simultaneamente, pode ser o responsável pela apreciação das denúncias. Nesse sentido, indagou-se respostas através do recurso a literatura estrangeira, mormente, anglo-saxónica, decompondo os conceitos *Whistleblower* (e as suas classificações: interno e externo) e denúncia (e os seus tipos: interna e externa, identificada ou anónima, autorizada e não autorizada), chegando-se à conclusão que não se poderá excluir a possibilidade de os auditores serem responsáveis pela apreciação das denúncias[32], sem prejuízo de também poderem ser denunciantes ou denunciados (desde que não assumam, cumulativamente, dois tipos de intervenção no procedimento e processo)[33].

De acordo com a Deliberação, nos termos da Lei n.º 67/98, de 26 de outubro, alterada pela retificação n.º 22/98, de 28 de novembro, Lei n.º 103/2015, de 24 de agosto, antiga Lei de Proteção de Dados Pessoais (LPDP), alínea d) do art. 3.º: "(...) o responsável pelo tratamento é 'a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais'".

A Deliberação, que deverá ser apreendida pela lei nacional que transponha a *Diretiva*, carece de adequação à lei de execução do RGPD (Lei n.º 58/2019, de 8 de agosto, também conhecida por – atual – LPDP) que,

---

[32] Uma vez que a Deliberação diz que "(...) na linha do previsto no Código do Governo das Sociedades CMVM, a gestão e a apreciação preliminar das denúncias apresentadas deve ser adstrita a entidades de auditoria, independentes, às quais cumpre, entre outras funções, controlar o procedimento através do qual a sociedade cumpre as disposições em vigor no que diz respeito à possibilidade de os empregados notificarem irregularidades."

[33] Para mais desenvolvimentos vide Pitta Simões, Patrick, "O Whistleblowing em Portugal. Será que pode ser praticado pelo auditor?", *Revisores & Auditores*, revista da Ordem dos Revisores Oficiais de Contas, edição 84, janeiro-março 2019, p. 20-31. Disponível em: <http://hdl.handle.net/10400.21/11354>.

por sua vez, deve ser conjugada com a Deliberação 2019/494, da CNPD, de 3 de setembro (referente à desaplicação de algumas normas da Lei de Execução do RGPD).

Ela esclarece que a entidade responsável deve ser individualmente responsável, só se admitindo a corresponsabilidade entre instituições em casos de absoluta impossibilidade de determinar individualmente a responsabilidade pelo tratamento.

De acordo com a mesma, o responsável será a sociedade que adote procedimentos internos e assegure meios que permitam a denúncia e a ulterior investigação de comportamentos contrários à lei ou às políticas da sociedade ou grupo de sociedades e decida, a final, sobre o destino a dar à denúncia apresentada.

Tenha-se em atenção que a Deliberação, não dizendo expressamente que se aplica ao setor privado, nada diz, *a contrario sensu*, que seja aplicável à Administração Pública. Pode presumir-se que não se previa a sua aplicabilidade por desnecessidade, uma vez que a Deliberação no seu enquadramento refere a Lei n.º 19/2008, de 21 de abril, que estabeleceu garantias aos denunciantes que sejam trabalhadores da Administração Pública e de empresas do sector empresarial do Estado. Todavia a sua aplicabilidade ao sector público não é tão clara como a Diretiva (vide proémio do n.º 1 do art. 4.º deste diploma legal).

Para a Deliberação, ao responsável pelo tratamento cumpre estabelecer as regras para implementar a comunicação e o tratamento das denúncias, com indicação das pessoas ou órgãos que no seio da sociedade ou do grupo de sociedades estejam especialmente encarregues da recolha e do tratamento das denúncias, as quais deverão ser em número limitado, com formação técnica adequada e adstritas ao dever de confidencialidade assumido contratualmente.

Estas entidades deverão pautar a sua actuação por princípios de independência e imparcialidade e pelo respeito pelos princípios vigentes no direito interno, em particular no Código do Trabalho e no Código do Processo Penal.

Numa interpretação literal do considerando 74, que pode ser conjugado com o n.º 5 do art. 12.º, somente as autoridades competentes (responsáveis pelos canais de denúncia externa – art. 10.º a 14.º da Diretiva) terão o dever de receber formação profissional, nomeadamente, sobre as normas aplicáveis em matéria de proteção de dados, para tratar das denúncias

e assegurar a comunicação com os respetivos denunciantes, bem como dar o seguimento adequado à denúncia.

No entanto, os responsáveis pelos canais de denúncia interna (art. 7.º a 9.º da Diretiva) também tem os mesmos deveres que os trabalhadores das autoridades competentes (vide considerando 73, 77, alínea 12) do art. 5.º ou arts. 16.º a 18.º da Diretiva), pelo que dever-se-á por isso ter em conta o elemento sistemático da interpretação do considerando.

Assim, faz-se uma interpretação sistemática da necessidade de formação, ainda que a título recomendatório, para todos responsáveis, públicos ou privados, pelo tratamento das denúncias, de canais externos e internos.

Mencione-se ainda que o considerando 59 da Diretiva, referindo-se a informações de esclarecimento que as entidades públicas e privadas que dispõem de procedimentos para a denúncia interna (*Whistleblowing*) devem prestar às pessoas para que ponderem denunciar; deverão incluí-las em cursos e seminários de formação sobre ética e integridade. Deste modo acredita-se que estas matérias estarão incluídas nas ações de formação para responsáveis pelo tratamento das denúncias (internas e externas – autoridades competentes).

Não obstante eventuais regimes de subcontratação, o responsável pelo tratamento está adstrito à verificação do cumprimento das medidas de segurança, sobre quem impende a obrigação legal e a salvaguarda das medidas adequadas.

A Deliberação especifica que medidas de segurança podem ser adotadas, tal como a Diretiva, ainda que esta de forma mais dispersa. Não se vai desenvolver neste texto estas, mas tenha-se presente que a Deliberação refere, a este propósito, que o "(...) responsável pelo tratamento tomará as precauções necessárias para preservar a segurança dos dados, quer na ocasião da recolha, quer na da sua comunicação ou conservação. Independentemente das medidas de segurança adoptadas pelo responsável pelo tratamento, é a este que cabe assegurar o resultado da efetiva segurança da informação."

Se houver recurso a prestação de serviços para recolher ou tratar os dados, as pessoas especialmente encarregadas dessa missão, no seio do organismo prestador de serviços, só acedem aos dados dentro dos limites das suas competências (no caso de dados pessoais essa matéria é regulada no capítulo IV, mormente secção 1, do RGPD).

O prestador de serviços assume, por via contratual, a responsabilidade de não utilizar os dados para outros fins, assegurar a sua confidencialidade, respeitar o prazo de conservação e proceder à destruição ou à restituição de todos os suportes manuais ou informáticos dos dados pessoais no termo da sua prestação.

Não obstante as obrigações contratuais descritas, sempre haverá a realçar a obrigação de resultado que impende sobre o responsável pelo tratamento na salvaguarda da qualidade e da segurança dos dados[34].

A Deliberação esclarece ainda, relativamente à entidade responsável pela apreciação das denúncias, que ou esta entidade se encontra prevista na estrutura societária, sem prejuízo do exercício das funções descritas com independência e com salvaguarda da confidencialidade, não se verificando recurso à figura da subcontratação, aplicando-se-lhe o regime do responsável pelo tratamento; ou se verifica o recurso a entidade externa à estrutura societária, caso em que se aplica o regime de subcontratação.

Deste modo, se observa que a Deliberação permite que o auditor, interno ou externo, possa ser denunciado, como todo e qualquer trabalhador (ou se preferirmos colaborador)[35], e ser responsável por tratar as denúncias[36].

Independentemente da interpretação que se possa fazer da Deliberação, relativamente à natureza (interna ou externa) da entidade (de auditoria) responsável pela apreciação (tratamento) das denúncias, crê-se que as dúvidas quanto a esses profissionais (auditores) se dissiparam, no sentido que antecipadamente se indicou[37], com a publicação da Diretiva.

A Diretiva esclarece no considerando 54 que terceiros (fornecedores de plataformas de denúncias externas, consultores externos, auditores,

---

[34] Para uma reflexão complementar do exposto na Deliberação, vide Menezes Cordeiro, A. Barreto, *Direito da Proteção de Dados – à luz do RGPD e da Lei n.º 58/2019*, Edições Almedina, 2020, p. 307-317, 391-393.

[35] Não se desenvolverão as questões doutrinárias terminológicas tais como trabalhador, empregado ou funcionário. Parta-se do pressuposto que colaborador engloba todo o tipo de relação profissional.

[36] Não se olvide que um auditor subcontratado, apesar de ser externo à estrutura da organização, pode ser considerado interno se desempenhar tarefas de auditoria interna.

[37] Cf. Pitta Simões, Patrick, *Os limites da Auditoria Interna – O perfil do Auditor e o Whistleblowing*, dissertação de mestrado defendida no ISCAL, 2017. Disponível em: <http://hdl.handle.net/10400.21/8921>.

representantes sindicais ou representantes dos trabalhadores) podem ser igualmente autorizados a receber denúncias em nome de entidades dos setores privado e público, desde que ofereçam as devidas garantias de independência, confidencialidade, proteção de dados e sigilo. Os canais de denúncia podem ser operados internamente por pessoas ou serviços designados para o efeito ou disponibilizados externamente por terceiros (cf. n.º 5 do art. 8.º da Diretiva).

Não obstante, igualmente, é possível que uma pessoa (responsável operacional)[38], serviço imparcial competente ou departamento, possa receber as denúncias e manter comunicação com o denunciante (dar retorno de informação)[39].

A escolha das pessoas ou dos departamentos de uma entidade do setor privado para receber e dar seguimento às denúncias varia em função da estrutura da entidade, mas, em qualquer caso, o desempenho da função deverá assegurar a independência e a ausência de conflitos de interesses. Nas pequenas entidades, aquela poderá corresponder a uma segunda tarefa de um empregado da empresa, bem posicionado para comunicar diretamente com o dirigente da organização, tais como o chefe do gabinete de conformidade (vulgo *Compliance Officer*), o responsável pelos recursos humanos, o responsável pela integridade, o responsável por questões jurídicas ou de privacidade, o diretor financeiro, o auditor-chefe ou um membro do conselho de administração (cf. considerando 56 da Diretiva).

Se se observar a sistemática da Diretiva, que diferencia denúncias internas de externas e ambas de divulgação pública, pode entender-se que existirão diferentes responsáveis pelo tratamento de denúncias internas (das entidades do setor privado e público) e externas (das autoridades competentes). Tenha-se em conta que a Deliberação nunca referiu a possibilidade de a divulgação pública poder ser protegida pelo sistema de *Whistleblowing*.

Ainda relacionado com o responsável pelo tratamento do *Whistleblowing*, como se tem vindo a mencionar, há que ter em conta a autoridade competente, ou seja, qualquer autoridade nacional designada para receber

---

[38] Cf. se extrai da parte final do n.º 5 do art. 8.º da Diretiva.

[39] Cf. alínea c) do n.º 1.º do art. 9.º da Diretiva.

denúncias externas e dar aos denunciantes retorno de informação[40] (seguimento)[41]; que é diferente da figura de responsável pelo tratamento da denúncia (interno).

Caberá aos Estados-Membros designar as autoridades competentes para receber e para dar o devido seguimento às denúncias. Estas poderão ser autoridades judiciais, organismos reguladores ou de supervisão competentes nos domínios específicos em causa, ou autoridades com competências mais gerais a nível central num Estado-Membro, autoridades de aplicação da lei, organismos de luta contra a corrupção ou provedores de justiça (cf. considerando 64 da Diretiva).

Como já defendido[42], julga-se que fará sentido haver autoridades competentes por setores[43], com diferentes níveis de responsabilidade, cf. se depreende do considerando 77. Muito provavelmente, estas serão os Serviços de Inspeção Geral, Autoridades ou Entidades Reguladoras[44], a Comissão do Mercado de Valores Mobiliários, a CNPD, as Ordens Profissionais ou mesmo o Provedor de Justiça. Mencione-se que as instituições, órgãos ou organismo da União, são tidos como entidades externas à autoridade competente (que é sempre nacional) para efeitos de denúncia.

Por último, não se crê que o responsável pelo tratamento da denúncia, que será o responsável máximo pela organização e por isso o maior interessado na eficiência e eficácia do *Whistleblowing*, não delegue, sobretudo em organizações de significativa dimensão, competências de apreciação preliminar ou instrutória a um trabalhador, deixando para si apenas o poder de decisão final (vide considerando 55 e 56).

---

[40] Definida na alínea 13) do art. 5º da Diretiva.

[41] E, ou, designada para desempenhar as funções previstas na Diretiva (cf. definição prevista na alínea 14) do art. 5.º).

[42] Em Pitta Simões, Patrick, "O Whistleblowing é um caso de polícia(s)?", in *Polícia(s) e Segurança Pública: História e Perspetivas Contemporâneas*. MUP – Museu da Polícia, p. 482-483.

[43] Por exemplo o considerando 21, referindo o art. 11.º da Diretiva 89/391/CEE do Conselho, de 12 de junho de 1989, refere a existência de uma Autoridade para a área de Saúde e Segurança no Trabalho.

[44] Algumas destas previstas no DL n.º 276/2007, de 31 de julho, alterado pelo DL n.º 32/2012, de 13 de fevereiro e pela Lei n.º 114/2017, de 29 de dezembro.

3. Da teoria ao *Whistleblowing* autorizado

Analisado o porquê de existir o *Whistleblowing*, o que é, e quem são os seus intervenientes, com destaque para quem pode ser responsável pelo seu tratamento, vejamos agora, da teoria à prática, quantas, de onde e como eram as entidades que foram autorizadas pela CNPD a implementá-lo em Portugal, e ainda quem era responsável pelo tratamento de dados gerados pelo *Whistleblowing* em 4 das 5 maiores empresas de auditoria, a que se chamou de "*Four Big Five*"[45].

Para o efeito, utiliza-se, com as devidas adaptações, o estudo efetuado aquando da realização da dissertação de mestrado em que se solicitou à CNPD o acesso à sua base de dados, de modo a analisar-se as informações disponibilizadas pelas instituições que a tivessem notificado para a autorização de um tratamento de dados pessoais, com a finalidade de gestão das comunicações internas de atos de gestão financeira irregular.

Entendeu-se que se devia pedir diretamente à Autoridade Nacional de Controlo de Dados Pessoais, legítima e competente para, à data (cf. arts. 27.º e 28.º da antiga LPDP), autorizar previamente a implementação do sistema de denúncias internas, daí que o nome escolhido para este capítulo seja: *Whistleblowing autorizado* (oficialmente declarado e em conformidade com a Deliberação)[46].

Mencione-se também que, honrando o compromisso, previamente assumido, com a CNPD e com todas as SROC que se interpelaram, independentemente de terem ou não colaborado, entendeu-se como uma legítima limitação de âmbito do estudo empírico realizado na dissertação, não se correlacionar as informações recolhidas junto daquela

---

[45] As quatro das cinco maiores empresas de Auditoria, que colaboraram no estudo empírico foram: a BDO & Associados, Sociedade de Revisores Oficiais de Contas (SROC), Lda.; a Deloitte & Associados, SROC S.A.; a Ernst & Young Audit & Associados, SROC, S.A. e a KPMG & Associados, SROC, S.A.

[46] Uma forma alternativa de identificarmos organizações que implementaram o *Whistleblowing*, seria analisar os relatórios de governo das sociedades, conjugados com regulamentos de comunicação de irregularidades das empresas que disponibilizassem os mesmos nos seus *websites*. Porém, correr-se-ia o risco de ser uma informação dispersa, não uniforme e de dificuldades acrescidas face à maior ou menor pública destas informações.

com a identificação destas, incluindo as respostas obtidas pelas "*Four Big Five*".

Refira-se ainda que se ponderou apurar até que ponto o *Whistleblowing* se revela eficiente e, ou, (des)vantajoso e dispendioso[47]; porém, para além dessa avaliação qualitativa que poderia ser encarada como uma intromissão na gestão de informação financeira e por isso um trabalho estéril; considerando, que o setor empresarial está saturado de inquéritos[48]; achou-se que, numa relação de custo-benefício, não se seria tão produtivo e se afastaria do propósito da dissertação de mestrado.

Por fim, ressalva-se que, relativamente à data a que se reportam as autorizações analisadas, a base de dados eletrónica que foi facultada pela CNPD não permitia saber, *ab initio*, detalhes de todos os processos (autorizações solicitadas) por não estarem informatizados os anteriores ao ano de 2011, o que limitou o tratamento ou a profundidade de algumas questões tratadas.

Feita esta clarificação, balizou-se a amostra às 131 entidades a quem foi autorizado, de acordo com a Deliberação, o tratamento de dados[49], desde janeiro de 2011 até 31 de agosto de 2015[50]. Assim, em termos evolutivos, cf. ilustra a figura 1, verificou-se que entre os anos civis completos de 2012 e 2014, houve uma tendência crescente de autorizações de *Whistleblowing*, o que pode ser indiciador de que este sistema foi sendo cada vez mais utilizado. Ideia reforçada pelos dados de 2015 que, apesar de serem referentes ao final do mês de agosto, portanto a pouco mais de metade do ano, já superavam as 19 autorizações atribuídas em 2012.

---

[47] Em abono da verdade, em grande parte o *Whistleblowing* é um assunto "melindroso" para que nos fosse facultado algumas informações, tais como quantas situações foram detetadas ao seu abrigo.

[48] Nomeadamente os que permitiriam aferir estatística e qualitativamente a eficácia e, ou, eficiência dos serviços.

[49] Alguns dos 174 processos identificados, distintos em número, eram referentes à mesma entidade. Seriam os casos em que a organização requerente tivesse mudado algum dos dados fornecidos no formulário de notificação geral, à data disponível no *website* da CNPD, e por isso deu origem a um novo número de processo, ou ainda nas situações em que inicialmente se arquivou o processo, por insuficiência de garantias ou inconformidade com a Deliberação, e depois foi reaberto com um outro número.

[50] Data a partir da qual as autorizações ficaram suspensas cf. se irá ver de seguida.

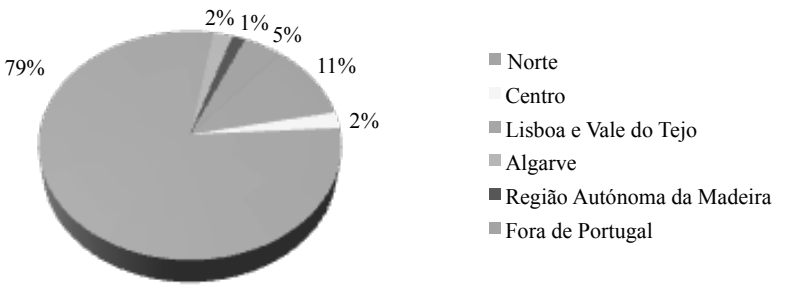
Possivelmente o número de autorizações seria maior se o austríaco *Maximilian Schrems* não tivesse movido, junto do Tribunal de Justiça Europeu, uma ação de reenvio prejudicial contra a *Data Protection Commissioner*, por não ter investigado a sua queixa contra a filial do *Facebook* na Irlanda (a *Digital Rights Ireland Ltd.*), em virtude de esta violar as leis de proteção de dados pessoais europeus.

Figura 1 – Notificações autorizadas por ano.

Fonte: CNPD. Elaboração própria.

No que diz respeito à origem geográfica das entidades, observando a Figura 2, ficou-se a saber que a esmagadora maioria (79%, correspondente a 103 empresas), se localizava na região de Lisboa e Vale do Tejo, seguida da Região Norte (11%). As restantes regiões, juntas, apenas representavam 10%. Refira-se ainda que duas entidades que notificaram um tratamento de dados no âmbito das Linhas de Ética, eram da Região Autónoma da Madeira. Nenhuma das 131 entidades é da Região Autónoma dos Açores ou do Alentejo. Curiosamente, sete (5%) declaravam estar sediadas fora de Portugal.

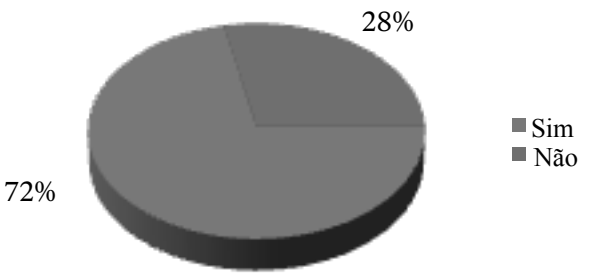
Figura 2 – Incidência geográfica do *Whistleblowing*, entre 2011 e meados de 2015, por Nomenclatura de Unidade Territoriais para Fins Estatísticos (NUT) II[51].



Fonte: CNPD. Elaboração própria.

Destas empresas sabiamos também, cf. a Figura 3, que a maioria (94), representando 72% do total, subcontratava uma entidade externa para tratar dos dados decorrentes das denúncias, garantindo assim a sua imparcialidade[52], e apenas 28% não o fazia.

Figura 3 – Subcontratação do tratamento.



Fonte: CNPD. Elaboração própria.

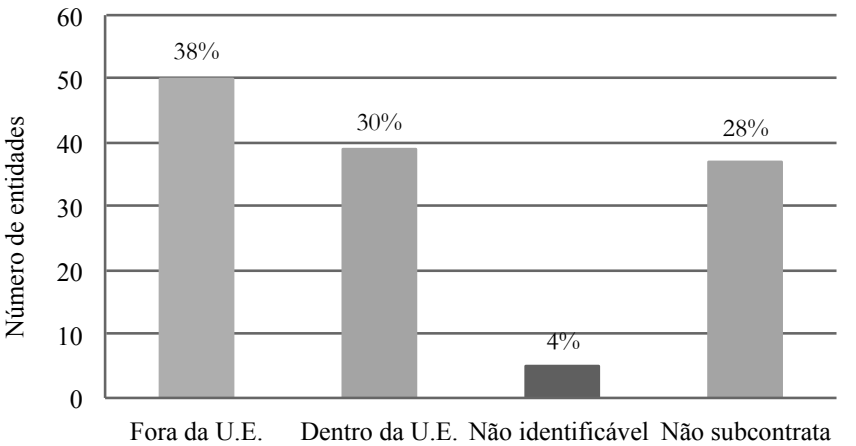
---

[51] Matrizes de delimitação geográfica, designadas por NUT, foram aprovadas pelo DL n.º 46/89, de 15 de fevereiro; alterado pelo DL n.º 163/99, de 13 de maio; pelo DL n.º 317/99, de 11 de agosto; pelo DL n.º 244/2002, de 5 de novembro; e pela Lei n.º 21/2010, de 23 de agosto.

[52] O tratamento por subcontratante devia respeitar o disposto nos arts. 14.º e 16.º da antiga LPDP. Vide art. 28.º do RGPD.

Daquelas, 39 entidades subcontratavam empresas europeias e 50 subcontratavam empresas não europeias, concretamente dos EUA, conforme se ilustra na figura 4.

Figura 4 – Origem da entidade que processa.



Fonte: CNPD. Elaboração própria.

Esclareça-se que as empresas norte-americanas tinham de assegurar a melhor proteção possível dos dados pessoais (quando eram exportados), respeitando os normativos da UE, nomeadamente quando a transferência de dados pessoais era efetuada para fora da UE devia respeitar-se os arts. 19.º e 20.º da antiga LPDP[53].

A CNPD manifestou, através das suas autorizações (por exemplo a n.º 2717/2017, de 7 de março), que não estava em condições de decidir de forma definitiva sobre a transferência de dados pessoais para o território

[53] Vide art. 22.º da atual LPDP e arts. 44.º a 50.º do RGPD. Não se abordará as transferências de dados pessoais gerados pelo *Whistleblowing*, entre Estados-Membros e entre estes e um país terceiro, no entanto, retenha-se que se no primeiro caso o RGPD, aplicável diretamente, assegura um nível de proteção de dados adequado, no segundo caso é necessário ter a certeza que o país terceiro respeita requisitos de segurança.

dos EUA, uma vez que, por força do acórdão do Tribunal de Justiça da União de Europeia, de 6 de outubro de 2015, relativo ao processo C-362/14, já referido, foi declarada inválida a Decisão 2000/520/CE, da Comissão Europeia, de 26 de julho de 2000, que no seu anexo I estabelecia princípios internacionais de auto-certificação, que deveriam garantir que as entidades norte-americanas respeitavam a privacidade e a segurança das informações pessoais dos cidadãos da UE e Suíça, aquando de fluxos de dados transatlânticos designados por *Safe Harbor.*

Nestes termos, tendo a CNPD que proceder a uma análise aprofundada da legislação vigente nos EUA, com vista a apurar se aquela se sobrepunha, de modo desnecessário e desproporcionado, às cláusulas contratuais[54] adequadas que o responsável e os destinatários da informação subscreviam, apenas emitiu autorizações provisórias (cf. seu Comunicado de 23 de outubro de 2015).

Feita esta explanação e prosseguindo, da teoria à prática, interrogou-se as *"Four Big Five"* no sentido de saber se dispunham de algum sistema que se traduzia na criação de condições para a denúncia de comportamentos fraudulentos ou irregulares (*Whistleblowing*). Todas responderam que sim, exceto uma que não chamava de sistema de denúncias[55].

Neste último caso, em particular, existiam três áreas diferentes, não divididas por gabinetes, mas sim por sócios responsáveis: pela transparência, sistema interno de controlo da qualidade e ética. "Todas as pessoas [tinham] trimestralmente um conselheiro, exceto os sócios, a quem reporta[va]m todas as questões de análise de *performance,* funcionando como um canal de informação que saí[a] da hierarquia operacional. Qualquer questão relativa ao seu superior hierárquico pod[ia] ser reportada ao seu Conselheiro".

Refira-se também que uma das SROC reportava que ajudavam "empresas a montar o sistema". Porventura os auditores internos seriam os mais bem preparados para auxiliarem nesta tarefa.

---

[54] Cláusulas contratuais-tipo, contratos entre empresas do mesmo grupo – acordos intragrupo – ou outros contratos *ad-hoc.*

[55] Repita-se que as informações que ora se mencionam foram obtidas no âmbito da dissertação de mestrado, pelo que se desconhece se ainda se mantem os factos ou procedimentos relatados pelos entrevistados.

Em seguida, perguntou-se a quem ficava a cargo a análise e a gestão do *Whistleblowing*. Começando pela entidade que tinha aquela particularidade, o Conselheiro podia ser um dos sócios ou um dos diretores, mas nunca seria o superior hierárquico direto do trabalhador. Ao Conselheiro competia perceber as situações em que o trabalhador entendia revelar o que não estava bem, ou se estava satisfeito com a sua hierarquia operacional. «O Conselheiro dev[ia] comunicar, em função da gravidade, aos sócios executivos (...).»

Outra das "*Four Big Five*", respondeu que «[n]uma primeira fase [era] cometida ao Diretor de Ética (cargo desempenhado por um sócio), que far[ia] a triagem do assunto e reportar[ia] ao Diretor de Risco e Reputação (cargo também desempenhado por um sócio). Por sua vez, numa segunda fase, este direcionar[ia] a denúncia para outros Diretores, tais como o de Auditoria Interna ou de Independência».

Uma outra SROC inquirida replicou-nos, sucintamente, que quem analisava e fazia a gestão do *Whistleblowing* era a "empresa mãe' e outra específica".

Por fim, uma quarta entidade afirmava ter "uma área independente da estrutura onde pod[ia] ser comunicada a situação" mencionando ser dever do órgão de fiscalização receber as irregularidades apresentadas por acionistas, colaboradores ou outros [cf. alínea j) do n.º 1 do art. 420.º e f) do n.º 1 do art. 422.º do CSC; se fosse o Fiscal Único ou o Conselho Fiscal; alínea j) do n.º 1 art. 423.º-F do CSC; se fosse a Comissão de Auditoria; ou alínea j) do n.º 1 do art. 441.º do CSC se fosse o Conselho Geral de Supervisão].

4. Responsabilidades intrínsecas ao *Whistleblowing*

Entende-se que esta temática mais do que interessar ao investigador ou à academia, deve interessar à sociedade de forma transversal, uma vez que qualquer pessoa pode ser envolvida num assunto de *Whistleblowing*, mesmo que não queira ou faça, no seu entender, algo passível de tal "enredo".

Viu-se que os denunciantes podem denunciar a qualquer momento, desde que tenham alguma relação profissional com a entidade a quem reportam a irregularidade ou violação ao Direito; bem como o responsável pelo tratamento, de canais de denúncias internas e externas, é diferente

da autoridade competente, entidade externa que será responsável pelo canal de denúncias externo.

Considera-se que a lei que venha a transpor a Diretiva, deverá ter em conta que a Deliberação não foi revogada e as suas Linhas de Ética deverão estar em conformidade com o RGPD. O que parece não ser o caso da Lei de Execução do RGPD, atual LPDP, cf. Deliberação 2019/494, da CNPD, de 3 de setembro.

Para o gestor (ou responsável pelo tratamento) do *Whistleblowing*, as informações produzidas deverão ser protegidas por técnicas de codificação ou encriptação, o que as tornam logo *a priori* informações classificadas[56], ainda que devam ser entendidas como diferentes das mencionadas na alínea a) do n.º 3 do art. 3.º da Diretiva.

Haverá matérias cujo conteúdo será sensível e que carecem de ser vedadas a um "*Whistleblowing* mais amplo", nesses casos o legislador europeu contemplou que a Diretiva não afeta a aplicação do direito nacional ou da União nesses temas.

Poder-se-á subdividir e classificar o *Whistleblowing* como procedimento, isto é, a sequência funcional de atos conducentes à identificação dos intervenientes e dos factos; e como processo, ou seja, o apuramento da veracidade dos factos e assunção do direito.

O primeiro impulso procedimental por parte de um denunciante será dar a conhecer a um responsável pelo tratamento da denúncia a informação que dispõe (preferencialmente suportada em evidências/ /provas). A tarefa do responsável pelo tratamento das denúncias inicia-se com a denúncia (informação que deve ficar documentada)[57], incide sobre a mesma (a que não estiver documentada não tem evidências de que foi efetuada) e finda com a elaboração e aprovação de um parecer, relatório ou decisão final (informação documentada). Ser responsável pelo tratamento das denúncias é ser também guardião da documentação produzida no âmbito do *Whistleblowing*.

O procedimento de denúncia tem sempre de ter uma iniciativa e apreciação preliminar, por sua vez o processo de denúncia terá de ter

---

[56] Por serem classificadas devem ser protegidas dessa forma. Estas informações podem englobar segredos comerciais, como diversas vezes referido na Diretiva (vide por exemplo o n.º 4 do art. 16.º).

[57] Vide art. 18.º da Diretiva.

uma instrução e uma decisão final, que poderá conter a formulação de recomendações pelo representante (máximo) legal da organização, responsável final pelo tratamento das denúncias.

Se houver uma separação de tarefas, o que se considera aconselhável, haverá um responsável pelo tratamento das denúncias (inicial) que fará um relatório ou parecer, com uma proposta de decisão, contendo ou não recomendações, conforme a configuração da situação justifique.

As organizações públicas e privadas devem ter em conta, o que não é explícito na legislação nacional e europeia, a adequada proteção do responsável pelo tratamento das denúncias que, tal como os outros intervenientes no sistema de *Whistleblowing*, também está sujeito a retaliações, quer pela informação que passa a ter conhecimento, quer pela(s) decisão(ões) que toma ou poderá tomar.

O responsável pelo tratamento das denúncias pode também ser alvo de assédio moral (já para não falar de crimes contra a sua honra), designadamente destrato, perseguição ou devassa da sua vida pessoal (escrutínio não legítimo), de modo a ser corrompida a sua idoneidade e imparcialidade ou a ser pressionada em determinado sentido, através de coação, alguma decisão instrutória ou final.

Criar um mecanismo de *Whistleblowing* olvidando este pilar estrutural, pensando apenas na salvaguarda de direitos, liberdades e garantias do denunciante e denunciado, não só torna menos atrativo e mais árido o trabalho subjacente à tarefa do responsável pelo tratamento das denúncias, como pode pôr em causa a integridade e fiabilidade de todo sistema.

Se não forem pensadas medidas para acautelar eventuais incidentes relativos aos responsáveis pelo tratamento das denúncias, tais como a sua proteção jurídica caso venham a ser notificados num processo judicial em consequência de um assunto de *Whistleblowing* que estejam a tratar ou tenham tratado, esta função não será tida como apaziguadora em si mesma.

O *Whistleblowing* não deve ser entendido apenas como um mecanismo de prevenção e, ou, combate à corrupção. Ele engloba também a melhoria de condutas não corruptivas, fraudulentas ou que indiciam sobre a prática de outro crime e, ou, infração conexa. Este sistema deve permitir a prevenção e correção de *performances* laborais, de modo a melhorar a economia, eficiência e eficácia das organizações públicas e privadas.

O responsável pelo tratamento das denúncias deve garantir a proteção de dados pessoais (informação sobre a identidade da entidade responsável);

a finalidade prosseguida; os domínios abrangidos pela denúncia; o carácter facultativo do dispositivo; a inexistência de consequências pela não utilização do dispositivo; a transparência do processo aos destinatários da denúncia; a eventual transferência de dados para Estado exterior à UE em conformidade com a legislação europeia sobre proteção de dados; a existência de um direito de acesso e de retificação por parte das pessoas identificadas; e a não divulgação das suas identidades; deveres de confidencialidade; tratamento de dados apenas relevantes; conservação das denúncias, incluindo "conservação alheia" (isto é, não intromissão ou modificação de uma denúncia dirigida a pessoa não competente para a apreciação da mesma); proibição de retaliação; medidas de apoio para denunciantes e para denunciados; e a irrenunciabilidade dos direitos e das vias de recurso.

Ainda que a denúncia, anónima ou não, deva ser voluntária, os Estados-Membros devem: assegurar que as entidades jurídicas dos setores privado e público estabeleçam canais e procedimentos para denúncia interna; designar as autoridades competentes para receber, dar retorno de informação e dar seguimento a denúncias, dotando-as dos recursos adequados; e assegurar que as autoridades competentes revejam regularmente os procedimentos para a receção de denúncias e o seu seguimento.

Considerações finais

A temática do *Whistleblowing* em Portugal, que para alguns poderá significar o ato de denunciar ou, de uma forma abrangente (e correta), todo o procedimento e processo gerado pela denúncia, tem ganho importância acrescida, passando de recomendações, a artigos de leis até à publicação de uma Diretiva (de *soft* para *hard law*) que, por seu turno, em breve, deverá ser transposta para o ordenamento jurídico nacional.

Quando isso acontecer as organizações vão deparar-se com uma pergunta crucial: e agora, quem pode ser o responsável pelo tratamento das denúncias?

Com este texto pretendeu-se, em primeiro lugar, alertar a sociedade, em geral, e a comunidade científica, em particular, para este assunto e, em segundo lugar, asseverar, dentro do que é possível, a resposta de quem poderá ser o responsável pelo tratamento da denúncia.

A legislação existente e a que venha a existir terá de estar, forçosamente, em conformidade com o RGPD que é de aplicação direta, ainda que não seja totalmente uniforme, face a várias possibilidades que deixa ao legislador de cada Estado-Membro.

Existem direitos, mas também deveres, para todos os intervenientes no mecanismo do *Whistleblowing*, e todos os participantes no sistema devem ter a obrigação e garantia de defesa da confidencialidade dos dados pessoais.

Anseia-se por ver qual será a relação profissional entre *Compliance Officers*, Auditores, Encarregados de Proteção de Dados e responsáveis pelo tratamento das denúncias (se estes não forem os dois primeiros), ou destes com outros profissionais, e verificar se haverá uma articulação ou separação de competências relativamente ao *Whistleblowing* de modo a não haver um conflito positivo ou mesmo negativo no tratamento destas competências sobreposta. Ou, ainda, ninguém especificamente responsável, de modo a gerar um circuito vicioso de não competência direta sobre o sistema de *Whistleblowing*, ou de não decisão tempestiva.

De igual modo, acompanhar-se-á o desenvolvimento da atuação das Autoridades Competentes que venham assim ser denominadas ou eventualmente criadas. Como supervisionarão o *Whistleblowing*? Haverá alguma com atribuições ou competências para agregar e coordenar a informação estatística sobre as denúncias externas, as destinadas às autoridades competentes, a serem apresentadas anualmente à Comissão Europeia (cf. n.º 2 do art. 27.º da Diretiva)? Aguardar-se-á para ver quem serão os responsáveis pelo tratamento das denúncias internas e externas; quem serão os responsáveis pelo tratamento do *Whistleblowing*.

Algorithms and the GDPR: An analysis of article 22

Sandra Barbosa[*]
Sara Félix[**]

Abstract: The ever more current use of automated decisions, in the most various fields, has strike society's attention to the (lack) of protection given to data subjects when these decisions come to fruition. Since it is not a question of if they occur, but more so, of when and how, the General Data Protection Regulation, on its article 22, attempted to provide a framework for those decisions, aiming to put the data subject's rights, freedoms and legitimate interests at their forefront. The question that remains, and that we intend to answer, is if the use of automated decision-making is hindering that aimed protection so highly that it must be withdrawn, despite the supposed benefits they might bring to the entities making use of them.

Keywords: *Algorithms; Automated decision-making; Profiling; Bias; General Data Protection Regulation.*

Resumo: A utilização cada vez mais recorrente de decisões automatizadas, nas mais variadas áreas, tem despertado a atenção da sociedade para a (falta) de proteção dos titulares dos dados quando estas decisões são postas em prática. Uma vez que não se trata de uma questão de se podem ocorrer, mas sim de quando e como, o Regulamento Geral sobre a Proteção de Dados, no seu artigo 22, pretendeu estabelecer um mecanismo que colocasse os direitos, liberdades e garantias dos titulares dos dados em primeiro plano. A questão que permanece, e que pretendemos responder, prende-se com a utilização destas decisões automatizadas impossibilitar tanto essa desejada proteção, ao ponto

[*] Consultora na área da Proteção de Dados. Licenciada em Direito pela Escola de Direito da Universidade do Minho, frequenta o Master Degree in Law – Specialization in Law and Technology na Faculdade de Direito da Universidade Nova de Lisboa, em fase de dissertação.

[**] Licenciada em Direito pela Faculdade de Direito da Universidade de Lisboa, frequenta o Master Degree in Law- Specialization in International and European Law na Faculdade de Direito da Universidade Nova de Lisboa, em fase de dissertação.

de dever ser suprimida, pese embora os supostos benefícios que podem advir para as entidades que as empregam.

Palavras-chave: *Algoritmos; Decisões automatizadas; Definição de perfis; Enviesamento; Regulamento Geral sobre a Proteção de Dados.*

Introduction

In a digital and data driven era, the use of algorithms and data analytics has become a common business practice, especially towards consumers, that has also spread to public entities and state services. Currently, companies base their probabilities of attracting more consumers and achieving more efficiency on technology, and algorithms play one of the main roles for their potential success. Profiling individuals, either in public or private institutions, has proven to be the desirable key for progress.

Indeed, profiling methods regarding the use of algorithms can, and generally do, give a basis for automated decision-making (also mentioned in this article as "ADM"), which consists in the ability to, using technological means, make decisions with none (solely automated) human involvement. These methods use, among others, personal data, which in nature can become a highly privacy-invasive process. Moreover, artificially intelligent agents, often based on machine learning systems, can be quite opaque on their procedures, sometimes carrying inherent biases that can put data subjects in a very unsafe position.

As technology has been evolving quite rapidly and strongly over the last two decades, due, inter alia, to the exponential increase in computing power, the concerns with automated decision-making processes, already addressed on article 15[1] of the Data Protection Directive 95/46/EC (DPD), published in 1995, were reiterated, and updated, in the General

[1] "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

Data Protection Regulation[2] (hereinafter "GDPR" or "Regulation"), published in 2016, with its article 22, a successor of DPD's article 15, aiming to define a set of rules to protect data subjects from the risks posed by ADM and uphold human dignity through the process[3].

This article thus seeks to dive into provision 22 of the GDPR, conceptualizing the undefined concepts, deconstructing the demandable requirements, always with a conscious data subject protection against algorithmic bias, aiming to be a beacon to companies and organizations that are lost in the vast sea of data protection.

1. Principles Applicable to Automated Processing

Based on the conception of privacy and data protection as a fundamental right, enshrined in articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU)[4], the GDPR intends, also respecting article 16 of the Treaty of the Functioning of the European Union (TFEU), to lay down the data protection rules for the processing of personal data within the scope of Union law[5]. As the Regulation's material scope comprises, among other, the processing of personal data wholly by automated means[6], its data protection rules apply, as well, to the automated decisions under consideration here.

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

[3] Mendoza Isak, Bygrave Lee A., "The Right Not to Be Subject to Automated Decisions Based on Profiling", *University of Oslo Faculty of Law Research Paper*, No. 2017-20, 2017.

[4] Article 7 of the CFREU establishes the right to respect for everyone's private and family life, home and communications, as article 8 recognizes an explicit right to the protection of everyone's personal data, who must be processed fairly for specified purposes.

[5] Article 16 of the TFEU not only recognizes the right to the protection of everyone's personal data, but also obliges the EU to "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data".

[6] As defined in GDPR's article 2.

As such, it is on article 5 that the GDPR lays down the principles that generally apply to the processing of personal data. Concerning automated decision-making, certain principles govern the use and creation of algorithms. One of those is the transparency, lawfulness and fairness principle, present in article 5 (1) (a), which requires controllers to take the appropriate measures to keep data subjects informed about how their data is being used. Thus, when using ADM systems, data controllers shall inform the data subject, about the logic behind the algorithms. The Article 29 Data Protection Working Party's (hereinafter "WP29") Guidelines on Automated Individual Decision-Making and Profiling for the purposes of Regulation 2016/679 gives an example[7] of the appropriate information that shall be given when automated processing exists. The information given needs to address which data, that it is being processed under those means, was collected and the consequences of it, aligning, as well, with the information and access requirements present in articles 13 to 15 of GDPR. As such, data subjects have the right to be informed by data controllers about the existence of ADM and to be given information about the logic involved and the envisaged consequences of such automated processing [as provided in articles 13 (2) (f) and 14 (2) (g)], as well as to be given details about their personal data that is being used for ADM [as determined in article 15 (1) (h)].

This information and access rights can be perceived as a right to an *ex ante* generic explanation about the system functionality and its consequences to the data subject, though a right to an *ex post* explanation is not included in the provision[8]. However, as we will see further on, although this information may be given, every so often data subjects may not engross the information.

In addition, it is also important to mention the principle of data protection by design and by default, which includes those two complementary concepts that can jointly fortify each other, and ultimately, the protection of personal data. According to GDPR's Article 25, data controllers must consider the protection of personal data, both at the

---

[7] WP29, p.10. Example of the insurance company that offers insurance according to the profiling of the individuals, based on their driving behaviour.

[8] A brief analysis about the existence of a right to explanation on the GDPR is provided further on, in point 5.3.

design stage of the processing activities and during the processing itself, by implementing the appropriate technical and organizational measures and default settings to meet the demands of the Regulation's principles[9]. Regarding ADM, such measures should ensure the accuracy and quality of the data, to minimize the possibility of false, non-representative or biased outputs and, also, the respect for the fairness principle, under which personal data cannot be processed in a manner that is unjustifiably detrimental and discriminatory, by allowing, for example, the necessary human intervention to uncover machine bias and review the fairness of the algorithms used. Therefore, controllers must carefully consider the use of ADM, when designing its processing activities, applying the necessary safeguarding measures at that stage and ensure that, by default, data subjects' personal data is protected.

Other principles that significantly apply to ADM are the principle of purpose limitation, in article 5 (1) (b), which encompasses that the data collected for a specific purpose shall never be processed for a different one; the principle of data minimisation, in article 5 (1) (c), that respects to the minimum necessary extent to which the data shall be processed and applies either to quantity and quality, meaning that one cannot process an excessive amount of data, and equally, cannot go beyond the limit that was established as necessary to process it; the principle of accuracy, in article 5 (1) (d), that requires the data processed to be accurate and kept to date, relating to the right of data rectification; and finally the principle of storage limitation, in article 5 (1) (e), according to which personal data shall be stored for an amount of time that is considered essential for the task of processing and, in line with Recital 39[10], controllers shall establish a time limit during which these data will be stored.

---

[9] EDPD Guidelines 4/2019 on Article 25, Data Protection by Design and by Default; available at: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>. Last visited on 17.04.2021.

[10] Recital 39 GDPR, "(...) In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. (...)".

2. Deepening the analysis of Article 22

Article 22 consists of four paragraphs: in short, paragraph 1 states that individuals shall not be subject to the automated processing of personal data, as a general rule; paragraph 2 states the exception, specifying three situations in which ADM processing is allowed; the 3rd paragraph alludes to the safeguards that must be applied when ADM processing can occur, to ensure protection of data subjects' rights and interests; and finally, paragraph 4 refers to special categories of data present in article 9. To fully comprehend article 22 and how it needs to be addressed, each paragraph will be considered.

2.1. The construction of the data subject's "right"

Prior to a deeper analysis of the requirements of paragraph 1, it is important to address the proper construction of this "right" of the data subject. Indeed, as Maja Brkan[11] further developed, the right hereby in scrutiny can be understood either as an active right, dependent on the data subjects' effective exercise, or as a passive one, that the data controller in charge of an automated decision must observe without their active claim.

Construing this as an active right would make its exercise solely dependent on the data subject's choice and will. This could lead, on a worst-case scenario, to data controllers lawfully taking automated decisions, having the characteristics described in paragraph 1, without the necessary safeguards to protect data subjects' rights, freedoms, and legitimate interests, as described in paragraph 3 (further analysed below). The detrimental effects of that omission present a clear burden on the data subject's back, who is probably not sufficiently knowledgeable to understand the impact of such omission of conduct. Another issue raised here are the effective legal consequences that derive from its exercise – does this right translate into a right to object automated decisions? Or as a right to request human intervention in the decision?

---

[11] Brkan Maja, "Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond", *Conference Terminator or the Jetsons? The Economics and Policy Implications of Artificial Intelligence*, 2017, p.1-29.

Consequently, interpreting article 22 (1) as giving the data subject the burden of actively exercising this right could, therefore, go against the aim of this provision, which is to protect data subjects from a general possibility of an automated decision being applied to them. Systematically, article 22 implies that all decisions which fulfil the requisites of paragraph 2 must be accompanied with paragraph 3's safeguards, otherwise will not be authorised by the GDPR.

Taking all this into account, scholars such as Mendoza and Bygrave[12], claim (and correctly, in our opinion) that, to achieve the ultimate goal of this provision, it is more appropriate to construct this "right" of the data subjects as a general prohibition to data controllers of fully automated decision-making. Actually, such interpretation of article 22 (1) aligns with the wording of article 11 of the Directive on Data Protection in Criminal Matters which gives the Member States a clear obligation to prohibit automated decisions having certain characteristics and provide appropriate safeguards for the data subjects' rights and freedoms.

In sum, construing the data subjects' "right" as a general prohibition of certain types of automated decisions is, in our opinion, the better way to ensure the protection of their rights, freedoms and legitimate interests.

2.2. Paragraph 1

According to the first paragraph of article 22, "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.", the data subject shall not be subordinated to ADM systems[13]. This prohibition has specific criteria – the ADM needs to be based *solely* on automated processing, and it must produce *legal effects* or *similarly significant effects*. To grasp better the meaning of this paragraph we need to analyse each criterion.

---

[12] Mendoza Isak, Bygrave Lee A., "The Right Not to Be Subject to Automated Decisions Based on Profiling", *University of Oslo Faculty of Law Research Paper*, No. 2017-20, 2017.

[13] Office of the Data Protection Ombudsman, *Automated Decision Making and Profiling*, Finland. Available at: <https://tietosuoja.fi/en/automated-decision-making-and-profiling>. Last visited on 23.09.2020.

Firstly, an automated decision-making system, based solely on automated means will be any processing that is operated without human intervention, and that leads to a decision upon personal data. This lack of human intervention means that, even though a human input in the system may have existed or a human may have interpreted the decision[14] in the end, the decision itself, did not have any human interference. The focal point in this definition is that it not only needs to be solely based on algorithms, but it also needs to be a full decision. After all, if we have systems that only prepare the basis for human intervention or systems that help in the interpretation of the decision humanly made, those will not be under article 22, because the decision, ultimately, is carried out by a human. Human involvement must be meaningful to align with the definition as a decision solely based on automated means. Otherwise, if the processing does not fulfil the criteria, it will not be relevant for article 22, since it will not jeopardize the data subject in a significant manner, thus being permitted. However, that does not mean that it will not fall under the scope of GDPR – if it includes personal data processing it is concerned by the Regulation.

When we read article 22, we see that one example given of ADM is profiling. Profiling is probably the most common reference to ADM that we find; nevertheless, the provision opens the scope for any other type of ADM. Hence, what can we define as profiling?[15] The GDPR describes it in article 4 (4) as the processing of personal data by automated means

---

[14] Intervention in the decision process is different from the interpretation of a decision. As described, for automated decision making to not be considered as solely automated, human intervention must comprise the making of a decision, rather than just its interpretation. When making a decision, the human has a meaningful intervention on the process, with decisive involvement and power to change the course of the automated process. On the contrary, the interpretation of an already-made automated decision would reduce the human involvement to an *ex-post* action, without the ability to change, in fact, the decision, which, in our opinions, cannot be considered as an intervention per se and, therefore, does not fall under the scope of article 22.

[15] The European Commission dedicates on its website some webpages to enlighten citizens on their data protection rights. The webpage dedicated to automated individual decision-making, including profiling is available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_en>. Last visited on 23.09.2020.

to assess, infer or predict individual aspects of a data subject such as health or working performance, personal interests, or economic situation, among other examples. Profiling creates the always desired but never achieved possibility to predict the behaviours of individuals, which can be a very useful tool for companies. These data can be collected from social media, online forms, video surveillance, among other sources. Valeria Ferraris[16] explains in her work that we can have individual or group profiling, the latter consisting of gathering and assessing data of a community or of a group of people that share the same attributes. Profiling uses algorithms to complete the correlations between the personal data that was collected and the intended result of it, like, finding a pattern in the economic behaviour of a certain group of people, regarding the opening of a specific store. Some companies use profiling to perform their recruitment, others for marketing purposes (one of the main uses of profiling); police departments can use profiling to predict certain behaviours and act upon it; and doctors can make use of it to know the right treatments to apply to a patient[17].

Following the analysis of paragraph 1, it is necessary to define "legal effects" and "similarly significant effects", for the provision to be understood completely. Regarding the first one, "producing legal effect", will be every decision or action that affects someone's rights or legal status, or even their rights under a contract. Examples of such situations could comprehend impacts on the right to vote, the right to receive a monthly pension for disability, or the ability of someone to enter in a country. Moreover, legal effects also play a role in contracts, for example, if a contract is terminated due to ADM.

The criterion of "significant similar effects" opens a broad scope for the application of article 22 (1) which might lead to confusing and uncertain situations for data controllers, when they are deciding on the use of ADM, aiming to maintain GDPR compliance. Similar effects to the legal ones will be those consequences that although do not create

---

[16] Ferraris Valeria, Bosco Francesca, Cafiero Gioacchino, D'Angelo Elena, Y Suloyeva and Koops Bert-Jaap, "Working Paper: Defining Profiling", 2013. Available at: <https://www.academia.edu/4834070/Defining_Profiling>. Last visited on 23.09.2020.

[17] Bietti Elettra, "Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR", *Institute for Research and Publication Journal*, 2017.

an impact on someone's legal rights, will, either way, have a significant weight on their lives[18]. The effect will be relevant enough if the data subject, due to ADM, finds him/herself in a situation where protection is needed because it influenced one's choices, behaviours, or circumstances. Recital 71 of GDPR gives examples of what can be thought as similar effects: the refusal of an online credit application that, even though it does not imply any right, thwarts the expectations of an individual; or recruitment that happens without any human interference and one may feel, when looking for a job, that being analysed and further on chosen or not by an e-recruiter system will have a significant impact on his/her life. WP29 refers as well to examples of situations that can significantly affect someone, such as, on an education level, in the case of someone not entering in their desired university based on an automated decision. Some of the most extreme cases of similarly significant effects can be those that lead to discriminatory outcomes. As written on the provision, a similar effect needs to be significant and here is where the threshold becomes difficult to meet. Consequently, not every automated decision will have a significant impact – for example, the recommendations of music on an app based on what you want, like or hear the most, occur due to profiling and are not prone to have a significant impact. On the contrary, there is a case for targeted advertisement that in principle cannot be considered as pertinent to be forbidden under 22 (1)[19]. According to what WP29 refers to, to understand if targeted advertising can be acknowledged as having significant similar effects, we need to see how much intrusiveness is present due to profiling or which are the particular vulnerabilities of the data subjects, in a case-by-case basis. A practical example will be if a person that is in financial debt and is known to have a gambling problem keeps being targeted with an advertisement for gambling. The vulnerabilities may lead to discriminatory outcomes and those are the cases that need to be avoided.

---

[18] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law, 2018 Edition,* April 2018.

[19] The European Data Protection Supervisor referred that targeted advertisement is an activity without significant importance to the audience that is targeted by it.

2.3. Paragraph 2

Tackling the second part of article 22, we are presented with exceptions to paragraph 1, based on the lawful processing basis that the GDPR entails in its article 6. The first one, in subparagraph (a), is the processing necessity to enter in or to perform a contract between the data subject and data controller. WP29[20] states that the data controller must be able to show this necessity, demonstrating that the usual way to conduct that contract would have been prejudicial or impractical. If any other way, that creates fewer risks on the fundamental rights of the data subject, is possible to be exercised, that shall be used.

The ICO[21] states that this necessity does not have to be considered essential, but shall be a reasonable way to achieve the parties' contractual goals. The essentiality referred by the ICO, and as stated by the EBDP on its Guidelines on the processing of personal data under article 6 (1) (b)[22], relates to the objective necessity of the processing for a "purpose that is integral to the delivery of that contractual service to the data subject".

As such, the processing must be more than useful for the performance of the contract, but it does not have to be the only way. Thus, the necessity will be determined considering the personal data and processing operations concerned and their impact on the performance or non-performance of the contractual service.

In subparagraph b) we have the permission to use ADM, if allowed either by EU Law or Member States law, to which the data controller is subject. Recital 71 gives some hints about these laws, such as the monitoring and prevention of fraud and tax evasion, as well as systems that are designed to safeguard the security of a specific service provider[23]. For

---

[20] WP 29, p. 23.

[21] Statement made on the ICO's website, in its dedicated guideline to organisations: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection–regulation-gdpr/automated-decision-making-and-profiling/when-can-we-carry-out-this--type-of-processing/>. Last visited on 23.9.20.

[22] EBDP Guidelines 2/2019 on the processing of personal data under article 6 (1) (b) GDPR in the context of the provision of online services to data subjects. Available at: <https://edpb.europa.eu/sites/edpb/files/ files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf>. Last visited on 17.4.21.

[23] WP29, p. 21.

this to be allowed, either the EU or the Member States law shall consider the protection of the freedoms and legal interests of data subjects and create safeguards when applying it. The ICO's point of view is that, when approaching companies and institutions that may wish to perform with ADM systems, even though this exception is predicted in the GDPR, the data controller needs to show that it is reasonable to do so.

The last exception regards to the consent of the data subject. The definition of consent is present in article 7 and it needs to be explicit, which means that the consent cannot be inferred from the silence of the individual. For this specific consent to be explicit, the data subject needs to be informed that the decision will be based entirely on automated systems. Dreyer and Schulz note that in the case of this specific consent, we face an intricate question[24]. Indeed, regarding ADM, data subjects will not only consent to the processing of their personal data, but they will consent as well to the automatic performance of the decision, hence this consent needs to be an extended and complex declaration. This consent should include all information required by articles 13 or 14 (depending if personal data was or was not collected from the data subject), and, specifically, the information about the existence of automated decision--making. This should include, at least, "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject", as demanded by article 13 (2) (f) or article 14 (2) (g).

3. Risks and Benefits

Although ADM is forbidden under the criteria expressed, paragraph 2 provides an exception in three situations. We believe that this occurs because, even though ADM can create some risks to data subjects, it also brings numerous benefits, especially to businesses. The prohibition from

---

[24] Dreyer Stephan and Schulz Wolfgang, "The General Data Protection Regulation and Automated Decision-making: Will it deliver?", *Bertelsmann Stiftung*, 2019. Available at: <https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GDPR.pdf>. Last visited on 23.09.2020.

22 (1) arises mainly due to the necessity of protecting the legal interest and rights of data subjects.

One of the main risks associated with ADM is the possibility of discrimination. Algorithms are designed for people, so, like humans themselves, they can carry inherent (or not inherent) biases that can provoke discriminatory outcomes regarding data subjects' characteristics, such as, their ethnic origin, sexual orientation, economic situation, gender, among others. Discrimination may arise out of the design but also from improper datasets that, for example, contain inaccurate data or in which data sampling is flawed, due to having over or underrepresent groups in the training data[25]. Recital 71 specifically addresses the question of discrimination, stating that ADM can only be admissible if it prevents discriminatory outcomes rather than provoking them.

Besides this major risk, we also have the question that, quite a lot of times, ADM is incomprehensible for individuals. Even supposing that individuals may have some information about it, as for its technological features, which involve numerous scientific methods that most of us are not familiar with, in the end, it is a black box matter. In short, the Black Box phenomenon, usually associated with AI built by machine-learning algorithms[26], considered by ICO as "one of the technical mechanisms that underpins and facilitates AI"[27], concerns to the human inability to fully understand the process of decision-making of these systems, as they are capable to arrive to determined solutions or decisions based on specific patterns of massive amounts of data, that humans, even the ones

---

[25] As an example, Buolamwini and Gebru found that facial detection technologies had higher error rates for minorities, particularly for darker females, probably due to under-representative face data sets: Buolamwini Joy and Gebru Timnit, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research: Conference on Fairness, Accountability, and Transparency*, 81, 2018, p.1–15.

[26] Machine learning algorithms are differentiated from other ones, due to their ability to learn from data, test the probabilities and make a decision, without human pre-written instructions. For a more in-depth analysis on machine learning algorithms and the black-box problematic, see Bathaee Yavar, "The artificial intelligence black box and the failure of intent and causation", *Harvard Journal of Law & Technology*, Vol. 31, 2, 2018.

[27] ICO, "Big data, artificial intelligence, machine learning and data protection", available at: <https://ico. org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Last visited on 28.04.2021.

who created the system, cannot perceive. This human inability, created, among other, by algorithmic opacity and unpredictability[28], can lead to non-transparent decisions, which consequently are more difficult to audit and review, and, ultimately, present a threat to data subjects' rights. Those same data subjects that, in a more vulnerable position than the creators of such systems, who also may not understand them, are clueless consenting with ADM.

Nevertheless, ADM advantages, especially to businesses, involve an increase in efficiency and in innovation as it allows for further innovation and less bureaucracy. These advantages are visible as well in public institutions because it also can help the judicial sector, the educational sector, healthcare, social security, and police investigations for it hands in reducing the time to collect the pieces of evidence.

4. DPIA – Data Protection Impact Assessment

To mitigate the above-mentioned risks, the GDPR provides a major tool for data controllers that allows them to ensure their processing is compliant with the regulation and to guarantee that no data breaches will occur or will not expectedly occur. The DPIA, defined in article 35 GDPR, comprises an assessment of the potential and real impact of determined processing operations on the protection of data subjects' personal data. It is considered a mandatory assessment when processing operations, particularly when new technologies are used, and considering their nature, scope, context and purposes, are likely to result in a "high risk to the rights and freedoms of natural persons"[29]. As for ADM, article 35 (3) (a) demands a DPIA when the personal aspects relating to natural persons are subject to a systematic and extensive evaluation based on automated processing, including profiling, that serve as a base for decisions that "produce legal effects concerning the natural person or similarly significantly affect the natural person".

---

[28] Burrell Jenna, "How the machine "thinks": Understanding opacity in machine learning algorithms", Big Data & Society, 2016.

[29] GDPR's article 35 (1).

The concept "systematic", though not defined in the GDPR, is interpreted by the WP29 Guidelines on DPOs[30] as meaning a systematic processing based on a system, and/or with a methodical or organised method, and/or taking place as part of a general plan for collecting data and/or carried out as part of a strategy.[31] Whereas the concept "extensive" also not defined in the GDPR, is interpreted by ICO as a processing which involves a large-scale area, a wide range of data or that affects a large number of data subjects.[32]

Nevertheless, considering the risks and impacts already mentioned[33], even if no extensive and systematic evaluation based on automated processing is conducted, we believe that it is highly likely, due to its (more or less) opaque nature, that any automated decisions which fall within the scope of article 22, will be required a DPIA, given the potential high risk to the data subjects' rights and freedoms.

WP29 points out that this provision does not refer to "solely" automated means, but rather to systems "based on automated means", which indicates that this assessment shall be conducted not only when using ADM systems as of article 22 (1), but as well when using those that are not solely automated. Subsequently, if a company already knows that its system fits under article 22 requirements, a DPIA must be conducted to assess the risks. If it falls under article 22 (1) and there are no exceptions, it cannot be admitted. This practice allows companies to move towards good policies and procedures and to consider significantly the possible dangers that may arise with their processing activities to data subjects. Specifically, regarding ADM, we understand from this provision that the data controller does not need to refrain from using it at all, but it may need to take some precautions when using some specific algorithm.

---

[30] WP29 Guidelines on Data Protection Officers (DPO), available at: <https://ec.europa.eu/ information_society/newsroom/image/document/2016-51/wp243en40855.pdf?wb48617274=CD63BD9A> Last visited on 17.04.2021.

[31] The WP29 interprets the word "systematic" as meaning one or more of the definitions provided. These definitions are alternative but might also be cumulative.

[32] Statement on the ICO's website regarding the concepts of systematic and extensive on GDPR: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when8>. Last visited on 18.04.2021.

[33] Cf. Paragraph *3. Risks and Benefits.*

5. Introducing paragraph 3

Article 22, as previously mentioned, provides that there is a general prohibition of solely automated decision-making, including profiling, which produces legal or similarly significant effects on the data subject. Though we have exceptions to this rule, suitable measures that safeguard the data subject's rights, freedoms and legitimate interests should be in place. Paragraph 3 comes along regarding those suitable measures, stating the following:

"In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." Although not mentioned, if the basis for processing is article 22 (2) (c), it is desirable that the Member State law that authorises such processing, provides for appropriate safeguarding measures as well.

5.1. The alignment with the information and access rights

Transparency, as we have stated, is one of the core principles underpinning the GDPR and acts as the background rationale for a significant number of its provisions. Specifically, regarding the ones directed to ADM, transparency poses as a foundation for the data controller's duties, as they must make sure they explain clearly and intelligibly to data subjects these processes, its consequences and provide them with tools to act against them, if they intend too[34]. Though we are focusing on a deeper analysis of this last duty, it is important to address that the safeguards provided by paragraph 3 come as a complement and reinforcement of the information and access rights stated in GDPR's articles 13, 14 and 15 as they act almost in symbiosis. Understanding the Information and

[34] Regarding this topic, Recital 60 of the GDPR states, "The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes."

Access Rights' logic can help us get a better grasp of the rationale behind paragraph 3.

Indeed, the GDPR, through its articles 13 (2) (f) and 14 (2) (g), requires controllers, when using ADM processes, to explicitly inform data subjects that they are employing these types of activities and meaningfully explain what the logic involved is and the specific consequences of such processing, in a way that is intelligible to them[35]. This does not mean that the technical process behind that automated decision must be explained to the data subject, either because that (probably) belongs to companies' trade secrets[36] or because (and mainly) the data subject will not understand nor need that kind of information, to comprehend the effects of the decision. Article 15 (h) (1), on the other hand, provides a special type of right to the data subject when giving them the possibility to obtain confirmation on whether or not personal data concerning them is being processed. If that confirms, the data subject has also the right to access that personal data and all the information already mentioned for article 13 and 14.

Providing this information to data subjects will ultimately enable controllers to ensure they are meeting the required safeguards referred to in article 22 (3) and its connected Recital 71, regarding a decision based on automated processes, as they are already equipped with meaningful information to pursue their contesting intentions.

In fact, complementing the information duties pertinent to the information and access rights with specific mechanisms that provide data subjects with the possibility to effectively exercise their rights will,

---

[35] Dreyer Stephan and Schulz Wolfgang, "The GDPR and algorithmic decision-making – Safeguarding individual rights, but forgetting society", Völkerrechtsblog, 2019. Available at: <https://voelkerrechtsblog.org/articles/the-gdpr-and-algorithmic-decision-making/>. Last visited on 25.09.20.

[36] The WP29 Guidelines, on page 17, states, "Recital 63 provides some protection for controllers concerned about revealing trade secrets or intellectual property, which may be particularly relevant in relation to profiling. It says that the right of access 'should not adversely affect the rights or freedoms of others'. (...) Controllers should not use this as an excuse to deny access or refuse to provide any information to the data subject. These rights should be considered in context and balanced against individuals' rights to have information." Indeed, as a protective mechanism for their interests, companies can make use, e.g., of non-disclosure agreements.

ultimately, reinforce article 22 (3)'s purpose of rendering automated decisions contestable.

5.2. Deepening the analysis of paragraph 3

Moving on to a more in-depth analysis of paragraph 3, it is important to understand that the 'suitable measures' required by it are only a minimum standard to be met by data controllers, but any other that can complement them in safeguarding the data subjects' rights could, of course, be considered as a good practice. Another relevant point is the fact that, although these measures seem defined as independent, they can actually be interdependent, especially the right to express his or her point of view, that is seen as a subsequent step to both the right to obtain human intervention and the right to contest the decision, as we will see.

5.2.1. Right to obtain human intervention

Human intervention is a key element in the whole paragraph. The WP29 Guidelines clearly state that any review of any automated decision must be carried out by someone who has the appropriate authority and capability to change the decision, assertively opening the possibility of human intervention when an automated decision is taken.

In a way, human intervention is meant to provide input and solve problems raised by these decisions that cannot be solved or addressed by current machine capabilities, but it can also be sustained in the necessity of preserving human dignity. Regarding the prior, since we have experience--based knowledge and intuitions, that are challenging for algorithms to represent, a human reviewer can serve as a machine-error antidote and identify mistakes committed by machines. This kind of quality control is quite crucial due to the possible large-scale harms that these decisions can cause to data subjects. Even though technology is developing at full speed and systems that can accurately codify human intuitions are already seen as a possibility, for the time being it is not something we can count on. Up until we have machines that are able to internalize the

effects of their decisions and judgements on humans, human oversight and intervention must remain a possibility for data subjects.

Notwithstanding, when it comes to decisions only based on data analysis, human intervention can be quite limited in altering the result, unless we only take into consideration the statistical correlation. Consequently, unless the human reviewer has a minimal knowledge of data analysis, in order to distinguish relevant from irrelevant correlations to the automated decision, as well as to reduce false positives[37], this human intervention may only be a formal requisite in the future. Towards a better accomplishment of this duty, a multidisciplinary team with data analysts will be essential.

5.2.2. Right to express his or her point of view

As a complement to the prior safeguard, and to allow the data subject intervention in an automated decision concerning him or her, the right to express his or her point of view is also vital.

Nevertheless, neither the provision nor the WP29 Guidelines mention clearly when, in the automated decision-making timeline, are data subjects able to communicate their point of view. It is the understanding of some scholars[38] that in a machine learning context, the data subject should be consulted prior to the final definition of the automated decision, guaranteeing in that way a more efficient process. This interpretation is supported by GDPR's article 25 (1) which establishes that the protection of the data subjects' rights – including this one – should be pursued "both at the time of the determination of the means for processing and at the time of the processing itself", therefore requiring, in this case, data controllers to provide for suitable measures at every step of the

---

[37] Regarding the occurrence of false positives, Antoni Roig in his contribution on the European Journal of Law and Technology [Vol 8, No 3, 2017] titled "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", states that "The possibility of having false positives due to meaningless statistical correlations is a major risk scenario to be tackled by human expert data analyst intervention. Obviously, even without false positives the tool can also discriminate and have negative effects on citizens."

[38] Leenes Ronald, Van Brakel Rosamunde, Gutwirth Serge and De Hert Paul, *Data Protection and Privacy: The Age Of Intelligent Machines*, Hart Publishing Ltd, Oxford, 2017.

ADM process. However, this may be quite challenging in situations where decisions are taken in response to data in real time. More clarity regarding this subject matter, either from the European Data Protection Board (EDPB) or the European Court of Justice (ECJ), in a future decision, could be helpful in this case.

5.2.3. Right to contest the decision

The wording of the GDPR using the term "contest" connotes more to a right of recourse rather than to a mere opposing, requiring data controllers at least an obligation to hear the merits of the appeal and to provide data subjects the legitimising grounds behind the decision. Indeed, the expression "right to contest the decision" makes a clear statement on the obligation to render automated decisions contestable or cease them at all. As such, more than disclosure or meaningful information, it is required a mechanism to ensure that the outcome decision will be sufficiently interpretable and the logic behind the system tractable enough, at least, to be argued against a human arbiter. For that, the controller needs to provide a simple way for the data subject to exercise these rights, or he/she will not be able to contest without fully understanding how the decision has been made and on what grounds. And that is what we find tricky in this provision.

First of all, though article 22 does not specify if the decision hereby in scrutiny has to be the final or if it could be an intermediate one in the whole automated processing spectrum, it has been discussed that a broader interpretation of the provision, in alignment with Recital 71[39], allows for contestation of an 'interim' decision or measure.

Secondly, the provision remains unclear to who the data subjects must appeal when they want to contest the decision. On this matter, the GDPR does not specify that the contestant has to appeal to a human or if that can be made to a machine. It appears however, from the approach taken in article 22, that the data subjects must at least be granted the possibility

[39] GDPR's Recital 71 clearly states that decision may include a 'measure' and if so, in a broad interpretation, we could include intermediate or 'interim' decisions: "The data subject should have the right not to be subject to a decision, which may include a measure".

of requiring human intervention in the decision-making process and, if requested by them, a human should be tasked with reviewing the decision. Having said that, it stands unclear who this human should be and how he/she will be able to review a decision or its process that may have been based on third party algorithms or on opaque machine learning systems. Nor is it clear if this human reviewer could be the same person who firstly provided this decision to the data subject, still potentially consciously or subconsciously biased towards him or her.

One might ask, taking into consideration the ambiguity involved in human-subjected appeals, if it is fairer for data subjects to be able to appeal to a machine instead. Though machines can inherently carry bias with them, as explained above in point 3, technology development is opening the possibility for it to be designed in order to disregard certain sensitive characteristics (e.g., race, age, religion, etc.), hence leading to machine learning algorithms achieving higher levels of objectivity and neutrality that humans would effectively do. This does not mean that indirect discrimination is impossible to occur, due to the correlations that can result between inputs (e.g., one may infer a person's race by their address, if they live in a specific race-limited neighbourhood) or as a result of shadowing certain groups of people on account of under representative datasets, but fairer results could be achieved using machines trained as mentioned. Nonetheless, WP29 considers human intervention as a key element in the revision of automated decisions and recommends that any review must be carried out by "someone who has the appropriate authority and the capability to change the decision", appearing to be inclined for human (and not machine) revision of automated decisions.

Lastly, neither the GDPR nor the WP29 or other EU-provided resources make a stand regarding the legal effects of this right to contestation on the decision itself. The question that remains unsolved is what happens after a decision goes through an appeal? Taking a look into 'traditional appeals', when customers disagree with a company's decision, they can either contest that decision directly to the company's responsible department or to a government provided service. They also have the possibility to take the decision to an Arbitral Centre that the company has adhered to. When they disagree with the appeal's decision, the possibility of recourse to a supervisory authority of that specific market is always available. It is our understanding that we can take inspiration from these procedural

methods, adapting them to ADM systems. Thus, it is important that data controllers provide for a specific department responsible for analysing these decisions (whether human or machine-controlled ones) and that Governmental Services, Arbitral Centres and Supervisory Authorities are technically prepared to analyse appeals that refer to ADM.

Ultimately, article 79 of GDPR grants data subjects the right to an effective judicial remedy against a controller or processor, if they consider that their rights under the GDPR have been infringed due to non-compliance with the Regulation. Data subjects also have the right to receive compensation if the infringement of the GDPR has caused material or non-material damage on them, from such controller or processor, who shall be held liable for that damage, in accordance and subject to the conditions of GDPR's article 82.

5.3. What about a right to an explanation?

Having stated all that, contesting a decision without at least a simple but meaningful explanation on the grounds behind it, would probably remain difficult for the data subjects to enforce their rights. Considering the pattern in the 'traditional world', where decisions are solely made by humans, if the concerned party disagrees with a decision attributed to him or her and intends to appeal against it, the minimum requisite for such contestation is an explanation on the reasoning of the decision. Moreover, the lawmakers behind the GDPR thought the same, at least before they released the final version of the Regulation where they included the right to an explanation as a suitable measure[40]. As we saw, the final version of the provision does not include that, however, the wording of the paragraph on "at least" indicates that other measures can be included.

It is our understanding that, the Recitals here, serve not only as a guidance for interpretation but also for a broader perception of the

[40] Prior to the release of GDPR's final version, the right to an explanation was included in the number 5 of article 20 as a suitable measure to safeguard data subjects' rights, freedoms and legitimate interests. Vid. European Parliament legislative resolution of 12 March 2014. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=PT>. Last visited on 17.04.2021.

minimum suitable safeguards, including in fact a right to an explanation of the decision reached after such assessment[41].

The discussion around the existence and enforceability of this right to an explanation has been quite inflammatory leading to lots of pages being written about it[42]. Scholars, specifically Wachter et al.[43], have argued that, while the GDPR grants a right to an *ex ante* generic explanation about the system functionality, which is almost equivalent to the traditional right to be informed (and, therefore, does not add to the information rights already in place), a right to an *ex post* specific explanation about the decision's rationale is not clearly expressed in the GDPR, besides the mention on Recital 71, which, as an interpretative mechanism, is not legally binding[44]. Nevertheless, at this point, the majority of the literature on this topic, to which we subscribe, seems to agree that this reasoning is erroneous and that, in fact, we can perceive this right to an explanation as a suitable and enforceable safeguard[45]. The WP29 upholds this interpretation as

---

[41] Recital 71 states for the matter "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, *to obtain an explanation of the decision reached after such assessment* and to challenge the decision."

[42] This matter, as mentioned, has been thoroughly discussed in literature and plenty of pages could be written about it. However, for the purpose of this paper, and in order to limit the analysis to the essential of the topic, we refer, for a more in-depth investigation, to Kaminski, Margot E., "The Right to Explanation, Explained", *Berkeley Technology Law Journal*, Vol. 34, 189, 2019, p. 190-217.

[43] Wachter Sandra, Mittelstadt Brent and Floridi Luciano, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, 2, 2017, p. 76–99.

[44] Idem. Though the position of Wachter et al. is more complex and nuanced than what was briefly explained, for the purpose of limiting to the essentiality of the topic, and as mentioned in a previous footnote, we refer, for further development, to the authors analysis.

[45] Goodman Bryce and Flaxman Seth, "European Union regulations on algorithmic decision-making and a 'right to explanation'", *AI Magazine*, Vol. 38, 3, 2017, p. 50-57 (They recognize the existence of the right to explanation in the GDPR, stating that "The law [referring to the GDPR] will also effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them."). Brkan Maja, "Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond", *International Journal of Law and Information Technology*, Vol. 27, 2, 2019, p. 91-121 ("Dismissing the possibility of the existence of the right to explanation altogether because recitals are not legally binding is too formalistic, in particular in the light of the CoJ's

well, when referring to the need for this transparency mechanism since an individual can only challenge a particular decision or express his or her view if he/she actually understands "how it has been made and on what basis.". Meaning that this right to an explanation is essential to enable data subjects to invoke the other rights explicitly enumerated in article 22 (3).

Accordingly, the kinds of information that should be provided by data controllers in this case are exemplified in those same guidelines. Indeed, it is mentioned that individuals should be provided with the categories of data that have been used in the process and why those categories are considered relevant. Furthermore, information on "factors taken into account for the decision-making process, and (. . .) their respective 'weight' on an aggregate level (. . .)" are expected to be provided as well as a simple explanation on how the profiles are built, why they are relevant to the decision-making process and how it is used for it[46].

On an ending note, companies should also make an effort to provide a simple and intelligible explanation to individuals that, mainly, are not well educated on this topic, using, for instance, visual schemes and user-friendly information.

6. Brief look over Paragraph 4

In the last paragraph of article 22, there is the reference to specific categories of data, such as health data or ethnic data which in general are

---

case law which regularly uses recitals as an interpretative aid.") and Selbst Andrew D. and Powles Julia, "Meaningful Information and the Right to Explanation", *International Data Privacy Law*, Vol. 7, 4, 2017, p. 233-242 ("Recital 71 is not meaningless, and has a clear role in assisting interpretation and co-determining positive law."). Malgieri Gianclaudio and Comandé Giovanni, "Why a right to legibility of Automated Decision-Making exists in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7, 4, 2017, p. 243-265 ("The right to obtain an explanation of the decision reached after the assessment should always be exercisable."). Kaminski Margot E., "The right to explanation, explained", *Berkeley Technology Law Journal*, Vol. 34, 1, 2019, p. 189-218 ("an individual has a right to explanation of an individual decision because that explanation is necessary for her to invoke the other rights – e.g., to contest a decision, to express her view – that are explicitly enumerated in the text of the GDPR.").

[46] WP29 p. 27-31.

forbidden to be processed, as quoted in article 9 (1). However, article 9 (2) sets some exceptions to such prohibition, and two of them, items (a) and (g), are also referred in 22 (4). If a controller uses ADM and it falls under the exceptions of article 22 (2) but the data is, for example, genetic data, it can only have a processing and a solely automated decision upon it, if the processing of that specific data is allowed. The permission will occur when the data subject has given his/her explicit consent [item (a)] or because it is a matter of public interest [item (g)]. This dual protection aims to safeguard the rights of data subjects, since this data is more sensitive and creates higher perils to individuals and, for that reason, more effective safeguards are paramount.

7. Children and Profiling

When the GDPR aims to protect data subjects from the automated decision-making systems, it does not specify in article 22 which subjects it refers to, therefore we could admit that it equally includes children. Under Human Rights Law, children are under extreme protection and their rights always need to be safeguarded. Respectively, Recital 71 refers that children shall not be subject to ADM when any of the exceptions predicted in the second paragraph occur. Even though it is projected in the recital, it is not binding, which leaves companies and organizations in a glassy floor, where doubt has the main role. To give some light to data controllers WP29 advises that, if the ADM fits in one exception of article 22(2) and the processing's end is the welfare of children, such as health care or education, it can be admissible. Anyhow, the safeguards of article 22 (3) and the best interest of the child shall be figured perpetually.

8. Good Practices for Data Controllers on the use of ADM

More than a mere explanation, it is inherent in the formulation of the rights conceded by paragraph 3, that this provision requires the implementation of the necessary mechanisms to ensure its ultimate goal – rendering automated decisions contestable.

As an effort to ease the concerns of data controllers, companies and organizations on having to completely disregard automated decisions, WP29 provided suggestions on good practices to apply, to ensure the compliance with the GDPR, such as, the implementation of regular quality assurance checks on their systems; the conduction of internal or external audits to the algorithms used or developed by machine learning systems, depending on the level of risk of the decisions on the individuals' sphere; the application of anonymisation or pseudonymisation techniques to ensure a higher level of protection; the strict compliance with the data minimisation principle, by establishing clear and strictly necessary retention periods of the personal data processed[47].

In line with the concerns brought by companies, we could say that the GDPR could have defined the "suitable safeguards" in the provision, to restring or impose determined measures, but did not. Their choices provide a possibility for companies to argue that the definition of those safeguards was meant to be flexible and adaptable to the market. It is our point of view that with the implementation of these and other good practices they can still conduct automated decision-making processes when allowed by the legislation.

Conclusion

Automated decision-making systems that have zero human intervention are considered great threats to data subjects' rights and freedoms. Article 22 (1) must be understood as a general prohibition of certain types of automated decisions and a passive right that controllers have to observe when taking them, without an active claim from the data subject. The criteria of this prohibition are quite specific, however, the threshold becomes thinner when the significant similar legal effects need to be assessed, as it is a broad undefined concept that can be assessed under different perspectives to determine if an automated decision falls within the scope of the article. The data controller shall conduct this assessment whenever an automated decision is at place, according to article 35 (3) (a).

---

[47] Other suggestions are provided in Annex 1 of WP29, p. 31-32.

Data Protection Impact Assessment is an excellent mechanism for ensuring compliance with the GDPR and it should be carried out every time a processing takes place.

The article analysed also requires, in paragraph 3, the implementation of suitable safeguards, when the automated decision falls under the exceptions of paragraph 2. Those include the right to obtain human intervention, to express his or her point of view and to contest the decision. Though the legal consequences of these rights remain quite unclear and require further development by a competent entity, like the EDPB or the ECJ, in the context of a new decision, these are seen as a minimum standard to be met by data controllers, that can and should provide more measures to ensure data subjects' protection.

On that note, though not explicit in the provision itself, a right to an explanation is considered to play an essential role in the exercise of the other suitable safeguards. Indeed, to counteract the maleficence algorithmic decisions, it is our understanding that all decisions based on automated decision making must be possible to be explained and understood not only by the subjects of those decisions but also by those who work side by side with this technology.

In sum, this article argued that data controllers, companies and organizations can still conduct these automated decision-making processes, when allowed by the legislation, and if they implement some good practices as a meaning to achieve the ultimate goal of this provision – protecting the data subjects' rights, freedoms and legitimate interests.

Dados e Inteligência Artificial: os efeitos jurídicos da discriminação algorítmica

Lucas Cortizo*

Resumo: O texto propõe-se a fazer uma análise sobre conceitos básicos de inteligência, inteligência artificial (IA), discriminação e discriminação algorítmica, interligando-os a fim de analisar juridicamente os respetivos efeitos tecnológicos. Para isto, o artigo realiza um levantamento de como o uso dos algoritmos de IA (que tomam decisões automatizadas) podem adotar uma postura discriminatória, sem prejuízo do princípio da neutralidade tecnológica. Neste levantamento sobre uma possível discriminação pelo próprio sistema de IA, um dos elementos analisados são os dados. Dados estes que são utilizados no treinamento dos sistemas de decisão, mas no cenário dos mesmos estarem enviesados, analisa-se a possibilidade do algoritmo emitir uma decisão discriminatória. Neste sentido, casos concretos são trazidos para evidenciar na prática como uma discriminação algorítmica tem efeitos jurídicos, atingindo inclusive Direitos Humanos e Princípios Fundamentais.

Palavras-chave: *inteligência, artificial, discriminação, direito, algoritmo.*

Abstract: The text proposes an analysis on basic concepts of intelligence, artificial intelligence (AI), discrimination and algorithmic discrimination, interconnecting them in order to legally analyse their respective technological effects. To do so, the article

* Advogado na Autoridade Nacional de Proteção de Dados do País de Malta; Representante de Malta na European Data Protection Board (EDPB) nos seguintes expert subgroups: International Transfers e Social Media; Representante de Malta na Global Privacy Assembly e na Common Thread Network; Participante da estratégia nacional de implementação da Inteligência Artificial em Malta; Especialista e Mestre em Direito e Tecnologia pela Universidade do Minho, Braga, Portugal; Graduado em Direito pela Universidade Federal de Pernambuco, Brasil; Coautor do livro União Europeia Interop 2019. Capítulo sobre Blockchain e e-Government, tendência da tecnologia na Administração pública; Fundador do Podcast "Direito Digital Cast"; Professor de Direito e Tecnologia em diversas instituições; Membro da European Artificial Intelligence Alliance, Bélgica.

conducts inquiries on how the use of AI algorithms (which make automated decisions) can adopt a discriminatory behaviour, without prejudice to the principle of technological neutrality. In such analysis on the possible discrimination by the AI system itself, one of the elements analysed is data. These data are used to train the decision systems, but in the scenario that they are biased, it is analysed the possibility of the algorithm issuing a discriminatory decision.In this sense, concrete cases are brought to show in practice how an algorithmic discrimination has legal effects, affecting even Human Rights and Fundamental Principles.

Keywords: *intelligence, artificial, discrimination, law, algorithm.*

Introdução

Nos últimos anos, uma área que tem sido bastante comentada e discutida é a inteligência artificial (IA), entretanto não foi ainda atingido um consenso sobre o que seria entendido por IA[1]. E dentro desta extensa área do conhecimento, o presente texto propõe-se, inicialmente, a fazer uma análise tanto do conceito de inteligência, como também aprofundar sobre a modalidade de inteligência que se enquadra como artificial. A análise conceitual também almeja definir o termo discriminação com intuito de, posteriormente, delimitar a discriminação algorítmica, para assim interligar conceitos de IA e discriminação, estudando os seus possíveis efeitos jurídicos.

Para estabelecer os mencionados efeitos jurídicos, o presente artigo realiza uma análise de quais seriam as causas para um eventual uso de algoritmos de IA[2] que possam resultar numa postura discriminatória[3].

---

[1] De acordo com Bertolini: "Regular inteligência artificial requer sua definição. Ainda não existe nenhum consenso sobre o que é entendido por IA". Ver mais em Bertolini, Andrea. *Artificial Intelligence and Civil Liability.* Policy Department for Citizens' Rights and Constitutional Affairs. Parlamento Europeu, 2020. Tradução livre.

[2] Algoritmos de IA são aqueles que tomam decisões automatizadas.

[3] Fala-se em "uso de algoritmos" e não algoritmos em si em respeito à neutralidade tecnológica, prevista no Considerando 15 do Regulamento Geral sobre a Proteção de Dados (RGPD), cf. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

Neste levantamento sobre uma possível discriminação pelo próprio produto do sistema de IA, um dos elementos analisados são os dados. Dados estes que são a matéria-prima no treinamento dos sistemas de decisão. Por isso é necessário estabelecer até que ponto o treinamento de IA com dados enviesados pode conduzir o algoritmo a uma decisão discriminatória.

E diante de uma possível relação entre dados de treinamento e resultados discriminatórios, o presente artigo traz casos concretos para analisar, na prática, se uma discriminação algorítmica pode ter repercussões na esfera jurídica dos indivíduos e atingir inclusive Direitos Humanos e Princípios Fundamentais.

1. Considerações iniciais sobre inteligência

Primeiramente, é importante traçar as noções basilares do que seria inteligência, não apenas do ponto de vista artificial, mas também do ponto de vista humano. A partir do momento que o próprio ser humano se intitulou o único ser racional do planeta, o monopólio da sabedoria foi definido pelo mesmo, sendo o único ser vivo a falar sobre inteligência ou considerar que é inteligente.

No momento em que seres humanos começaram a ter a consciência de que eram seres inteligentes, passou a existir um interesse crescente em desenvolver o conhecimento científico[4]. Uma competição histórica entre povos, que movidos por desenvolvimento científico, passaram a medir, comparar, e competir por conhecimento – todavia, ainda antes de amplamente definir o conceito de inteligência. Não obstante, pela forte relação que existe entre desenvolvimento científico e poder de conquista, historicamente, as grandes fontes da inteligência, representadas pelas grandes mentes da ciência, sempre foram cobiçadas pelas grandes civilizações[5].

---

[4] WARNER defende que esta corrida acontece ao longo da História e remete a ciclos. Ver mais em Warner, Michael. *The Rise and Fall of Intelligence: an international security History*. Georgetown University Press, 2014.

[5] Referência ao fenómeno do "intellectual theft" cf. Mulkay, Michael J. "Norms and ideology in science". *Social Science Information*, v. 15, n. 4-5, 1976, p. 637-656.

É difícil encontrar um parâmetro objetivo para medir a inteligência. Principalmente, no contexto da geopolítica e da corrida científica, o que vai existir é uma análise de possível ganho, ou uma análise dos benefícios de uma inteligência individual que se juntará a outras para criar uma inteligência geral. E este foi o critério que fez com que cientistas, artistas e várias mentes notáveis das mais diversas áreas fossem disputadas por impérios na busca de expandir o seu domínio, não apenas territorial, mas intelectual[6].

A Guerra Fria representou uma parte da História em que cresceu uma cobiça pelo desenvolvimento científico[7], mas a própria II Guerra Mundial, em momento anterior, também foi resolvida pela ciência: a exemplo da invenção de Alan Turing, o computador, que foi uma das mais valiosas armas do Reino Unido contra a Alemanha[8]. A obra de Turing, por sua vez, traça um paralelo entre o conceito de inteligência sob a perspetiva da máquina, ao fazer a indagação de se seria possível as máquinas pensarem.

O paradoxo que surge é que, à medida que as grandes civilizações e impérios foram evoluindo, nunca houve tanto esforço no desafio de conceituar e avaliar de forma objetiva o que seria inteligência e qual sua extensão em cada pessoa. Os Estados Unidos e a União Soviética ao disputar uma grande mente não estavam prioritariamente em busca de provar, em caráter objetivo, o grau de inteligência de algum cientista estrangeiro, nem se aquele indivíduo oferecia um risco para os demais pensadores nacionais. E é por isso que a inteligência não costumava ser vista como uma ameaça interna, mas sim como objeto de desejo para aquisição externa pelos grandes países. Então, desde a revolução científica, a inteligência passou a ser vista como *commodity*[9].

---

[6] Para aprofundar sobre a corrida científica, principalmente no contexto da Guerra Fria, veja-se Nelson, Richard R.; Romer, Paul M. "Science, economic growth, and public policy". Challenge, v. 39, n. 1, 1996, p. 9-21.

[7] A cobiça pelo desenvolvimento científico foi marcada por um patrocínio à pesquisa e ao desenvolvimento acadêmico, muitas vezes distorcido e aumentado pelos Estados Unidos e União Soviética, nos termos de Hounshell, David. "The Cold War, RAND, and the generation of knowledge, 1946-1962". *Historical Studies in the Physical and Biological Sciences* 27.2 (1997): 237-267.

[8] Sobre este contexto, recomenda-se a obra: Hodges, Andrew. *Alan Turing: The Enigma*. Random House, 2012.

[9] Neste sentido, Pritchard defende que historicamente o conhecimento sempre foi um valor distintivo. Veja-se mais em Pritchard, Duncan. "The value of knowledge". *The Harvard Review of Philosophy*, v. 16, n. 1, 2009, p. 86-103.

Contudo, quando a inteligência chega à máquina, ela passa a ser atacada sob outro ponto de vista[10]. Se há quem considere a obra de Turing como a primeira que traz as bases do amplo ramo que seria posteriormente denominado Inteligência Artificial (IA)[11], a preocupação em definir e medir a capacidade das máquinas pensarem acompanhou a evolução deste conceito de IA. Indo além, construiu-se um ideal de apreensão, pois pela primeira vez foi criada uma tecnologia que poderia ultrapassar a inteligência humana[12].

Por isso, ao surgir uma inédita entidade que computa e processa informações de uma forma mais rápida que a humana, passou a haver uma preocupação em desenvolvê-la, mas simultaneamente entender seus limites. Mas, entender os limites de uma tecnologia pelo senso comum tem sido um tarefa que usa uma "régua humana" limitante: devem os limites de qualquer inteligência ser mesmo a própria inteligência humana? Até porque o conceito de inteligência surgiu por autoproclamação[13], e em consequência disto, existiu sozinho por centenas de anos em monopólio humano.

Neste momento, pode-se questionar que plantas e animais também são inteligentes. E é de admirar a complexidade e as características únicas que alguns deles possuem, mas o presente objetivo não é fechar uma conceituação de algo que jamais foi pacificamente conceituado. Busca-se mostrar que pela primeira vez, o ser humano sentiu-se ameaçado por reconhecer que o monopólio da inteligência, autoproclamado pelo "único animal racional"[14], agora poderia ser um oligopólio em que o ser

---

[10] Ponto de vista que supõe a inteligência artificial como ameaça, sustentado por grandes nomes como Stephen Hawking. Ver mais em: Cellan-Jones, Rory. "Stephen Hawking warns artificial intelligence could end mankind". BBC news, v. II, 2014, p. 10.10.

[11] Neste sentido, Moor, James (Ed.). *The Turing test: the elusive standard of artificial intelligence*. Springer, Science & Business Media, 2003. & "the father of AI and computer science" em Guo, Ting. "Spirituality as reconceptualisation of the self: Alan Turing and his pioneering ideas on artificial intelligence". *Culture and Religion*, v. 16, n. 3, 2015.

[12] Neste sentido, há várias obras como Kurzweil, Ray. *The age of spiritual machines: When computers exceed human intelligence*. Penguin, 2000. & French, Robert M. *The Turing Test: the first 50 years. Trends in cognitive sciences*, v. IV, n. 3, 2000, p. 115-122.

[13] Nenhum outro ser vivo jamais se proclamou inteligente cf. Pearce, John M. "Animal learning and cognition: an introduction". Psychology press, 2013.

[14] Conceito de Deleuze acerca da unicidade da racionalidade humana. Ver mais em: Rocha, André Menezes. "Formação da razão na ética de Espinosa, segundo Deleuze". *Cadernos Espinosanos*, v. XVI, 2007, p. 89-100.

humano deveria aprender a viver em relação simbiótica com os dispositivos inteligentes criados por si próprio.

Ao longo dos tempos, alguns métodos foram criados para objetivar a inteligência e um dos mais conhecidos é o método do "Quoeficiente de Inteligência" (Q.I.)[15]. Apesar te ter sido bastante utilizado, atualmente esta metodologia é considerada obsoleta por apenas exigir uma das várias formas que a inteligência pode assumir[16]. O teste de Q.I. preza pela inteligência lógico-matemática, favorecendo grandes mentes como Tesla, Newton e Einstein. O próprio Einstein teria afirmado que todos nós somos gênios, mas se você julgar um peixe pela sua capacidade de escalar uma árvore, ele passará o resto da vida acreditando não ser[17].

É por conta dessas múltiplas facetas que a inteligência pode assumir que muito se fala da Teoria das múltiplas inteligências de Gardner[18]. Listando as diversas formas, Gardner traz a inteligência linguística, musical, espacial, corporal cenestésica, intrapessoal, interpessoal, naturalista e existencial. E pela pluralidade deste conceito, faz-se necessário delimitar as perspetivas pela qual o âmbito do conceito de inteligência pode ser observada, o qual se passa a fazer a seguir.

2. Os limites da Inteligência Artificial

Se o parâmetro da inteligência for apenas uma de suas facetas, representadas pela excelência ao jogar xadrez, pode-se responder à pergunta de Turing: sim, as máquinas já pensam e já ultrapassaram o ser humano no critério inteligência. Mas se este critério de inteligência for um grande leque de diversas representações, a resposta do vencedor da competição

---

[15] Quociente de inteligência (QI), conforme Gould, Stephen Jay, *The mismeasure of man*. Nova York, Norton, 1996, p. 30-35.

[16] Ideia desenvolvida por Gould que na obra "a falsa medida do homem" demonstra os principais erros da investigação científica da inteligência humana escorada no quociente de inteligência (QI). Veja-se em Gould, Stephen Jay, ibid.

[17] Colombo, Jorge A. "A critical view of the quest for brain structural markers of Albert Einstein's special talents (a pot of gold under the rainbow)". *Brain Structure and Function*, v. 223, n. 5, 2018, p. 2515-2518.

[18] Ver mais Gardner, Howard. *A Multiplicity of Intelligences*. Scientific American, 1998.

virtual "inteligência humana *versus* inteligência artificial" não se limita a uma resposta simples.

Ademais, merece ainda levantar o potencial da IA para cada vertente de cada tipo de inteligência, o que pode levar a diferentes respostas. Por exemplo, poderá a IA compor músicas de uma forma melhor que os compositores humanos? Existem diversas soluções no mercado musical que oferecem auxílio por IA para músicos, sugerindo e complementando o trabalho de composição musical[19].

Uma das várias plataformas com inteligência artificial é a Amper[20]. Apesar de ser considerada uma IA que compõe músicas, é apenas um dos vários programas semelhantes que os músicos podem usar para compor músicas, incluindo Magenta do Google, Flow Machines da Sony e Jukedeck[21].

O que existe de comum nestas plataformas de IA musicais é que elas precisam de escolhas humanas. As máquinas não criam músicas por si só, mas precisam de intervenção humana prévia para definir os seus fins e meios, a exemplo da escolha da tonalidade da música, instrumentos específicos, as batidas por minuto do ritmo, etc. Então, a IA oferece uma gama de ferramentas que trabalham ritmos e estilos criados e definidos pelos humanos. Se esta capacidade for considerada "inteligência musical"[22], a IA vai apresentar uma das facetas descritas acima.

Se as máquinas puderem pensar, e, ainda, se apresentarem características que sejam enquadradas nas mais diversas inteligências que existem, vai ser discutido se aquilo que a IA produz corresponde a um processo de criatividade[23].

---

[19] Barrett, Maura; Ward, Jacob. *AI can now compose pop music and even symphonies. Here's how composers are joining in*. Disponível em: <https://www.nbcnews.com/mach/science/ai-can-now-compose-pop-music-even-symphonies-here-s-ncna1010931> Acedido a: 29.11.20

[20] Barrett, Maura; Ward, Jacob. *Ibid*.

[21] Briot, Jean-Pierre; Pachet, François. "Deep learning for music generation: challenges and directions". *Neural Computing and Applications*, v. 32, n. 4, 2020, p. 981-993.

[22] Tradução livre para *Musical Intelligence,* conforme definido por Roads, Curtis. "Artificial intelligence and music". *Computer Music Journal*, v. 4, n. 2, 1980, p. 13-25.

[23] Para aprofundar sobre este questionamento da criatividade na IA, veja-se Boden, Margaret A. "Creativity and artificial intelligence". *Artificial intelligence magazine,* v. 103, n. 1-2, 1998, p. 347-356.

Ainda sob o desígnio específico de uma IA para fins musicais, um algoritmo de aprendizagem que – ao ser treinado com todas as músicas de Beethoven – cria uma sinfonia inédita que poderia ter sido composta pelo músico e não foi, não há consenso se isto torna o algoritmo criativo. Até pelo facto de que a criatividade, assim como a inteligência, é um conceito amplo e subjetivo[24], não se deseja aqui debater a qualidade de uma composição de IA, mas se tal composição representa um exercício inteligente por parte da IA.

Desta forma, os algoritmos de IA oferecem ferramentas cada vez mais completas nas mais diversas áreas do conhecimento, não se limitando a cálculos computacionais, mas enveredando em searas artísticas, seja para auxílio dos indivíduos da área, seja como entidades inteligentes e criativas.

Ainda merece destacar o presente conceito de inteligência mais aprofundado, à luz da inteligência humana como parâmetro, o que difere do conceito de *smart devices* desenvolvido nos últimos anos. Apesar de em tradução literal significar aparelhos inteligentes, o grau de profundidade objetivado não pretende alcançar (ou ultrapassar) a inteligência humana. Merece ser trazida a definição de Lazar *et al*[25] sobre o movimento dos objetos *smart*: os dispositivos inteligentes surgiram na promessa de oferecer aos utilizadores uma "riqueza de informações que lhes permitirá se tornarem as melhores versões de si mesmos"[26].

A mesma obra mostra o quão descartáveis estes aparelhos podem se tornar ao coletarem demasiada informação e não atingirem o objetivo que os torna *smart*. Para citar como exemplo, muitos rastreadores "inteligentes" de atividades físicas fornecem aos utilizadores o número de medidas tomadas naquele dia, na pretensão de que o conhecimento dessas informações causará mudanças no estilo de vida, tais como o aumento da atividade física. Se a coleta de informações de cada passo

---

[24] Segundo Boden, criatividade é definível e há uma possibilidade da IA atingir os três pilares que a sustentam. "*Creativity isn't magical. It's an aspect of normal human intelligence, not a special faculty granted to a tiny elite. There are three forms: combinational, exploratory, and transformational. All three can be modeled by AI*". Cf. Boden, Margaret A. "Computer models of creativity". *AI Magazine*, v. 30, n. 3, 2009, p. 23.

[25] Lazar, Amanda et al. "Why we use and abandon smart devices". *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing*, 2015.

[26] Lazar, Amanda et al. Ibid. p. 635. (Tradução livre)

dado, sob a permissão de localização geográfica, não impactar e gerar mudança efetiva na vida do utilizador, o aparelho vai representar uma forma de coletar dados em excesso, por opção do próprio titular dos dados[27].

O movimento em voga de adicionar o selo *smart* em televisão, frigorífico ou em sensores diversos, sem que o utilizador explore em plenitude aquela "inteligência" oferecida, representa um uso que, além de não ser inteligente sob o ponto de vista da teoria de Gartner[28], o aparelho apenas vai ser resumido em coleta excessiva de dados pessoais, sem uma contraprestação a longo prazo ao seu utilizador. Se um objeto que anteriormente não acedia à *internet*, passa a aceder, não deveria, necessariamente, ser considerado inteligência artificial, sequer ganhar o selo de aparelho inteligente[29].

Ante o exposto, conforme discutido acima sobre os conceitos de inteligência, é aconselhável não perceber o fenômeno dos *smart devices* de forma literal, porque muitos não oferecem sequer recursos de Inteligência Artificial de forma predominante[30]. Via de regra, tais aparelhos apenas coletam dados para retribuir em novas funções de interconexão a outros aparelhos. O selo *smart* é muito mais um propósito comercial desvinculado a qualquer vontade de conferir inteligência ao aparelho, mas sim agregar valor a produtos comercializáveis.

E, portanto, o conceito apresentado de IA acaba por representar um grande escopo. O âmbito, para fins de investigação, segue o proposto por Fetzer que limitou o conceito de IA a apenas sistemas dotados da capacidade de aprender ou entender a partir da experiência[31]. E dentro deste âmbito, no qual a aprendizagem é requisito, a IA pode ser

---

[27] Ver mais em: Lazar, Amanda, et al. Ibid.

[28] Gardner, Howard. Ibid.

[29] A diferença técnica entre *smart devices* e algoritmos de IA vem definida em Schalkoff, Robert J. *Artificial intelligence: an engineering approach*. McGraw-Hill, 1990.

[30] A ausência de inteligência propriamente dita em aparelhos *smart* é bem observada em LEESA-NGUANSUK, Suchit. *Smart device market not so smart*. Disponível em: <https://www.bangkokpost.com/business/1075440/smart-device-market-not-so-smart> Acedido a: 02.12.2020

[31] Fetzer, James H. *Artificial intelligence: Its scope and limits*. Springer Science & Business Media, 2012.

subdividida em áreas como planejamento automatizado, aprendizagem de máquina, processamento de linguagem natural, robótica, dentre outras denominações[32].

Ao contrário desta conceção, a IA pode ser erroneamente associada a utilizações que não correspondem tecnicamente a uma inteligência propriamente dita pela ausência da mencionada capacidade de aprender. Mas esta associação pode ser proveniente da dificuldade de enquadramento do âmbito da IA pela complexidade dos conceitos abstratos trazidos pela própria expressão. O conceito de inteligência humana já oferece um significativo teor de subjetividade e de complexa limitação objetiva, por isso a inteligência da máquina, computador ou qualquer outra entidade que esteja abrangida pela ideia de "artificial" vai passar pela mesma dificuldade[33].

A dificuldade conceitual não pode ser utilizada como um artifício na perigosa generalização do conceito de IA, muitas vezes ligado a usos que não apresentam aprendizagem algorítmica, ou qualquer outra forma de criatividade e inteligência por parte da entidade computacional. Dito isto, parte-se a uma problemática que emerge do processo específico a respeito da aprendizagem de máquina[34], cujos resultados apresentam interpretações estatísticas que podem ser discriminatórias aos indivíduos a quem a decisão automatizada foi destinada.

3. A origem da discriminação

Se o presente objetivo é entender como a IA pode oferecer resultados discriminatórios, e uma vez introduzidos os conceitos de inteligência e de inteligência artificial, precisa-se apresentar previamente o conceito da discriminação. Esta pode ser percebida a partir de uma conduta

---

[32] Neste sentido, ver em Russell, Stuart; Norvig, Peter. *Artificial intelligence: a modern approach*. GEN LTC, 2002.

[33] Na dicotomia entre inteligência humana e inteligência artificial, cf. Kurzweil, Ray. Ibid.

[34] Tradução de *machine learning* cf. Ongsulee, Pariwat. "Artificial intelligence, machine learning and deep learning". In: *2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE)*. IEEE, 2017. p. 1-6.

de transgredir direitos humanos[35], mas na essência, a discriminação parte de outro princípio fundamental que é a igualdade entre os seres humanos.

A construção da discriminação deve ser à luz da prévia compreensão acerca do paradigma mundial que define a igualdade entre os povos[36]. Esta noção de igualdade entre povos, etnias e indivíduos de maneira isolada, foi adotada internacionalmente aquando da criação da Declaração Universal dos Direitos Humanos[37], que estabeleceu o princípio ético universal da igualdade.

A igualdade é um princípio que não funciona sob a ótica de igualdade absoluta entre indivíduos. A igualdade foi construída para ser interpretada à luz da isonomia material, uma vez que o mandamento constitucional não estabelece o tratamento de todos os indivíduos da mesma forma. A igualdade material orienta para um tratamento desigual na medida em que haja desigualdade. Em outras palavras, segundo o conceito aristotélico: "Entre semelhantes, a honestidade e a justiça consistem em que cada um tenha a sua vez. Apenas isto conserva a igualdade. A desigualdade entre iguais e as distinções entre semelhantes são contra a natureza e, por conseguinte, contra a honestidade"[38].

Portanto, desde Aristóteles, o tratamento diferenciado para que seja diferente não representa discriminação de conotação negativa pela noção de isonomia material. Conforme defende Sen[39], o objetivo da igualdade é preservar a individualidade, sem ignorar as diferenças culturais e materiais de cada indivíduo, a fim de uma busca pela equiparação de oportunidades. E é nesta análise de oportunidade que deve pender a balança imaginária

---

[35] Neste sentido, veja-se Vierdag, Egbert Willem. *The concept of discrimination in international law: with special reference to human rights*. Springer Science & Business Media, 2012.

[36] Lindoso, Maria Cristine Branco. *Discriminação de gênero em processos decisórios automatizados*. Repositório Universidade de Brasília, 2019.

[37] Organização das Nações Unidas. *Declaração Universal dos Direitos Humanos*, 10 de dezembro de 1948. Disponível em: <http://www.un.org/en/universal-declaration-human-rights/> Acedido a: 29.11.20.

[38] Conforme Aristóteles. *Política*. Coleção a obra prima de cada autor. Le livros. Disponível em <file:///C:/Users/ADM/Downloads/Livro%20A%20Politica%20-%20Aristoteles.pdf> Acedido a: 02.02.2020; p. 40.

[39] Sen, Amartia. *The idea of justice*. Belknap Press, 2011, p. 293-295.

que avalia a conduta como um tratamento diferenciado isonômico para um tratamento discriminatório.

Apesar de ter sido adotada na seara mais específica da discriminação de gênero, a definição adotada na Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Contra a Mulher, conforme explicado por Rios *et al*[40], ajuda na conceção da discriminação como qualquer distinção, exclusão, restrição ou preferência que tenha o propósito ou o feitio de anular ou prejudicar o reconhecimento, gozo ou exercício em pé de igualdade de direitos humanos e liberdades fundamentais nos campos econômico, social, cultural ou em qualquer campo da vida pública[41].

É imperioso destacar que esta definição de discriminação é abrangente do ponto de vista de atitudes (ao utilizar o termo "qualquer" antes de várias condutas), mas faz uma restrição relevante no que concerne aos efeitos destas condutas. Deve existir – intrinsecamente ao conceito discriminatório – uma violação jurídica de caráter de direitos humanos e liberdades fundamentais. Esta jusfundamentalidade é o parâmetro para separar um tratamento diferenciado isonômico[42] do tratamento discriminatório.

Por isso é que, quando a igualdade dos povos passou a ser um direito humano reconhecido internacionalmente, ao Estado passou a ser exigido a adoção de uma verdadeira atuação positiva para a equiparação de oportunidades na promoção do tratamento diferenciado isonômico, em nome da valorização de todas as vidas humanas, conforme foi desenvolvido por Dworkin[43]. E esta mencionada atuação positiva do Estado

---

[40] Veja-se em Rios, Roger Raupp; Silva, Rodrigo da. "Democracia e Direito da Antidiscriminação: interseccionalidade e discriminação múltipla no direito brasileiro". *Revista de Ciência e Cultura*, São Paulo, v. 69, n. 1, 2017, p. 44-46.

[41] Conceito adaptado da previsão do artigo 1º da Convenção sobre a Eliminação de Todas as Formas de Discriminação Contra as Mulheres Aprovada pela Assembleia Geral das Nações Unidas em 18 de dezembro de 1979. Disponível em <https://www.unicef.org/brazil/convencao-sobre-eliminacao-de-todas-formas-de-discriminacao-contra-mulheres> Acedido a 02.02.2020.

[42] Justificado pela inclusão e prática da isonomia material como desígnio da justiça.

[43] No conceito prático de "*equality*" a igualdade de oportunidades foi levada em consideração. Veja-se em Dworkin, Ronald. *Sovereign Virtue. The Theory and Practice of Equality*. London, England: Harvard University Press, 2002, p. 390.

não diz respeito apenas ao sentido de atuação jurisdicional mediante provocação do Judiciário por parte daqueles que sofreram alguma discriminação.

A atuação jurisdicional obedece ao princípio da inércia do Judiciário, que precisa de tal provocação do interessado para uma possível composição da lide[44]. A não discriminação passa a ser um direito com reflexos constitucionais reconhecidos que demanda a atuação positiva estatal independente de provocação, como por exemplo, iniciativa do Legislativo para combater a discriminação, ou programas do Executivo para coibir práticas discriminatórias, sendo a necessidade de combater a discriminação um ponto de convergência entre os três Poderes estatais, por sua elevação a direito humano reconhecido.

Portanto, a discriminação deve ser interpretada como uma violação de direitos humanos, com devidos efeitos jurídicos[45]. A juridicidade como requisito para a discriminação passa a funcionar como um elemento que confere segurança jurídica à própria proteção contra a discriminação, uma vez que evita a banalização do termo[46]. Não se deve generalizar a interpretação para abranger qualquer tratamento diferenciado sendo discriminatório, porque diversas vezes a diferença de tratamento vai ser em decorrência da isonomia material e no combate a uma desigualdade existente.

É sob este prisma que a discriminação praticada por sistemas de inteligência artificial vai ser analisada. Não se busca analisar cada efeito que uma decisão automatizada pode gerar, mas sim os casos em que o resultado de um sistema de IA pode gerar efeitos jurídicos indevidos na vida de algum indivíduo.

---

[44] Para aprofundar sobre a inércia e outros princípios da teoria geral do processo civil, veja-se Didier Jr., Fredie. *Sobre a Teoria Geral do Processo.* v. II. Salvador: Editora Jus Podivm, 2013.

[45] Nos termos do Artigo 7 da Declaração Universal dos Direitos Humanos. Disponível em <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos> Acedido a 19.04.21

[46] Sobre os riscos da banalização no contexto da diversidade étnico-cultural, veja-se Roshwald, Aviel. "Between Balkanization and Banalization: Dilemmas of Ethno-cultural Diversity". *Ethnopolitics,* v. 6, n. 3, 2007, p. 365-378.

4. A discriminação científica precedente à discriminação algorítmica

Antes de debater os algoritmos e seus efeitos, precisa-se trazer um problema que antecede a própria criação das mais diversas tecnologias. Apesar da tecnologia, por si só, ser um ponto final neutro, precede-lhe uma jornada feita por indivíduos, técnicos de alguma área do conhecimento e cientistas, que movidos pelas mais diversas motivações, buscam novos resultados. Ocorre que, segundo Cowan[47], desde os primórdios do desenvolvimento tecnológico não existe igualdade de participação na construção do conhecimento. A autora defende que um dos primeiros ambientes em que a tecnologia da informação revolucionou a vida cível foi o ambiente doméstico; mas ocorreu de forma incongruente.

Para ilustrar a origem da desigualdade tecnológica, Cowan cita os primeiros eletrodomésticos no contexto da sociedade patriarcal: os aparelhos iriam ser utilizados pelas mulheres, excluídas do mercado de trabalho e presas no âmbito doméstico, mas inexistiam mulheres participando da produção destes aparelhos. Havia uma inadequação do uso da tecnologia em relação à realidade das mulheres em decorrência da falta de participação feminina na vida científica[48].

Não é distante a correlação entre sub-representação de mulheres (ou qualquer outro grupo social) na produção do conhecimento e um desenvolvimento científico baseado na desigualdade. A pluralidade social na produção científica auxilia na consecução de usos tecnológicos positivos na esfera individual e coletiva, uma vez que os produtos da ciência são institutos que modificam a sociedade e atingem a esfera jurídica humana. Por isso é que, a fim de reduzir futuros efeitos discriminatórios, segundo a obra de Bray[49], há de se encontrar soluções para que os efeitos da desigualdade possam ser minimizados no (e através do) campo da ciência e da tecnologia.

Conforme é visto a seguir, a discriminação algorítmica pode atingir diversas minorias. Os grupos de notáveis cientistas da computação

---

[47] Cowan, Ruth. *More Work for Mother: The Ironies of Household Technology from the Open Hearth of the Microwave*, Basic Books, New York, 1983.

[48] Cowan, Ruth. Ibid.

[49] Bray, Francesca. "Gender and Technology". *The Annual Review of Anthropology*, 2007.

que desenvolvem os algoritmos deveriam precaver-se do tratamento discriminatório que resulta em danos jurídicos a serem reparados. Uma das formas de evitar danos discriminatórios seria antecipadamente promover, ainda na etapa de criação do sistema inteligente, a formação de grupos de desenvolvimento mais plurais. Há pesquisas indicando que mais representatividade pode liderar a um maior cuidado e atenção, não apenas no desenvolvimento, mas também na auditoria contínua do algoritmo[50].

A citar como exemplo, se algum sistema de IA for desenvolvido por um grupo de desenvolvedores que contenha mulheres, a representatividade feminina desde a conceção ajuda numa maior diligência prévia em relação ao algoritmo. Não significa que um algoritmo desenvolvido também por mulheres não possa adotar uma decisão automatizada discriminatória, mas a pretensão é que uma supervisão feminina em relação às bases de dados usadas nos treinamentos e nos resultados do algoritmo seja mais equilibrada.

Por isso, a pluralidade científica deve ser tomada como prioridade no momento antecedente ao desenvolvimento de alguma tecnologia, porque a diversidade vai auxiliar em precaução acerca dos sistemas discriminatórios, ou se mesmo assim o uso específico da tecnologia gere efeitos discriminatórios relacionados a alguma minoria, este grupo vai estar representado dentre os especialistas que podem reparar tal dano.

Sob esta perspetiva, a IA como conceito tecnológico amplo é neutra, mas o seu uso em específico pode gerar efeitos jurídicos discriminatórios. Conforme foi mencionado, a prevenção dos efeitos discriminatórios não se resume a uma fase do ciclo de vida do algoritmo, uma vez que a prevenção deve ocorrer desde o momento da conceção até ao acompanhamento constante no momento de utilização do algoritmo. E sobre os efeitos dessa possível discriminação passa-se a discorrer.

---

[50] Noção desenvolvida por no estudo da PRETALAB acerca do urgente debate sobre representatividade no universo da inovação. Veja-se em PRETALAB. Um levantamento sobre a necessidade e a pertinência de incluir mais mulheres negras na inovação e na tecnologia. 2018. Disponível em: <https://www.pretalab.com/>. Acedido a: 02.02.2020.

5. A Inteligência Artificial e a possível Discriminação Algorítmica

A participação e a representatividade na ciência, ao longo do tempo, tem sido uma das causas para a formação de novos cientistas e especialistas mais plurais[51]. E na seara da IA, a necessidade parte do mesmo pressuposto de pluralidade, sobretudo para evitar que uma decisão seja ao mesmo tempo injusta e automatizada.

Segundo Barocas et al[52], qualquer sistema de tomada de decisão é capaz de errar. Sejam decisões baseadas em métodos convencionais com envolvimento humano significativo ou completo, mas também os mais sofisticados algoritmos de aprendizagem que podem assumir as diferentes formas de tomada de decisão. Sobre estas várias possibilidades, a discriminação algorítmica tem definição dificultada por não ser um termo de arte, mas um termo geral que pode se referir a um viés específico ou uma coleção de vários deles[53].

Uma definição sobre discriminação algorítmica que leva esta complexidade em consideração é a que se refere tecnicamente a entradas ou saídas de um sistema de IA, onde tais resultados apresentam um resultado errôneo ou injustificado sobre dois grupos. Deve haver, neste sentido, tratamento diferenciado ilícito proveniente de erros ou problemas no sistema de IA, ou pelos dados que são utilizados, ou pelos efeitos por si, ou por todas as opções anteriores[54].

Em outras palavras, um viés algorítmico pode existir e levar a um tratamento diferenciado, mas isto demanda maior detalhamento sob o ponto de vista da já explicada isonomia material para fins de definir o grau tendencioso do referido algoritmo. Não obstante, deve-se analisar no caso concreto se tal decisão algorítmica representa uma discriminação ilegal, onde o resultado além de não possuir uma justificação legal, passa

---

[51] Neste sentido Reis, Claudio Ricardo Martins dos. *Ciência e Valores: em defesa de um pluralismo sensível ao contexto*. Lumes, 2019.

[52] Barocas, Solon; Selbst, Andrew D, "Big Data's Disparate Impact", v. 104, *California Law Review*, 2016, p. 671.

[53] Lee, Nicol Turner; Resnick, Paul; Barton, Genie. *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*. Brookings, 2019.

[54] Neste sentido, veja-se em: Lattimore, Finn. O'Callaghan, Simon; Paleologos, Zoe, et al. *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias*. Australian Human Rights Commission, Technical Paper, 2020.

a infringir direitos humanos e garantias fundamentais. Por isso, a atenção ao problema da discriminação algorítmica desde a conceção de qualquer produto que utilize IA vai ser importante para mitigar os riscos de uma violação de direito.

Para mitigar riscos de discriminação é relevante considerar que já existe uma desigualdade natural nas relações sociais[55], naturalmente extrínseca aos modelos de IA. Acima desta desigualdade existe a discriminação, fruto de decisão automatizada que pode ser apenas um reflexo da desigualdade social existente que gera dados enviesados ou resulta do próprio sistema algorítmico que foi mal desenvolvido, sob a perspetiva técnica.

Todavia, nem toda a discriminação algorítmica deve ser resultado de um erro técnico, mas pode também ser fruto de um algoritmo que funciona da forma exata para a qual foi desenvolvido, mas que foi treinado com dados enviesados. Os resultados vão depender dos dados através dos quais o algoritmo foi treinado[56]. Seja problema intrínseco ao sistema, seja uma polarização em resposta a dados enviesados ou treinamento tendencioso da máquina, para fins de relevância jurídica, apenas os resultados que infringem direitos devem ser levados em consideração, de modo a limitar o presente estudo e qualquer medida de mitigação a ser adotada.

Uma das vertentes trazidas é a discriminação algorítmica proveniente dos dados[57]. Os sistemas de IA são treinados a partir de significativas bases de dados, contudo a diferença é que algumas irão conter dados pessoais – sobre pessoas naturais identificadas, outras sobre pessoas naturais identificáveis[58]. Outras bases de dados promovem a atenção ao

---

[55] Conforme Johansen: A desigualdade nas relações sociais advém de uma natural distribuição de grupos populacionais com perfis socioeconômicos distintos. Ver mais em Johansen, Igor Cavallini; Carmo, Roberto Luiz do; Alves, Luciana Correia. "Desigualdade social intraurbana: implicações sobre a epidemia de dengue em Campinas, SP, em 2014". *Cadernos Metrópole*, v. XVIII, n. 36, 2016, p. 421-440.

[56] Neste sentido, Cowgill, Bo; Tucker, Catherine. *Algorithmic bias: A counterfactual perspective*. NSF Trustworthy Algorithms, 2017.

[57] Conforme identificado através do *data mining* e ciência dos dados, cf. Hajian, Sara; Bonchi, Francesco; Castillo, Carlos. "Algorithmic bias: From discrimination discovery to fairness-aware data mining". *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, 2016. p. 2125-2126.

[58] O que para fins do RGPD tem o mesmo efeito de proteção, cf. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016

princípio da proteção de dados e para fins de treinamento de algoritmos utilizam dados sintéticos provenientes de uma simulação[59]. Com dados sintéticos, os desenvolvedores de algoritmos podem treinar os sistemas de decisão com dados mais plurais[60].

Além de respeitar a privacidade e evitar um tratamento excessivo de dados pessoais, os algoritmos de IA treinados com base em dados sintéticos são mais ajustáveis do que os treinados com dados reais[61]. Alterar a realidade representa demasiado esforço, quando a realidade reflete formas de discriminação, é por isso que criar uma realidade artificial, com diversidade sociocultural, pode ser uma forma mais eficaz de combater discriminação algorítmica. Em outros termos, a capacidade de controlar um enviesamento dos dados, é possível com um simulador de dados; e tal simulação deve considerar desde a conceção as possíveis formas de discriminação para evitá-las[62].

Portanto, o uso de dados sintéticos vem sendo aventado como uma possível solução que ao mesmo tempo confere atenção a três importantes institutos: (i) a proteção de dados pessoais e a possível coleta excessiva para treinamento de algoritmos de IA; (ii) criação de uma realidade artificial que se sobrepõe e não reflete a acima mencionada desigualdade endêmica nas relações sociais, naturalmente extrínseca aos modelos de IA; (iii) capacidade de controlar um enviesamento dos dados que possivelmente vai gerar uma discriminação com efeitos jurídicos sobre os indivíduos.

---

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[59] Dados sintéticos são dados para teste que oferecem maior possibilidade de uma grande formação rotulada, pelo facto de serem artificialmente gerados. Conforme Dahmen, dados sintéticos oferecem menos limitações, porque "os conjuntos de dados do mundo real (...) são limitados em termos de disponibilidade e variedade". Veja-se em Dahmen, Jessamyn; Cook, Diane. *SynSys: A synthetic data generation system for healthcare applications*. Sensors, v. XIX, n. 5, 2019, p. 1181. Tradução livre.

[60] Sem precisar filtrar no mundo analógico situações que não tragam riscos de discriminação.

[61] O maior grau de ajustamento é bem explicado em He, Haibo et al. "ADASYN: Adaptive synthetic sampling approach for imbalanced learning". *2008 IEEE international joint conference on neural networks*, IEEE, 2008, p. 1322-1328.

[62] Neste sentido, veja-se em: Lattimore, Finn; O'Callaghan, Simon; Paleologos, Zoe, *et al*. Ibid.

6. Casos de estudo sobre discriminação algorítmica

Conforme foi visto, o âmbito da IA é amplo, e é por isso que os casos concretos a serem utilizados neste estudo devem atingir os requisitos teóricos do conceito. Esta definição, recorda-se, limita a IA aos sistemas dotados da capacidade de aprender ou entender a partir da experiência[63]. Em conformidade com este processo de aprendizagem de máquina, parte-se para analisar casos em que o sistema aprende e decide, dentre algumas das áreas que compreendem a IA.

Uma das searas que mais levanta discussões sobre os impactos do tratamento de dados pessoais sensíveis para fins de treinamento de sistemas de IA com elevado poder de interferência social é a do reconhecimento facial. Em estudo recente, Joy Buolamwini do Massachusetts Institute of Technology (MIT)[64] descobriu que três modelos de reconhecimento facial sobre o gênero, nomeadamente o sistema das empresas IBM, Microsoft e da empresa chinesa Megvii, podiam identificar corretamente o gênero de uma pessoa a partir de uma fotografia com taxa de 99% (noventa e nove por cento) de acerto. Contudo, a taxa de acerto foi demonstrada ser apenas para o reconhecimento de homens de pele mais clara. O reconhecimento de mulheres com cor de pele mais escura caía para 35% (trinta e cinco por cento) de acerto[65].

Uma queda significativa na taxa de acerto por um algoritmo, no que diz respeito a cor da pele, não quer dizer que o sistema de IA opta por alcançar estes resultados, inexistindo intenção algorítmica em ser racista. O algoritmo é apenas uma tecnologia e pode ser treinado e aprender a tratar as pessoas de diferentes cores de pele de forma isonômica. O caminho para este tratamento não discriminatório está no treinamento que gera o aprendizado de máquina. Neste interim, devem as empresas desenvolvedoras de algoritmos de IA utilizar uma quantidade igual de

---

[63] Fetzer, James H. *Ibid*.

[64] Sobre este estudo, veja-se Buolamwini, Joy. *Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*. Master of Science, Massachusetts Institute of Technology, Cambridge, MA, 2017.

[65] Revell, Timothy. *Face-recognition software is perfect – if you're a white man*. Disponível em: <https://www.newscientist.com/article/2161028-face-recognition-software-is-perfect-if-youre-a-white-man/> Acedido a: 02.12.2020

imagens de mulheres com a cor da pele escura e de homens com a cor de pele clara, por exemplo. Fazendo isto, o resultado do sistema de IA provavelmente não indicará tamanha discrepância nos resultados[66].

Não apenas para possíveis erros de caracterização étnica, mas os resultados deste algoritmo de reconhecimento facial lecionam que é imperioso o treinamento equilibrado com uso de dados não enviesados. Seguindo a pesquisa do MIT, a IBM anunciou de imediato que havia retreinado o seu sistema num novo conjunto de dados[67]. Este posicionamento público da empresa deixa evidente a mensagem que os resultados discriminatórios, por parte do seu sistema de reconhecimento, não se deram por erros técnicos, mas pelo conjunto de dados utilizados no treinamento do sistema. A *mea culpa* da IBM evidencia que o sistema funciona da maneira esperada, sem falhas técnicas evidentes, mas que precisa ser retreinado, porque os dados de treinamento, provavelmente, possuíam muito mais casos de indivíduos do sexo masculino com cor de pele clara, em detrimento de indivíduos do sexo feminino com cor de pele escura.

Ainda sobre a pesquisa do MIT, Ruchir Puri, cientista chefe da IBM Research, acabou por aproximar-se da pesquisadora Buolamwini após o estudo que revelou uma discriminação algorítmica de cor de pele. Em resposta ao resultado discriminatório e a outros incidentes, a IBM revelou que passou a utilizar um novo banco de dados com 1 milhão de imagens para melhor analisar a diversidade dos rostos humanos. Os sistemas anteriores têm sido excessivamente dependentes do que, segundo Buolamwini, são repositórios de imagens "masculinas pálidas"[68].

A citada falha do algoritmo de reconhecimento facial, por si só, já constitui uma violação de direitos humanos por praticar discriminação sobre cor e gênero, violando o direito fundamental da não discriminação, conforme Artigo 21 da Carta Dos Direitos Fundamentais da União

---

[66] Conforme defendido por Pena, Alejandro et al. "Bias in multimodal AI: testbed for fair automatic recruitment." In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*. 2020.

[67] Revell, Timothy. Ibid.

[68] O'Brien, Matt. *MIT Researcher Exposing Bias in Facial Recognition Tech Triggers Amazon's Wrath*. Disponível em: https://www.insurancejournal.com/news/national/2019/04/08/523153.htm> Acedido a: 02.12.2020 (Tradução livre)

Europeia (CDFUE)[69]; e o princípio ético universal da igualdade, segundo a Declaração Universal dos Direitos Humanos. Entretanto, não é apenas a igualdade que pode ser afetada por uma decisão automatizada tomada com base em dados enviesados ou incompletos. O direito fundamental à própria vida, garantido pelo Artigo 2 CDFUE e pela ordem constitucional, também pode ser afetado pela discriminação algorítmica.

Diante deste cenário, é interessante mencionar um estudo que foi divulgado sobre o descrito tipo de discriminação, nomeadamente a respeito dos sistemas de IA que guiam carros autônomos. Limitando a apenas os casos em que não há qualquer envolvimento humano, existe um perigo inerente quando o sistema de IA com poderes de autonomamente conduzir o veículo, incorre em má classificação de um indivíduo.

Em um estudo da Computer Vision Systems[70] foi concluído que os carros autônomos testados ofereciam uma maior dificuldade de identificar pessoas com tom de pele mais escura. Se existir este grau de dificuldade, a utilização deste sistema pode ser uma ameaça aos direitos fundamentais envolvidos nesta situação. A inexistência de qualquer tratamento diferenciado proveniente da cor da pele deve ser um requisito obrigatório para o uso de mercado deste conjunto de algoritmos de IA para fins de conduzir carros autônomos.

Ou seja, uma falha tecnológica da gravidade do algoritmo de reconhecimento não identificar pessoas de tom de pele mais escura seria um problema que ultrapassa o âmbito tecnológico. A discriminação inerente ao sistema iria ser discriminatória e por em risco a vida e a liberdade de um grupo de indivíduos, violando assim Direitos Fundamentais da CDFUE e possíveis legislações dos Estados-Membros.

Em contraponto, a especialista em IA, Kate Crawford, em reportagem do jornal *Independent,* aponta que os resultados da referida pesquisa da Computer Vision Systems são contestáveis. Ela explica com o argumento que o estudo não usou as mesmas bases de dados utilizadas pelos

---

[69] União Europeia. Carta Dos Direitos Fundamentais Da União Europeia (CDFUE), 2016/C, 202/02 que retoma a Carta proclamada em 7 de dezembro de 2000 e substitui-a a partir da data de entrada em vigor do Tratado de Lisboa.

[70] Associated Press. *AI researchers slam Amazon for selling 'biased' facial recognition tech to cops*. Disponível em: <https://nypost.com/2019/04/04/ai-researchers-slam-amazon-for-selling-biased-facial-recognition-tech-to-cops/> Acedido a 02.12.2020

desenvolvedores de carros autônomos. E isto pode não refletir a real exatidão dos sistemas do "mundo real, já que em um mundo ideal, os académicos estariam testando os atuais modelos e bases de treinamento usadas pelos desenvolvedores de carros autônomos"[71].

Ao ver sob esta perspetiva prática, destaca-se o facto de os primeiros acidentes envolvendo carros autônomos não terem envolvido pessoas com a cor da pele negra. Pode-se listar os primeiros casos como: (i) o chinês Gao Yuning faleceu devido o *autopilot* do seu Tesla ter chocado com um veículo, em 2016; (ii) o americano caucasiano Joshua Brown que faleceu devido ao mesmo sistema *autopilot* da Tesla ter colidido com um trator, em 2016; e (iii), a morte da também caucasiana Elaine Herzberg que foi atingida por um veículo autônomo da Uber em 2018, após ter surgido de uma sombra para a estrada[72].

De toda a forma, por mais que nos três casos citados a cor da pele não tenha sido um ponto essencial ao acidente, a discriminação algorítmica por cor, nos moldes do estudo da Computer Vision Systems, merece atenção no desenvolvimento e posterior utilização de carros autônomos (ou qualquer outra decisão automatizada). Dito isto, se de um lado, no caso dos carros autônomos, a discriminação pode gerar um risco iminente à vida dos indivíduos, por outro lado, existem casos que a vida de terceiros não está em risco, mas que representam também discriminação algorítmica.

Traz-se como exemplo o resultado do estudo da Universidade de Washington, que delineou uma espécie de discriminação de gênero. Na pesquisa de imagens sobre o termo "CEO", o estudo obteve como resultado que o Google apenas mostrava 11% (onze porcento) das pessoas sendo mulheres, embora um levantamento tenha mostrado que 27% (vinte e sete porcento) dos chefes-executivos no mesmo âmbito territorial do estudo seria do sexo feminino[73].

---

[71] Tradução livre de "In an ideal world, academics would be testing the actual models and training sets used by autonomous car manufacturers". Ver mais em Cuthbertson, Anthony. *Self-driving cars more likely to drive into black people, study claims.* Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/self-driving-car-crash-racial-bias-black-people-study-a8810031.html> Acedido a 17.04.2021

[72] Gray, Stuart. List of driverless vehicle accidents. Disponível em: <https://www.itgs-news.com/list-of-driverless-vehicle-accidents/> Acedido a 17.04.2021

[73] Ver mais em Panch, Trishan; Mattie, Heather; Atun, Rifat. "Artificial intelligence and algorithmic bias: implications for health systems". *Journal of global health*, v. 9, n. 2, 2019.

Estudar os resultados dos motores de busca acaba por ser um exercício para averiguar possíveis discriminações. Resultados enviesados de uma busca podem não apenas causar discriminação, mas também manipular grupos de pessoas. Um dos que defendem esta premissa é o autor e ativista Epstein[74]. Os motores de busca possuem o poder de influenciar opiniões e até eleições, através de um fenómeno denominado "SEME" (efeito manipulador do motor de busca)[75].

Contudo, a discriminação não se limita apenas aos efeitos da IA utilizada pelos motores de busca. Conforme debatido ao longo deste texto, a IA apresenta um amplo âmbito e diversas aplicações. Sendo o motor de busca enviesado apenas exemplo de um tipo de IA que pode oferecer resultados discriminatórios, há outras áreas que podem oferecer o mesmo efeito jurídico de discriminação.

Partindo desta premissa, exemplifica-se que, ainda na esfera da discriminação de gênero, os algoritmos de IA têm sido capazes de definir o futuro profissional das mulheres. Estudos conduzidos pela Carnegie Mellon University em Pittsburgh, EUA, concluíram que o sistema de publicidade online do Google mostrava empregos de alta renda para os homens com muito mais frequência do que para as mulheres[76]. Não obstante os efeitos discriminatórios inerentes, esta discriminação algorítmica pode levar a repercussões contrárias à luta por um mercado de trabalho igualitário, devido ao poder e alcance do referido motor de busca.

Tal estudo da Carnegie Mellon University traz em seu título – *A tale of opacity, choice, and discrimination*[77] – três institutos basilares na perceção da discriminação algorítmica: opacidade, escolha e discriminação. O encarregado de auditar um algoritmo de IA busca romper a barreira da opacidade, a fim de perceber como ocorreu o processo de escolha,

---

[74] Epstein. Robert. *Manipulating minds: The power of search engines to influence votes and opinions. in* Moore *et al*, *Digital dominance: The power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

[75] Significado da sigla: "SEME – the Search Engine Manipulation Effect". Ver mais em Epstein, R.; Robertson, R. E. *The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections*. Proceedings of the National Academy of Sciences USA, 2015.

[76] Datta, Amit; Tschantz, Carl Michael; Datta, Anupam. "Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination". *Proceedings on privacy enhancing technologies*, n. 1, 2015, p. 92-112.

[77] Ibid.

a tomada de decisão automatizada. Em seguimento à análise, um dos resultados vai ser justamente a resposta se houve ou não discriminação. Conforme esta metodologia, o referido estudo analisou um conjunto de algoritmos publicitários do Google.

Pode-se dizer que os pesquisadores encontraram evidências de que os anunciantes conseguem direcionar seus respetivos anúncios com base no gênero, e ainda que o algoritmo de IA poderia tomar decisões automatizadas alheias às definições de gênero definidas pelos anunciantes. Datta *et al* apontaram que o Google poderia ter determinado que os homens são mais adequados para cargos executivos por conta própria[78]. Facto é que tal decisão, por conta própria, configura uma tomada de decisão automatizada com efeitos jurídicos relevantes, uma vez que ao mostrar anúncios de empregos bem remunerados apenas a homens, haverá discriminação algorítmica de gênero com efeitos possíveis de enfraquecer a participação das mulheres no mercado de trabalho.

Apesar desses resultados apontarem para uma decisão automatizada obrigatória, os próprios pesquisadores expressaram que não obtiveram todas as informações, porque as mesmas foram ocultadas pela falta de transparência do algoritmo[79]. Isso mostra que a análise de discriminação pode ser dificultada pela opacidade algorítmica, quando ela apresenta uma "*black box*" intransponível a ser considerada[80].

E esta opacidade acaba por ser um obstáculo para que a ciência obtenha uma análise das aplicações práticas da IA. Pelo acima exposto, a transparência algorítmica, aliada à clareza dos respetivos dados de treinamento e do processo de tomada da decisão automatizada, são institutos basilares no combate ao viés discriminatório que a IA pode adotar.

Conclusão

Ante o exposto, uma vez percebido que independentemente dos limites da máquina, o atual estado da arte é que existem diversos tipos de

---

[78] Datta, Amit; Tschantz, Carl Michael; Datta, Anupam. Ibid.

[79] Datta, Amit; Tschantz, Carl Michael; Datta, Anupam. Ibid.

[80] Castelvecchi, Davide. "Can we open the black box of AI?". *Nature News*, v. 538, n. 7623, 2016, p. 20.

inteligência não-humana. Ainda é cedo para afirmar se um dia as novas manifestações de inteligências alheias ao ser humano podem ultrapassar as diversas formas de inteligência humana, mas já se faz imperioso discutir mais a fundo os efeitos das inteligências já existentes.

A prevista *singularity*[81], em que a IA vai ser a própria responsável e definir seus fins e meios, ainda é utopia. O palpável no momento é identificar os efeitos jurídicos da IA existente, que já define relações sociais e interfere juridicamente na vida dos indivíduos. E uma destas formas de interferência é a discriminação algorítmica que, conforme foi visto, é fruto de uma decisão automatizada por parte de um sistema de inteligência artificial.

Muitas são as razões que podem levar um sistema, neutro por definição, a tomar uma decisão discriminatória, e uma das mais aparentes foi o treinamento dos sistemas de IA com dados enviesados. A problemática levantada foi que tais dados enviesados podem expor estatísticas que serão base de uma decisão discriminatória, com poderes de até manipular grupos de pessoas e os rumos de eleições democráticas, conforme o caso debatido sobre a IA que filtra o resultado dos motores de busca.

Ainda sobre dados, segundo Barocas, o *Big Data* diz-se neutro, mas não é[82]. Pelo facto desta diferenciação poder ocorrer de forma natural, é necessário o exame dos dados que estão sendo usados para treinar sistemas de IA. Não suficiente, um trabalho constante de melhoria na análise acerca de como o sistema de IA está interpretando os dados também deve ser tomado como prioridade pelas entidades desenvolvedoras. Ou seja, um cuidado sobre o algoritmo que deve acontecer em 3 momentos: preventivo (ainda no seu desenvolvimento), durante o tratamento dos dados e após a tomada da decisão automatizada.

Desta forma, a IA pode aprender e chegar a conclusões sozinhas, mas se esta decisão for discriminatória cabe a quem a supervisiona detetar tal resultado. Em outras palavras, a discriminação algorítmica é um problema a ser concebido pelo ser humano, ao mesmo tempo que requer uma solução também concebida pelo ser humano.

---

[81] Upchurch, Martin. "Robots and AI at work: the prospects for singularity". *New Technology, Work and Employment*, v. 33, n. 3, 2018, p. 205-218.

[82] Barocas, Solon and Selbst, Andrew D. "Big datas disparate impact". *California Law Review*, v. 104, 2016.

Neste sentido, não existe (ainda) um problema de cognição de IA, cujo problema aguardaria uma solução de sensibilidade da própria inteligência artificial. A IA é maleável e pode ser ensinada a não apenas evitar a discriminação, bem como identificá-la e auxiliar numa rápida reparação, tendo em vista os seus efeitos jurídicos de natureza fundamental. Mas para isso, quem analisa a possível discriminação e quem ensina o algoritmo deve analisar o sistema de tomada de decisão e os dados de treinamento de forma mais transparente. Menos opacidade e mais transparência apontam para o caminho de uma IA menos discriminatória.

O papel fundamental da Cibersegurança na Proteção de Dados Pessoais

Diogo Lopes Alves*

Resumo: Constitui o objeto do presente artigo realçar a importância da integração da Cibersegurança na Proteção de Dados Pessoais, tanto de uma perspetiva legislativa, que estabelece a Cibersegurança como imperativo da condição para a *accountability* do RGPD, como da autorregulação, estando ambas dependentes de um grau de maior exigência do que aquele que têm tido. Almeja-se com este texto promover a consciencialização das organizações e das pessoas para a segurança dos seus dados pessoais, de forma a criar uma maior sensibilidade por parte de cada um em relação à segurança dos dados pessoais de que são responsáveis ou de que são titulares. Há, por isso, um longo caminho a percorrer para além das políticas de privacidade e dos acordos de subcontratação das organizações.

Palavras-Chave: *Proteção de Dados Pessoais; Cibersegurança; Ciberataques; Medidas de Segurança; Reporte de Incidente.*

Abstract: The purpose of this article is to highlight the importance of integrating Cybersecurity in Personal Data Protection both from the legal standpoint that establishes Cybersecurity as imperative to the accountability of GDPR, as well as self-regulation, the standards of which are now more demanding than ever before. This article aims to promote greater awareness and sensibility regarding personal data security on the part of organizations and individuals that hold such information. There is a long a road ahead beyond privacy policies and subcontracting agreements.

Keywords: *Personal Data Protection; Cybersecurity; Cyberattacks; Security Measures; Incident Report.*

---

* Advogado, Licenciado em Direito e Mestre em Direito da Empresa e dos Negócios pela Universidade Católica Portuguesa. Exerce funções de Legal & Compliance no Centro de Engenharia e Desenvolvimento (CEIIA). Frequentou a 7ª edição do Curso Breve de Proteção de Dados Pessoais da NOVA School of Law em 2018.

Introdução

A Proteção de Dados Pessoais e a Cibersegurança são dois conceitos indissociáveis na era digital, onde existe um ciberespaço sem demarcações nítidas e com uma débil regulação que traz desafios constantes para os nossos dados pessoais face ao rápido desenvolvimento da tecnologia, às novas ameaças diárias, ao esbatimento das barreiras físicas e à conectividade permanente que amplia a superfície de vulnerabilidade. A frágil, ou inexistente, noção da simbiose entre a Proteção de Dados Pessoais e a Cibersegurança por quem faz o seu tratamento, pode ter origem em vários elementos como, por exemplo: a desconsideração pela privacidade e a falta de formação nessas áreas, combinados com o facto de as pessoas serem o elo mais fraco da cadeia, pelo desconhecimento das tecnologias e dos procedimentos de segurança, pelo excesso de trabalho, pelas funções desajustadas e por atos maliciosos, intrínsecos à natureza humana. Dessa forma, para garantir a proteção dos dados pessoais, é necessário saber quais os perigos que existem no ciberespaço, na maior parte das vezes, desconhecidos de cada um de nós, e reconhecer as fragilidades técnicas e humanas existentes, sendo certo que só através do equilíbrio entre estes dois vetores será possível assegurar a proteção de dados pessoais de uma forma segura e condizente com a realidade atual.

Pese embora a ubiquidade do digital *(Internet of Things, Big Data, Cloud Computing, 5G*, etc.) representar uma vantagem para o desenvolvimento da sociedade, constitui, de igual forma, um fator de risco para os titulares dos dados pessoais que têm perdido o controlo sobre os mesmos, potenciando a redução da sua privacidade. Essa falta de controlo sobre os dados provém, não só, de quem os trata, mas também da condescendência com que são disponibilizados, muito graças à insipiência do seu ciclo de vida e do nível de sensibilidade nesta matéria por parte dos titulares dos dados, que contribui gradualmente para o aumento do risco, trazendo consequências inexoravelmente prejudiciais para a proteção dos dados pessoais. Na realidade, a gratuitidade do digital faz com que, frequentemente, cedamos, facilmente, os nossos dados, tendo apenas como contrapartida o acesso a um serviço. Tratar os dados como contraprestação, ajuda esta monetização dos dados, a hipótese do pagamento de um preço em troca de dados pessoais confere-lhes uma natureza de mercadoria, devendo

ser um caminho a evitar, visto poder não ter retorno. Acresce outro fator de risco que ocorre em contexto laboral decorrente do facto de a fronteira entre a vida profissional e privada ser cada vez mais ténue, seja pelo recurso ao teletrabalho, seja pela informação pessoal e profissional se encontrar num só dispositivo seja, finalmente, pelo uso de dispositivos pessoais no local de trabalho, tudo constituindo fatores potenciadores de riscos de Cibersegurança para os dados pessoais e que os tornam vulneráveis.

O Regulamento Geral de Proteção de Dados (RGPD) teve o condão de ter contribuído para a existência de uma ética no tratamento de dados pessoais através da redistribuição de responsabilidade entre as partes que os tratam com o intuito de assegurar que o titular dos dados tenha o controlo total e o poder de decisão sobre os mesmos.

A privacidade e a proteção de dados pessoais deixaram de ser conceitos etéreos e a violação das mesmas começaram a ter implicações financeiras[1] por não serem respeitadas. Porém, não nos podemos ater a essa premissa simplista pois uma organização pode sofrer consequências bem mais gravosas, quando é alvo de um Ciberataque, nomeadamente, ao nível reputacional, e traduzir-se em implicações diretas nos titulares dos dados pessoais. No seio de uma organização que lide com dados pessoais, a forma como a informação é tratada através de medidas de segurança e do reporte de incidentes vai ditar a sua "*accountability*"[2], não devendo, consequentemente, ser descurada a sensibilização de cada colaborador para esta temática, constituindo-se como elemento chave em cada organização que faça o respetivo tratamento, conferindo-lhe valor essencial e diferenciador no mercado. A constante mutação do tipo de ameaças requer, por outro lado, que a segurança tenha de ser cuidada, todos os dias, para evitar que os dados pessoais fiquem em risco, dependendo tal operação da organização interna da Cibersegurança, de boas bases de gestão de risco e da integração do princípio da Segurança e Privacidade desde a conceção e por defeito.

---

[1] Art.83.º do RGPD, Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

[2] N. º2 do art. 5.º, art. 24.º e considerando 89 do RGPD.

As medidas existentes, em termos de segurança e privacidade, apresentam-se, nos dias que correm, como insuficientes e a necessitar de outra abordagem de modo a criar uma sociedade digital consciente dos riscos relativamente à qual não poderá ser colocado de parte nenhum dos intervenientes já que uma sociedade só funciona, na sua plenitude, se existirem garantias de respeito dos direitos e liberdades fundamentais, não sendo a sociedade digital diferente, nem devendo ser tratada como tal, nem estar sujeita ao livre arbítrio de cada um.

Com o aumento dos Ciberataques, a proteção dos dados pessoais está, mais do que nunca, dependente da Cibersegurança, pelo que tentar proteger aqueles sem o recurso a esta última torna-se um desígnio ilusório e que dependerá, não apenas de alterações legislativas, mas sobretudo da melhoria das medidas de segurança que venham a ser implementadas e da forma como são executadas.

1. Proteção de Dados Pessoais

O RGPD constituiu um importante passo no aumento da consciência dos cidadãos da União Europeia sobre privacidade[3], muito graças às coimas[4] elevadas que estão previstas no referido diploma. Porém, o RGPD ultrapassa esse ditame pecuniário dado que a proteção da privacidade e a proteção dos dados pessoais são pilares fundamentais de uma sociedade evoluída e informada do valor dos seus dados, estando a mesma dependente do respeito destes direitos, consagrados universalmente[5] e que representam um valor incomensuravelmente maior que qualquer

---

[3] ENISA, "Good practices in innovation under ncss" – Good practices in innovation on cybersecurity under the national cyber security strategies, novembro 2019, p.8, disponível em: <https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1>, acedido a 23/03/2020.

[4] Desde maio de 2018 até março de 2020 as autoridades de controlo impuseram 231 coimas e sanções. CMS, GDPR, disponível em: <https://www.enforcementtracker.com/?insights>, acedido a 12/02/2020.

[5] N.º 2 do art. 1.º e considerando 4 do RGPD, art. 26.º e 35.º da Constituição da República Portuguesa, art.º 8.º da Convenção Europeia dos Direitos do Homem, art. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, art. 16.º do Tratado de Funcionamento da União Europeia, art. 12.º da Declaração Universal dos Direitos Humanos.

coima. O referido diploma procura assegurar a total e efetiva aplicação desses direitos[6], considerando que os dados não podem ser tratados a qualquer custo, devendo ser geridos de forma diferente dos dados corporativos, isto é, com um grau maior de sensibilidade. Caso flagrante da sua diminuta efetividade é o das políticas de privacidade, extremamente técnicas e ininteligíveis para a população em geral, sendo este, aliás, um dos fatores de falta de transparência de quem trata os dados e que vem favorecer o alheamento em relação ao controlo dos dados pessoais, criando uma exposição perigosa a possíveis "agendas escondidas" das organizações.

Se os dados pessoais são o novo petróleo, a sua proteção é o controlo da poluição. Quem os trata deve ter especial cuidado, não só pelo valor comercial que possam ter, mas sobretudo atendendo aos direitos fundamentais envolvidos, jamais podendo ser causa justificativa da violação desses dados, tanto a liberdade existente no ciberespaço, como o facto de a tecnologia avançar a uma velocidade difícil de acompanhar por qualquer ordem normativa. É nessa medida que a Cibersegurança pode ter um papel decisivo na proteção dos dados pessoais.

O RGPD veio revolucionar a cultura de negócio à volta dos dados, apresentando-se como uma oportunidade, não só forçando os intervenientes a respeitar as mesmas regras com os mesmos princípios, como permitindo criar produtos e serviços mais éticos, convertendo a proteção de dados pessoais num caminho que maximiza a criatividade e a inovação, exigindo que as organizações tenham uma abordagem mais abrangente em relação à proteção dos dados pessoais para assegurar o cumprimento do RGPD desde o início de cada processo. Existe, dessa maneira, a necessidade de salvaguardar a privacidade e os dados pessoais, na medida em que uma violação destes direitos, nos termos do considerando n.º 85 do RGPD, "...pode causar danos físicos, materiais ou imateriais às pessoas singulares como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos...".

---

[6] Training Data Protection Authorities and Data Protection Officers – T4DATA, *The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation*, julho de 2019, p. 21-26, disponível em: <https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf.>, acedido a: 16/04/2020.

Depreende-se do acima explicitado que estando os dados pessoais maioritariamente no ciberespaço e representando os Ciberataques uma inevitabilidade para o aumento do risco para os direitos e liberdades, torna-se primordial a realização de avaliações de impacto sobre a proteção de dados[7], cumprindo dessa forma o que vem preceituado no n. º1 do art. 32.º do RGPD. Outro contributo que o RGPD confere para elevar o nível de Cibersegurança no mercado único digital, será a certificação[8] que permitirá que os titulares dos dados avaliem rapidamente o nível de proteção de dados proporcionado pelos produtos, serviços e processos em causa[9], bem como também os códigos de conduta[10] que poderão consubstanciar um papel de garante do tratamento correto pelo responsável pelo tratamento e subcontratante[11]. Tanto os códigos de conduta como os procedimentos de certificação são fatores demonstrativos do cumprimento das obrigações, de acordo com o que dispõe o n.º 3 do art. 32.º do RGPD, ainda que nenhum destes mecanismos exclua, de forma automática, a responsabilidade, em caso de incumprimento.

A própria definição de violação de dados pessoais no RGPD refere que se trata de uma violação da segurança[12], donde se infere que a Cibersegurança é um imperativo normativo que demonstra a proximidade entre a proteção de dados pessoais e a segurança, realçando a importância de uma abordagem coordenada entre as duas para identificar e gerir os riscos, consequentemente, aumentando a eficácia e reduzindo os esforços[13].

É, ainda, de salientar a crescente preocupação dos titulares dos dados com a violação dos seus dados pessoais (55%), mais do que, por exemplo, em perder a carteira (23%) de acordo com um estudo relacionado com

---

[7] Alínea d) do n. º7 do art. 35.º do RGPD.

[8] Art.42.º do RGPD.

[9] Art.42.º e considerando 15 do RGPD, considerando 74 do Regulamento EU 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019.

[10] Art.40.º do RGPD.

[11] N. º3 do art. 24.º do RGPD.

[12] Art.4.º ponto 12) do RGPD.

[13] NIST Special Publication 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy*, dezembro 2018, p.163, disponível em: https://doi.org/10.6028/NIST.SP.800-37r2, acedido a 8/4/2020.

proteção de dados pessoais e Cibersegurança[14]. Por outro lado, 52% das pessoas não se sentem bem informadas sobre Cibersegurança de acordo com o Relatório Cibersegurança em Portugal de 2019[15], o que reflete uma assincronia entre a proteção de dados e a Cibersegurança, que deve ser urgentemente corrigida.

Ainda que seja utópica a ideia de um cumprimento integral do RGPD[16], não existirá uma efetiva proteção de dados pessoais no mundo digital sem Cibersegurança, sendo dois vetores que terão de estar sempre ligados, que vão para além do que esteja preceituado em qualquer diploma legal.

2. Cibersegurança

A Cibersegurança pode ser definida como qualquer medida implementada para proteção e segurança da informação que estiver no ciberespaço, como das infraestruturas onde residem, de possível disrupção e ataque[17]. Estando os nossos dados pessoais maioritariamente em modo digital e no ciberespaço, o RGPD constituiu um passo essencial ao nível da Cibersegurança, ao criar regras para o tratamento dos dados pessoais, do ponto de vista da segurança. Desse modo, a Cibersegurança deverá ser parte integrante da execução do RGPD por parte das organizações[18], a

---

[14] Radware's 2018 C-Suite Perspectives: *Trends in the Cyberattack Landscape, Security Threats and Business Impacts*, disponível em: <https://www.radware.com/LegalNotice/.consumer sentiments: cybersecurity, personal data and the impact on customer loyalty>, acedido a 13/05/2020.

[15] Observatório de Cibersegurança, Centro Nacional de Cibersegurança "*Relatório Cibersegurança em Portugal de 2019*", dezembro de 2019.p.7, disponível em: https://www.cncs.gov.pt/content/files/relatrio_sociedade_2019_-_observatrio_de_cibersegurana_cncs.pdf, acedido a 24/04/2020.

[16] O USBank assume na sua política privacidade que qualquer armazenamento e transmissão de dados não pode ser garantida a 100%, disponível em: https://www.usbank.com/about-us-bank/privacy/security.html, acedido a 2/07/2020.

[17] White Paper, Advisera, *Privacy, Cybersecurity and ISO 27001-How are they related?*, 2016.p.7, disponível em: <https://info.advisera.com/27001academy/free-download/privacy-cyber--security-and-iso-27001>, acedido a 18/04/2020.

[18] Considerandos 6 e 7 do RGPD.

evolução tecnológica assim o exige e só dessa forma se poderá estabelecer um quadro sólido de proteção de dados pessoais. O RGPD ao exigir um determinado patamar de medidas técnicas e organizativas que garantam a segurança de dados e o exercício dos vários direitos ali previstos (portabilidade, apagamento, acesso, etc.), sem os quais não é possível assegurar um grau adequado de privacidade, veio realçar a relevância da Cibersegurança, contribuindo para a maturidade digital de segurança das organizações. Por sua vez, o aumento do número de pessoas a utilizar o ciberespaço e do número de fontes de armazenamento de dados (muitos deles pessoais) resulta no aumento dos desafios da Cibersegurança dos dados pessoais.

Tendo em apreço o referido e de a conectividade ser o nosso oxigénio atualmente[19], sem o qual não podemos viver, potenciam-se, de igual forma, os Ciber riscos que podem afetar direitos fundamentais da forma mais simples, como seja um mero clique num *e-mail* de *phishing*.

A violação de dados pessoais é um risco real e um dos custos imediatos de um Ciberataque, devendo a proteção de dados pessoais ser sempre desenvolvida de forma centrada no respeito dos direitos humanos e das liberdades fundamentais, tendo por base os interesses dos cidadãos e organizações em conformidade com os direitos em matéria de privacidade e de proteção de dados. Ainda que a segurança dos dados pessoais não seja, suficientemente, relevante para as organizações, o risco da continuidade do negócio e a reputação poderão ser fatores determinantes para fomentar uma atitude diferente em relação àqueles[20].

Pelo bem dos dados pessoais, a solução poderá passar por integrar as políticas de Cibersegurança nos processos de negócio de uma organização.

---

[19] O número de aparelhos de IoT instalados espera-se que exceda os 21 biliões em 2025 no mundo inteiro-Statista 2019, disponível em: <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>, acedido a 05/05/2020.

[20] De acordo com inquérito sobre a perceção de ciber risco realizada a 1.300 executivos pela Marsh e pela Microsoft no qual se constatou que o cenário com maior potencial de impacto em termos de perdas está associado à "interrupção do negócio" (75%), seguido do risco de "danos reputacionais" (59%) e da "violação da informação dos clientes"(55%), revelador do grau de prioridade de cada um, disponível em:

<https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>, acedido a 16/05/2020.

Situação evidente da prioridade do negócio em detrimento da segurança é o da migração de dados para a *cloud* realizado pelas organizações, nomeadamente, para *clouds* públicas, aumentando o risco, decisão suportada unicamente no custo e funcionalidade (disponibilidade de acesso) e raramente na segurança. Adstrita a esta opção, as organizações negligenciam o facto de virem a ser responsabilizadas em caso de violação de dados pessoais e não o Encarregado de Proteção de Dados (EPD) ou o departamento de informática, o que deve conduzir à reflexão da questão da Cibersegurança como prioridade na sua estratégia (operacional e financeira, para além da legal).

As falhas na garantia de segurança poderão tornar-se, por essa razão, o melhor incentivo para que se invista na segurança, pois as perdas financeiras e os danos reputacionais poderão ser consideráveis, pense-se num Ciber incidente[21] que faça capa de jornais e no potencial do impacto catastrófico na balança comercial de uma organização, tendo em conta que o dano infligido aos dados pessoais será superior a qualquer coima[22]. Aliás, esta é a principal razão pela qual as organizações evitam comunicar incidentes o que, por sua vez, dificulta que outras tenham noção das potenciais perdas no caso de sofrerem um incidente, constituindo um desequilíbrio de informação entre as organizações, fruto do desconhecimento das consequências reais de um Ciberataque.

Naturalmente, os requisitos de segurança e os respetivos custos são proporcionais à sensibilidade da informação porém, a falta de responsabilização, muitas vezes por não se saber quem foi o autor de um ataque ou sequer se foram atacados, a dificuldade em obter o direito de

---

[21] Um incidente de Cibersegurança traduz-se em qualquer ação não autorizada ou ilegal que envolva computadores (sistemas ou aplicações) ou redes, representando quebras nas medidas de Cibersegurança e as medidas de resposta envolvem o bloqueio do ataque e a reposição do normal funcionamento, bem como a identificação das causas do incidente de forma a prevenir futuros ataques, fraudes e extorsões, disponível em: <https://www.gee.gov.pt/pt/documentos/estudos-e-seminarios/temas-economicos/7237-te54-a-economia-da-ciberseguranca/file>, acedido a 2/6/2020.

[22] O *data breach* da empresa Talk Talk em 2015 causou enormes danos reputacionais, não só expôs dados pessoais de mais de 150 mil clientes, mas viu a sua receita reduzida em mais de 20 milhões de dólares e perder mais de 100 mil clientes. Passado um ano do ataque o valor de mercado desceu e passado quatro anos continua abaixo do valor de 2015, disponível em: <https://www.ft.com/paidpost/aon/cyber-risk-counting-the-cost.html>, acedido a 7/05/2020.

regresso sobre os danos que sejam causados, a sensação de impunidade, o anonimato e ausência de fronteiras, desconsidera os custos dos incidentes de segurança, tornando difícil de justificar possíveis alocações em segurança preventiva. Com a agravante de o custo de um incidente poder não ser mensurado financeiramente quando ocorre, uma vez que o incidente pode demorar anos a ser resolvido – algumas organizações podem nunca recuperar – e o titular dos dados pessoais poder perder, de forma irreversível, a confiança na mesma, com os prejuízos imediatos que isso pode comportar.

Ao contrário do que se possa julgar não é um investimento sem retorno, a poupança será maior que o investimento, pois a Cibersegurança permitirá diminuir os custos relacionados com os incidentes que podem salvaguardar a continuidade do negócio.

Entende-se que a implementação de medidas simples de Cibersegurança (como o uso extensivo de cifragem) será uma solução associada a redução de custos de incidente, além de ser um facilitador de oportunidade de negócio e não um fator impeditivo daquele e conferir um selo de qualidade na forma segura como são tratados os dados pessoais. A preocupação das organizações com a segurança será tanto maior quanto mais tiverem a perder com essas falhas, contudo, a grande questão é saber se existe estímulo suficiente para que invistam em Cibersegurança, isto é, se têm perceção das potenciais perdas financeiras que poderão resultar de Ciberataques.

O facto de grande parte das organizações ainda optar pela internalização desta função, por não a considerarem uma área prioritária, poderá ser explicado pelo facto de o tecido empresarial ser constituído na sua grande maioria por PME´s, com menor capacidade financeira para fazer face às necessidades de uma política de Cibersegurança eficaz. Não obstante isso, o facto de o tecido empresarial português ter essas caraterísticas não pode ser justificação para a escassa consciência da importância da Cibersegurança, visto este tipo de organizações pequenas poderem ser encaradas pelos atacantes como alvos fáceis tornando-as um foco de risco, para além de, em caso de transferência de dados pessoais para um operador de infraestruturas críticas, ser um risco ainda mais acrescido.

Convirá realçar que nenhuma organização é demasiado pequena para ser atacada, logo, a maneira mais fácil de motivar uma organização a adotar

serviços de segurança é depois de ela sofrer um ataque, devendo-se essa mentalidade ao conhecimento – muitas vezes inexistente – que as organizações têm sobre estes temas, por não estarem cientes da necessidade que existe em proteger a sua infraestrutura, as suas operações e o seu próprio negócio.

A realidade é que, e a menos que seja estritamente necessário por questões legais (e aqui, pode ser determinante o RGPD e a sua execução), os ataques não são comunicados. Esta perceção de um aparente conforto leva as organizações a negligenciar a segurança da sua informação.

Acresce a este cenário, ainda, a confiança "cega" na tecnologia que podem possuir que, diga-se, por muito melhor que seja, não transfere um grande valor para a organização se não for implementada, gerida e monitorizada de forma adequada, já que por vezes a falta de recursos não é na tecnologia, a qual já pode existir dentro da organização, mas na inexistência de procedimentos para as utilizar, por exemplo, a existência de uma *firewall* não é suficiente se não tiverem um controlo de acesso à informação.

Em resultado da existência de uma utilização massiva das tecnologias de informação por parte das organizações, estas não podem querer mudar digitalmente e não serem responsáveis pela Cibersegurança. No caso da segurança dos dados pessoais, dificilmente a segurança é demonstrável, mas facilmente se identificam as quebras de segurança, ficando a Cibersegurança dos nossos dados a depender do rigor colocado na *accountability* do RGPD por parte das autoridades de controlo, isto é, na capacidade de se poder comprovar o cumprimento por parte dos responsáveis pelo tratamento, que poderá ser insuficiente face à realidade atual e que não garante, por si só, o que se pretende proteger, dados pessoais. O facto de a Cibersegurança afetar toda a organização deverá ser condição suficiente para o Ciber risco ser integrado nos riscos da mesma, o qual pode ter origem, não só, num determinado ativo, mas numa vulnerabilidade no sistema daquela. É, por consequência, necessário ter uma visão ampla da Cibersegurança, dado que esta se relaciona com vários setores e tem implicações em serviços essenciais, administração pública, empresas, indivíduos, convocando várias áreas: tecnologias de informação, comunicação, segurança, direito, economia, sociologia ou relações internacionais, o que não lhe confere um caráter isolacionista de vertente técnica ou criminal.

A Cibersegurança é um processo contínuo, na linha do cumprimento do RGPD, seja através da atualização das políticas (evidencia-se que não é por ter muita documentação que as pessoas cumprem o que está preceituado) seja da monitorização do sistema de gestão da informação, é, em síntese, um trabalho que nunca acaba; convém é, em alguns casos, iniciá-lo.

Estamos, evidentemente, perante uma grande mudança de práticas estabelecidas que vão sendo alteradas de uma forma suave, em todas as organizações, devendo ser encontrados pontos de entendimento que resultem em que os intervenientes (colaboradores, subcontratados e titulares de dados pessoais) vejam vantagens em a adotar. Compromisso que só resultará se for estabelecida como um integrador em cada departamento da organização e, para isso, tem de fazer parte da estratégia da mesma e não ser um elemento facultativo. Um caso paradigmático é o envio dos dados encriptados por *e-mail* conferir a proteção face a terceiros para que estes não tenham acesso aos dados em apreço, ainda que possa ser um processo moroso a implementar numa fase inicial. Na prática, todos os dias, tomamos decisões de segurança tão simples como trancar a porta de casa, ainda que não saibamos como funciona o mecanismo da fechadura, trata-se de um ato natural e, desse mesmo modo, deverá ser entendida a Cibersegurança, posto que se esta não tiver a adesão das pessoas e continuar a ser um elemento estranho significa que não alcançou a efetividade necessária e os dados pessoais continuam em risco. Entendida a premência da existência de um ambiente seguro para estabelecer e desenvolver qualquer atividade económica ou social, a segurança deve existir para libertar os cidadãos e as organizações de preocupações, de modo a que se possam focar nas suas atividades[23].

Da parte do titular dos dados, também existe pouco estímulo para exigir a Cibersegurança dos seus dados pessoais porque, a maior parte das vezes, não tem perceção do alcance do risco, já que grande parte dos utilizadores do ciberespaço não são capazes de distinguir quais são os dispositivos/sistemas que são seguros ou não, levando a essa falta de exigência. Ao não existir essa perceção por parte dos utilizadores

[23] Centro Nacional de Cibersegurança *Quadro Nacional de Referência para a Cibersegurança*, p.10, 2019.

também não haverá estímulo para que as organizações promovam a Cibersegurança.

A preocupação com a Cibersegurança de cada um, seja em atividades laborais ou na esfera pessoal, pode ter resultados vantajosos, quando tratamos os dados pessoais de terceiros, podendo esta consciencialização ser um ponto de inflexão na questão da mesma.

O RGPD não especifica medidas de Cibersegurança concretas, mas que sejam tomadas as medidas adequadas[24], ainda que não exista um modelo ideal e do ónus de cada organização ter as suas idiossincrasias, o compromisso da direção, a existência de políticas, definição dos responsáveis, evolução da performance, monitorização e auditoria interna tornam-se fatores diferenciadores de um programa de Cibersegurança robusto que vai para além do cumprimento de qualquer diploma. Necessitando, para alcançar o sucesso, não apenas da componente técnica mas também da identificação do contexto onde é utilizado, da proteção dos sistemas e dos ativos, da deteção de desvios, das respostas prévias aos incidentes e do estabelecimento de operações de continuidade de negócio[25], mas sobretudo depende de uma boa relação das pessoas com a Cibersegurança, do reconhecimento que as pessoas representam a parte mais frágil nas cadeias de Cibersegurança e de criar condições para torná-las *firewalls* humanas robustas contra os Ciberataques[26]. A criação de uma cultura de Cibersegurança constitui-se, dessa forma, como essencial para solucionar os problemas que possam surgir, de uma forma adequada[27] e que não se cinja a uma *accountability* não representativa da realidade, em face duma exigência diminuta por parte da autoridade de controlo, com os efeitos

---

[24] National Cyber Security Center "Cyber Security Toolkit for Boards", p. 18, abril 2019, disponível em: https://www.ncsc.gov.uk/collection/board-toolkit, acedido a 27/05/2020.

[25] NIST, "Cybersecurity approach to cybersecurity Framework (CSF)", white paper series, issue 5, p.8 2019.

[26] ENISA, "Cyber Security Culture in organisations", *European Union Agency For Network and Information Security*, novembro 2017, p.29, disponível em: <https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations>, acedido a 1/7/2020.

[27] Centro de Ciberseguridad Industrial "CCI, roadmap de la ciberseguridad industrial en españa, 2019-2020", 2019, p.10, disponível em: <https://www.cci-es.org/detalle-actividad/-/journal_content/56/10694/974082>, acedido a 16/03/2020.

irreversíveis para a organização e para os titulares dos dados pessoais que daí podem resultar[28-29-30].

Abreviadamente, as organizações devem assumir que nunca estão seguras e não podem confiar que o cumprimento da lei as exime de qualquer responsabilidade, tendo de ter, também, em linha de conta que os processos legislativos tendem a ser mais lentos que a evolução tecnológica (desenvolvimento de *malware* que está constantemente a criar novas ameaças, p.ex.).

A dúvida sobre os Ciberataques não é em saber se vão existir, mas em saber, quando vão acontecer.

3. Ciberataques

Muitas são as organizações que têm fragilidades na segurança e se deparam com Ciberataques aos dados pessoais que possuem, cada vez com mais frequência[31]. Esta é uma situação que normalmente não é bem

---

[28] Como prova de que a Cibersegurança e a Proteção de Dados Pessoais andam de mãos dadas, temos o caso do ciberataque à EasyJet, onde foram revelados dados de *e-mail* e dados de viagens de aproximadamente 9 milhões de clientes, assim como mais de 2000 clientes viram os dados dos seus cartões de crédito expostos, tendo sido acedidos por uma parte não autorizada. A autoridade de controlo do Reino Unido lançou uma investigação e o Centro Nacional de Cibersegurança está a trabalhar com a Easyjet para perceber como o ataque afetou os cidadãos do Reino Unido, disponível em: <https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card>, acedido a 8/8/2020.

[29] Em 16 de outubro a British Airways foi multada pela autoridade de controlo (ICO) pela falta de proteção de dados dos seus clientes, o ciberataque permitiu aceder a dados pessoais de mais de 400.000 clientes da companhia, o que revelou não existirem medidas de segurança adequadas, disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers>, acedido a 19/10/2020.

[30] A autoridade de controlo do Reino Unido impôs uma sanção de 20.7 milhões de euros à Marriott por não assegurar medidas de segurança apropriadas no processamento de dados pessoais dos seus clientes, violação que teve origem num ciberataque que comprometeu o sistema de IT, disponível em: <https://gdprhub.eu/index.php?title=ICO_-_Monetary_Penalty_on_Marriott_International_Inc.&mtc=today>, acedido a 17/11/2020.

[31] A Uber referiu que duas pessoas que não trabalhavam para a empresa acederam a dados através de um serviço de *cloud* que a empresa utiliza, disponível em: https://us.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html, acedido a 23/08/2020.

acolhida externamente, quer por colocar em evidência as insuficiências, quer por revelar uma segurança deficitária que resulta num impacto negativo na sua credibilidade. Convém dar nota que a exposição aos riscos é uma condição intrínseca de estarmos no ciberespaço permanentemente e os Ciberataques abrangerem todo o tipo de organizações, independentemente da dimensão. Estando o ciberespaço ainda a caminho da sua maturidade civilizacional, marcada pela assimetria entre os conhecimentos necessários para cometer um cibercrime e as competências necessárias para se defender dele com as consequentes ausências de regras que daí decorrem, tornam a Cibersegurança uma prioridade para as organizações que têm como foco a proteção dos dados pessoais.

No que concerne aos Ciberataques, propriamente ditos, estes podem ter vários tipos de objetivos como o roubo de dados pessoais, o uso abusivo dos mesmos, roubo de identidade, divulgação indesejada/ não autorizada de informação, destruição de reputação, etc., sendo os meios para aceder a estes variados: engenharia social, *phishing, ransomware, malware*, redes sociais, *cloud computing, DDO's* (ataques de negação de serviços), etc.[32] Ao contrário do que se possa pensar, a maioria dos ataques são baseados em técnicas já conhecidas e não somente em técnicas sofisticadas, começando,

---

Em abril mais de metade de um bilião de ficheiros de usuários do Facebook foram expostos por uma terceira parte não protegida de um serviço de *cloud*. A informação financeira de mais de 80 milhões de americanos foi exposta através de um ataque a um serviço de *cloud*, disponível em: https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report/Capital One- personal information of more than 100 million individuals, including Social Security numbers and bank accounts, was compromised in a massive data theft <https://eu.usatoday.com/story/money/2019/07/29/capital-one-data-breach-2019-millions-affected-new-breach/1863259001/>, acedido a 3/9/2020.

A Equifax anunciou que dados de mais de 147 milhões de pessoas foram expostos através de uma violação de dados, disponível em: <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>, acedido a 9/9/2020.

A companhia área Cathay Pacific Airways Limited foi multada em £500,000 por falhas de segurança aos dados dos seus clientes, entre outubro de 2014 e maio de 2018 não existiam medidas adequadas de segurança que levaram a que os dados ficassem expostos, disponível em: https://ico.org.uk/action-weve-taken/enforcement/cathay-pacific/, acedido a 17/9/2020.

[32] Os *hackers* maliciosos precisam de começar seja através de servidores vulneráveis, *e-mails* de *phishing* ou de credenciais furtadas. Verizon, "2019 Data Breach Investigations Report", p.66-67, disponível em: <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>, acedido a 9/7/2020.

por vezes, com técnicas muito simples, sendo o *e-mail* a forma mais comum para um ataque[33].

Não fossem já suficientes os meios existentes, todos os dias há novos tipos de *malware*, o que torna premente uma adequada Cibersegurança que vise proteger a privacidade e os dados pessoais[34]. Em 2021, espera-se que eventos de Ciberataques tenham custos de 6 triliões de dólares[35], ainda que o custo total não seja compreendido no impacto que provoca o incidente. Os Ciberataques tornaram-se um perigo comum para os indivíduos e para os negócios, de acordo com o relatório global de riscos do WEF, que se refere àqueles como um dos maiores riscos para realizar negócios globalmente, nos próximos 10 anos[36].

Se por um lado, os Ciberataques se tornam mais intensos, complexos e sofisticados, por outro, existe uma maior partilha de informação, mais massa crítica e novos processos tecnológicos e organizacionais que ajudam a reduzir o fosso existente entre os intervenientes.

No entanto, nenhuma organização vai estar verdadeiramente preparada para um Ciberataque, o que torna a preparação para o rescaldo de um incidente um fator distintivo nos resultados a longo prazo. Deve-se, de igual forma, estar preocupado não só com a prevenção, mas, em especial, com a "cura" da violação dos dados pessoais.

Por sua vez, a implementação do RGPD, ao ter obrigado as organizações a rever os seus processos, políticas, a averiguar que dados tinham armazenados e as respetivas medidas de segurança, deverá constituir condição suficiente para colocar na ordem do dia o impacto de um Ciberataque e vir a estabelecer a Cibersegurança como prioridade para a proteção dos dados pessoais.

---

[33] *Idem,* p.13 "90% das organizações recebem *malware* através deste canal."

[34] European Data Protection Supervisor "Leading by Example, EDPS 2015-2019", 2019, p.68, disponível em: <https://edps.europa.eu/data-protection/our-work/publications/strategy/leading-example-edps-2015-2019_en>, acedido a 26/04/2020.

[35] Cisco and Cybersecurity Ventures Press Release 2019, Cybersecurity Almanac, junho de 2019, disponível em: <https://cybersecurityventures.com/cybersecurity-almanac-2019/>, acedido a 3/9/2020.

[36] World Economic Forum "The Global Risks Report 2020", 15ª edição, p.12, disponível em: <https://www.weforum.org/reports/the-global-risks-report-2020>, acedido a 6/8/2020.

4. Proteção e segurança de dados desde a conceção e por defeito

A proteção de dados desde a conceção e por defeito, preceituadas no art. 25.º do RGPD, têm um papel fulcral nos dados pessoais, podendo resultar do seu não cumprimento a aplicação de coimas[37], o que implica que a privacidade esteja integrada no conjunto de requisitos não funcionais desde o momento em que se concebe e desenha[38] e devendo, em função disso, ser também arquitetada uma segurança desde a conceção e por defeito, através de medidas técnicas e organizativas. De igual modo, a proteção por defeito (n.º 2 do art. 25.º do RGPD) tem um papel importante, no que à Cibersegurança diz respeito, através da limitação de acesso ou na minimização dos dados[39] que resulta numa postura mais cautelosa em relação àqueles, protegendo a sua segurança.

Por via disso, a proteção de dados pessoais (Cibersegurança) não pode jamais ser encarada como colocando em causa a funcionalidade e viabilidade de uma organização, sob pena de colocar em risco os dados que ela se propõe tratar.

Não ter isso em conta será como construir um automóvel sem cinto de segurança.

Atualmente, já temos departamentos jurídicos, *developers*, marketing e recursos humanos, todos sentados à mesma mesa para assegurar que as medidas de proteção dos dados pessoais e a sua ética estejam integradas ao longo do ciclo de vida de um produto/serviço, que se faz realizando a integração da proteção de dados pessoais e da Cibersegurança de uma forma colaborativa, quase orgânica. Tratando-se de um processo contínuo, pode suceder que uma medida implementada no início já não esteja a proteger nas mesmas condições, o que pode resultar no aumento de risco, daí ser necessário ter em atenção o estado da arte, conforme decorre do próprio artigo, não significando, por isso, que seja necessário um investimento avultado, como também no sentido oposto, a falta de

---

[37] Alínea c) do n.º 1 do art. 38.º da Lei nº 58/2019 e alínea a) do n.º 4 do art. 83.º do RGPD.

[38] Agencia Española Protección Datos, "Guía de Privacidad desde el Diseño", outubro 2019.p.8, disponível em: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad--desde-diseno.pdf>, acedido a 24/07/2020.

[39] Alínea c) do n. º1 do art. 5.ºdo RGPD.

investimento não pode ser causa justificativa para o não cumprimento da proteção de dados pessoais.

Cumpre, ainda, referir que não existem medidas de segurança mais adequadas do que outras, o que é relevante é a sua eficácia, este é o cerne do conceito de proteção de dados desde a conceção[40] e, por conseguinte, da Cibersegurança.

É, em função do acima descrito, essencial que o responsável pelo tratamento, quando esteja a implementar as medidas, tenha o entendimento necessário dos direitos e princípios que estão em causa e saiba que estão em causa direitos dos titulares dos dados que devem ser invioláveis.

Assegurar a privacidade e a segurança dos dados pessoais não podem ser obstáculos, mas premissas de quem os trata, desde a conceção e por defeito.

5. As Medidas de Segurança

O RGPD[41] refere a obrigação do responsável pelo tratamento e o subcontratante aplicarem medidas técnicas e organizativas de forma a assegurarem um nível de segurança adequado ao risco, sendo necessário, portanto, analisar qual o nível de adequação exigido para essas medidas garantirem a segurança dos dados.

Os sinais dados não são promissores, por exemplo, quando na alínea g) do n.º 1 do art. 30.º do RGPD se faz referência ao registo das atividades de tratamento e de que neste deve constar a descrição geral das medidas técnicas e organizativas no domínio da segurança, "se possível", o que lhe retira relevância e lhe confere um caráter opcional, negligenciando o facto de os dados pessoais estarem no ciberespaço implicar inevitavelmente um risco[42] para os direitos dos titulares, devendo, por essa ordem de razão, constituir, desde logo, um caráter obrigatório de implementação

---

[40] European Data Protection Board "Guidelines 4/2019 on Article 25, Data Protection by Design and by Default" novembro 2019, p.7, disponível em: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en>, acedido a 10/07/2020.

[41] Alínea f) do n.º 1 do art. 5.º, 32.º e considerandos 74 e 78 do RGPD.

[42] N. º 5 do art. 30.º do RGPD.

de medidas de segurança, não apenas para organizações com mais de 250 trabalhadores.

Outra questão que requer algumas cautelas diz respeito às "medidas técnicas e organizativas adequadas" que surge no RGPD como conceito indeterminado e deixa ao livre arbítrio de cada organização definir quais são e vir a descurá-las, resultando em efeitos severos para a proteção dos dados pessoais.[43]

No que às medidas de segurança o RGPD se refere, surge a pseudonimização[44] como uma das medidas técnicas possíveis e recomendadas para a segurança dos dados, segundo a alínea a) do n.º 1 do artigo 32.º, ainda que possa não ser a mais adequada dado poder haver o risco de uma "inversão não autorizada"[45] e dessa forma ser reversível. Por essa razão, vê-se como mais aconselhável[46] a cifragem para dados mais sensíveis, podendo ser uma medida alargada a todo o tipo de dados pessoais, o que diminuiria o risco de violação dos mesmos.

A tecnologia tem aqui um papel fulcral para o cumprimento da proteção de dados pessoais tanto na cifragem de todos os dispositivos que contenham dados pessoais (PC´s, telemóveis, *pens* USB), como na cifragem de todos os *e-mails* que contenham dados pessoais (evitandas situações de envio de *e-mail* para destinatário errado com dados pessoais) e na cifragem da informação em serviços *cloud*. Por conseguinte, perante situações de perda ou violação de dados, se a organização detiver total controlo sobre a cifra, pode resguardar-se do embaraço de ter de notificar a autoridade de controlo, bem como os titulares dos dados, dessas falhas de segurança – isto, porque os dados são incompreensíveis fora do universo interno da organização.

Cifrar os dados, implica torná-los indecifráveis para quem não tenha autorização de acesso aos mesmos, sendo uma medida básica de mitigação

---

[43] Conforme decorre da Deliberação nº 984/2018 da Comissão Nacional de Proteção de Dados "as limitações técnicas não podem justificar a adoção irrestrita de procedimentos de validação de acessos que praticamente tornam irrelevante o núcleo essencial do direito fundamental à proteção de dados pessoais".

[44] Ponto 5 do art.º 4.º e considerandos 26, 28, 29 e 78 do RGPD.

[45] Considerandos 75 e 85 do RGPD.

[46] Grupo de Trabalho do Artigo 29.º, Parecer n.º 5/2014, 2014 p.33, disponível em: <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>, acedido a 9/07/2020.

do risco de perda ou roubo de dados pessoais, tornando-os, por essa via, ininteligíveis em casos de ataques de *ransomware* ou de outro tipo de violação de segurança.

Também a alínea b) do n.º 1 do art. 32.º e o considerando 39 do RGPD podem ser exemplificadores na importância da Cibersegurança no RGPD, atendendo a que a segurança é um estado transitório e que requer, para a atenuação dos riscos, que sejam cumpridos determinados requisitos para cumprir o desiderato a que se propõe desde o início.

As informações devem estar disponíveis para utilizar quando for necessário e os sistemas que a fornecem possam resistir adequadamente a ataques e recuperar ou evitar falhas (disponibilidade)[47], as informações serem observadas ou divulgadas apenas para aqueles que têm o direito de a saber (confidencialidade)[48], as informações devem ser completas, precisas e protegidas contra modificações não autorizadas (integridade)[49], as transações comerciais, bem como as trocas de informações entre empresas ou parceiros, devem ser confiáveis (autenticidade e não repúdio)[50], requisitos que facilmente serão postos em causa, se não existir um programa de Cibersegurança robusto.

O RGPD realça, de igual modo, a necessidade de realizar uma identificação e avaliação de riscos[51] dos ativos e dos processos de negócio, seguida da implementação de controlos de segurança de diferentes classes (tecnológicos, físicos e organizativos) em função das estratégias para a gestão das ameaças. A organização deve classificar os seus ativos (humanos, tecnológicos de *hardware* e *software*, dispositivos, dados, tempo e aplicações), de acordo com a criticidade e valor que estes ativos representem para si, quanto maior o risco para os direitos e liberdades para os titulares dos dados, mais rigorosas deverão ser as medidas a

---

[47] Art. 13.º e 15º do RGPD, que podem ficar em risco devido a ataques de negação de serviço, causas estruturais, causas naturais p.ex.

[48] Alínea f) do n.º 1 do art. 5.º e considerandos 75 e 83 do RGPD, através de acessos não autorizados, exfiltração de dados, espionagem comercial e/ou industrial, engenharia social, por exemplo.

[49] Alínea f) do n.º 1 do art. 5.º do RGPD, que podem ficar fragilizadas devido a fraudes, ataques à cadeia de distribuição, ataques *man-in-middle* p.ex.

[50] Considerando 49 do RGPD.

[51] N. º 2 do art. 32.º do RGPD.

implementar[52]. Esta decisão pode passar por mitigar, transferir ou evitar ou aceitar o risco, devendo apenas aceitar-se este quando não acarrete consequências significativas para a concretização das atividades críticas do negócio (dados pessoais).

De referir que os riscos de Cibersegurança não são muito diferentes dos riscos no espaço físico, a diferença assenta no impacto e na magnitude que têm os primeiros, devendo ser encarados como cruciais para os dados pessoais. Com uma clara visão sobre os riscos[53] será possível escolher as medidas de segurança dos dados pessoais que são necessárias[54]o que só resultará da integração da Cibersegurança e Proteção de Dados Pessoais.

Depois de definido o programa de Cibersegurança a implementar, é necessário realizar auditorias de segurança e mecanismos de supervisão, bem como a consolidação de informação de registo e monitorização num sistema integrado de gestão de eventos (SIEM) como formas de cumprir a alínea d) do n.º 1 do art. 32.º do RGPD e de aferir a eficácia do mesmo. Esta alínea é demonstrativa da sua relevância pelo facto de em grande parte das organizações as medidas apenas serem atingidas formalmente, o que não é suficiente, já que devem envolver a monitorização contínua dos controlos, avaliação e revisão recorrentes, criando uma melhoria eficiente na Cibersegurança da organização.

Posto isto, tanto o responsável pelo tratamento como o subcontratante[55] têm a obrigação de aplicação de medidas técnicas e organizativas

---

[52] ENISA, "Handbook on Security of Personal Data Processing", janeiro 2018, p. 6, disponível em <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing>, acedido a 18/05/2020.

[53] Considerandos 75, 76, 77 e art.83.º do RGPD.

[54] Information Commissioner's Office "A practical guide to IT security ideal for the small business", p.4, disponível em: <https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf>, acedido a 3/06/2020.

[55] No que diz respeito aos subcontratantes é necessário averiguar que medidas são tomadas efetivamente por estes e evitar ficar refém, de um acordo formal de subcontratação, pouco efetivo. Se o grau de exigência colocado por parte das organizações em relação ao tratamento dos dados pode ser frágil, em relação aos subcontratantes não é diferente, no que concerne à Cibersegurança, veja-se o caso dos provedores de *cloud services* subcontratados, contratos de "pegar ou largar" condicionando a segurança de quem os contrata. Montagnani, Maria Lillà e Cavallo, Mirta Antonella, "*Cybersecurity and Liability in a Big Data World*", *Market and*

adequadas para proteger os dados pessoais[56], cujo incumprimento pode resultar na aplicação de uma coima[57], tornando-se decisivo o grau de responsabilidade de cada um, no incumprimento do estabelecido nos art. 25.º e 32.º do RGPD.

A organização tem de centrar-se, para além do risco da própria organização, no risco do titular dos dados visto poder ainda acrescer à coima, instaurada pela autoridade de controlo, uma ação judicial[58] instaurada pelo titular dos dados pessoais, podendo resultar numa indemnização pelos danos sofridos[59], ficando a cargo de quem trata os dados pessoais[60] provar que não foi responsável, não desprezando, todavia, as consequências reputacionais que daí podem advir.

Ter uma Cibersegurança de dados pessoais deficitária não isentará, certamente, dessa responsabilidade como fica patente pelas ações tomadas por várias autoridades nacionais de controlo de vários países europeus que aplicaram sanções a organizações por incumprimento do art. 32.º do RGPD[61].

Contudo, mais do que avaliar as opções do legislador ou o grau de exigência da autoridade de controlo em relação às medidas de segurança adequadas, cumpre-nos indicar soluções[62] que podem, inclusivamente, ser encontradas no nosso ordenamento jurídico, podendo ter um papel

---

Competition Law Review, Volume II, No. 2, outubo 2018, p. 91-92 Art. 28.º e considerando 81 do RGPD.

[56] Art. 24.º e 28.º do RGPD.

[57] Alínea d) do n.º 2 do art. 83.º do RGPD e alínea i) do n.º 1 do art. 38.ºda Lei nº 58/2019.

[58] Art. 79.º do RGPD.

[59] Art. 82.º do RGPD e art. 33º da Lei nº58/2019.

[60] N. º 3 do art. 82.º do RGPD e n.º 2 do art. 33.º da Lei nº 58/2019.

[61] Disponível em: <https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_pt>; <https://edpb.europa.eu/news/national-news/2019/romanian-national-supervisory-authority-issues-fine-against-fan-courier_pt>; <https://edpb.europa.eu/news/national-news/2019/norwegian-data-protection-authority-imposes-fine-city oslo_en>; <https://gdprhub.eu/index.php?title=ANSPDCP__Fine_against_Enel_Energie_Muntenia>; <https://www.datatilsynet.no/contentassets/9d5792264c884f3a903d3981c38812ac/~-20_02191-1-vedtak-om-overtredelsesgebyr---ralingen-kommune-202444_10_1.pdf>, acedido a 17/11/2020.

[62] O recurso a normas de certificação e boas práticas de gestão de Segurança da Informação (ISO/IEC 27001 e NIST 800-53 poderão ser uma solução eficaz na segurança dos dados pessoais.

importante o recurso à Resolução do Conselho de Ministros 41/2018, de 28 de março de 2018, destinada a definir orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais e aplicá-las nas organizações excluídas da obrigação de possuírem medidas de segurança específicas, podendo ser uma ferramenta útil para as organizações, atendendo ao facto de ser neutra quanto ao tipo de tecnologia a utilizar e definir padrões mínimos.

Não tendo pretensões de se exibirem competências técnicas que não se possuem, elencam-se algumas medidas técnicas e organizativas, recomendadas pelo Centro Nacional de Cibersegurança, que podem representar o nível de adequação que pode estar implícito naquele conceito indeterminado anteriormente referido, de que são exemplo: a implementação de uma política de segurança, procedimento de notificação de incidentes, desenho e implementação de arquitetura e segurança perimétrica (*firewalls*, sistema de deteção e proteção de intrusão IDS/IPS/HIDS), implementação de sistema de recolhas e armazenamento de fluxos de tráfego, inventariação de ativos (CMDB), mapa de rede, recolha centralizada de registos (*logs*),criação de instrumentos de correção ou mitigação de incidente, entre outras.

Para além das medidas técnicas existentes, as medidas organizacionais são essenciais para prevenir e gerir um ataque, que passará por cada colaborador ter consciência do impacto do seu comportamento para evitar a concretização de um Ciberataque, o que requer o conhecimento não só da organização (vulnerabilidades e ameaças a que estão expostos) como também depende do nível da preparação, implicando testar, fazer simulações de ataques para responder de forma rápida quando acontecer, com o fito de melhorar a capacidade de resposta.

Clarificador da importância do acima referido é importante enquadrar em que ponto nos encontramos atualmente, e que de acordo com o *EY Global Information Security Survey 2019*, a informação mais valiosa para os ciberatacantes é a informação de clientes (17%), sendo os maiores Ciber riscos para as organizações, o *phishing* (22%) e, em segundo lugar, o *malware* (20%), o que evidencia a relevância da Cibersegurança para os dados pessoais.

Cumpre, por sua vez, fazer referência ao que está a ser realizado em termos de medidas implementadas, e que de acordo com o Eurostat

6/2020[63] de 13 de janeiro, 93% das empresas da União Europeia utilizam pelo menos um tipo de medida de segurança; 62% consciencializam os colaboradores das obrigações de medidas de segurança; apenas 24% disponibilizam formação; 34% têm documentos com políticas e medidas de segurança e 12% tiveram pelo menos um incidente de Cibersegurança em 2018. Segundo o referido estudo as medidas mais comuns são: atualizações de *software* (87%), autenticação de password forte (77%), *back up* (76%), controlo de acesso (64%), uso de VPN (42%), utilização de técnicas de encriptação para dados, documentos e *e-mails*, (38%) e testes de segurança (36%).

Não obstante tudo o que foi referido anteriormente, convirá ter a perceção de que não existe nenhuma medida técnica e organizacional de segurança que garanta na íntegra a segurança da proteção de dados e de que a única forma de garantir uma segurança impenetrável é não tratar os dados, que não é o que se pretende.

6. Firewall Humana

O elemento central da Cibersegurança são as pessoas, que atuam como a primeira linha de defesa na deteção de uma falha de segurança, devendo, dessa maneira, a segurança da organização ser uma responsabilidade daquelas[64], que será tão ou mais efetiva se lhe retirarmos a conotação tecnológica que ainda possui, de forma a que aquelas sejam sempre entendidas como parte fundamental.

A sensibilização dos colaboradores de uma organização torna-se essencial já que são eles quem efetivamente trata os dados pessoais, estando os responsáveis pelo tratamento e os subcontratantes obrigados a

---

[63] No que diz respeito a Portugal temos, 98% das empresas têm pelo menos uma medida de segurança; 28% têm documentos e medidas de cibersegurança, 54% consciencializam os colaboradores para estas medidas, 8% experienciaram pelo menos um incidente, disponível: <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>, acedido a 14/07/2020.

[64] World Economic Forum "The cybersecurity guide for leaders in today´s digital world", outubro 2019, p. 19, disponível em: <http://www3.weforum.org/docs/WEF_Cybersecurity_Guide_for_Leaders.pdf>, acedido a 12/06/2020.

assegurar que aqueles e terceiros estejam consciencializados das medidas de segurança e que as cumprem independentemente da dimensão que possuam[65].

As organizações devem procurar a consciencialização e não a imposição, devendo centrar-se no efeito positivo que vão ter, de forma a que as pessoas fiquem incentivadas a ter comportamentos ciberseguros, sendo algo intrínseco, que se torna um hábito nos processos de trabalho, mais ainda, quando falamos em tratamento de dados pessoais de outrem, não devendo interferir na produtividade, para se vir a estabelecer como um dos fatores potenciadores da Cibersegurança dos dados pessoais.

Ainda que, a Cibersegurança, sem dúvida, dependa da vertente tecnológica, a natureza humana, através da componente comportamental, tem um papel relevante que não deve ser descurado tendo em conta fatores comuns de não cumprimento das medidas de segurança como são o excesso de trabalho e a complexidade do sistema de segurança[66], a que acresce o desconhecimento de tecnologias e dos procedimentos de segurança. Para além disso, comportamentos que se registam a título pessoal, seja através de *apps* ou do *e-mail* pessoal, são mimetizados para a organização onde trabalham, desse modo, o que se faz atualmente na esfera da nossa vida pessoal e profissional não pode já ser considerado como desconexo ou passível sequer de não ser tido em conta, pois cada ação exercida numa das esferas de atuação pode ter um impacto efetivo e sério na outra. De facto, se tivermos em apreço que a grande maioria das pessoas passa uma parte substancial do seu tempo útil de vida, no seu local de trabalho, torna-se inegável que às organizações já não é possível deixar de assumir alguma responsabilidade pelos comportamentos pessoais dos seus colaboradores que terão impactos diretos na organização.

Situação evidente é a presença dos dispositivos móveis pessoais no local de trabalho, que é atualmente prática corrente, que deverá atentar as organizações para os riscos que possa representar para os dados

---

[65] Data Protection Comission "Guidance for Controllers on Data Security", fevereiro 2020, p.3, disponível em: <https://www.dataprotection.ie/sites/default/files/uploads/2020-02/Data%20Security%20Guidance_Feb20.pdf>, acedido a 22/04/2020.

[66] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity",abril 2019, p.13 disponível em: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, acedido a 19/06/2020.

pessoais ali tratados e que poderá constituir um incentivo para a criação de uma política de uso aceitável dos recursos de cada um (política *Bring Your Own Device*) como medida de segurança em razão de os dispositivos nem sempre estarem devidamente protegidos, devendo, por essa razão, conduzir a organização a ter como prioridade a formação inicial a todos os colaboradores, optando por treino de Cibersegurança pessoal para depois as pessoas atuarem com o mesmo rigor no local de trabalho, no sentido de garantir a segurança do mesmo. Entende-se que segregar a Cibersegurança a um único departamento é um equívoco, dada a abrangência daquela e do facto de todos os colaboradores serem uma das razões do sucesso e, claro, do insucesso, designadamente através de publicidade encoberta ou ataques de engenharia social, que procuram tirar partido da apetência natural do individuo para ser curioso e social. Aliás, a grande maioria dos ataques com sucesso, não se reveste de grande complexidade, antes resulta da fragilidade do fator humano na sua interação com as tecnologias ao invés das fragilidades das mesmas, sendo os ataques informáticos, na sua grande maioria, facilitados pelos colaboradores que desconhecem os "sinais" de alerta[67].

Como até nos melhores sistemas de segurança existem erros, requer-se uma resposta para esses incidentes como efeito mitigador, antecipando o que deve ser realizado, pois ainda que as medidas técnicas e organizativas estejam a funcionar, a medida mais importante em qualquer organização é assegurar que os colaboradores estejam cientes das suas responsabilidades[68].

Criar a perceção da importância da Cibersegurança dos dados pessoais entre os colaboradores é fulcral para que, quando estiverem a ser alvo de um ataque, saibam como responder, pois muitas vezes, nem sabem que foram alvo de um, nem como devem atuar, o que resulta na sua não comunicação, traduzindo-se em efeitos desastrosos para a organização, mas acima de tudo para os titulares dos dados pessoais.

---

[67] De acordo com o estudo IBM 2018 Cyber Security Intelligence Index, 75% dos incidentes de cibersegurança que envolviam *malware* estavam relacionados com negligência dos colaboradores, e consistem em clicar em links de *phishing*, uso de USB inseguras, uso de passwords fracas, por exemplo, disponível em: <https://www.ibm.com/security/data-breach/threatintelligence>, acedido a 12/07/2020.

[68] Alínea b) do art. 11.º da Lei 58/2019 e art. 24.ºe 37.º a 39.º do RGPD.

7. O Reporte de Incidente

O reporte de incidente de uma violação de dados pessoais está indissociavelmente associado à Cibersegurança em caso de um Ciberataque, e para o qual o RGPD os art. 33.º e 34.º preceituam a necessidade de notificar a autoridade de controlo e, em casos mais graves, o próprio titular dos dados em caso de violação de dados pessoais, podendo resultar o seu não cumprimento numa coima[69].

A obrigação do responsável pelo tratamento em relação aos incidentes de violação da proteção de direitos pessoais surge do princípio de *accountability* (responsabilidade) do n.º 2 do art. 5.º e do n.º 5 do art. 33.º do RGPD.

Tratando-se de um Ciberataque, estes tipos de notificações só serão fidedignas e, principalmente, eficientes, se houver um entendimento claro do que é a Cibersegurança de forma a responder da forma mais exata ao que vem elencado no n.º 3 do art. 33.º do RGPD, nomeadamente em termos de medidas a tomar, das consequências e, acima de tudo, da abrangência da violação. O n.º 4 do art. 33.º do RGPD refere, ainda, situações em que não seja possível fornecer todas as informações ao mesmo tempo, aqui, facilmente, se enquadrando alguns tipos de incidentes de Cibersegurança, que constituem violações mais complexas, em que seja necessária uma investigação forense aprofundada para determinar plenamente a natureza da violação e em que medida os dados pessoais foram afetados[70].

É, igualmente, importante ter em atenção que, em certos casos, a não notificação de uma violação, ou uma notificação incompleta, pode revelar uma ausência de medidas de segurança ou uma inadequação das medidas de segurança existentes. Por isso, uma organização que queira ser *accountable*, que pretenda respeitar as obrigações de segurança de dados, terá precauções com a violação da proteção de dados e, no caso de ocorrer, possuir procedimentos para identificar e comunicar o incidente,

---

[69] Alíneas j) e k) do n. º 1 do art. 38.º da Lei nº 58/2019 e alínea a) do n.º 4 do art. 83.º do RGPD.

[70] Grupo de trabalho do artigo 29 para a proteção de dados, "Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679", fevereiro 2018 p.12, disponível em:

<https://ec.europa.eu/info/law/law-topic/data-protection_en, acedido a 3/7/2020>.

reduzindo o dano infligido aos titulares dos dados pessoais, diminuindo o nível de exposição do responsável pelo tratamento em sofrer sanções e danos reputacionais.

Podemos, então, concluir que apenas notificar e comunicar não é suficiente, transcendendo a questão formal, pois, quando uma organização sofre um Ciberataque que resulte numa violação de dados pessoais, é necessário dar resposta imediata ao incidente e ter a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico[71]. Passará por estabelecer procedimentos e responsabilidades para assegurar uma classificação e resposta eficazes aos incidentes de segurança, através da criação de um procedimento interno para notificação de incidentes que indique como deve proceder um colaborador perante um incidente ou um evento suspeito, da preparação de um plano de monitorização, da posse de equipamento que permita a salvaguarda de informação considerada prioritária para a organização, possibilitando a respetiva reposição em caso de necessidade (*backup/restore*), de ter implementado um mecanismo de prevenção de perda de dados, ou DLP (*Data Loss Prevention*) que se traduz uma abordagem integrada e consolidada da segurança da informação, registo e análise de toda a atividade de acessos de modo a procurar ameaças prováveis[72].

Devem, por conseguinte, fazer parte do Plano de Continuidade de Negócio os elementos essenciais que permitam à organização continuar em operação perante um qualquer desastre ou incidente que cause (ou tenha potencial para causar) uma disrupção, significativa ou até total, na atividade, criando contactos alternativos em caso de reporte de incidente e de os sistemas ficarem comprometidos, impedindo o contacto[73].

Os responsáveis pelo tratamento devem, ainda, documentar todos os incidentes que ocorram, incluindo quando e como aconteceram e as ações de reparação adequadas, que lhes permitam demonstrar estar em

---

[71] Alínea c) do n. º 1 do art. 32.ºdo RGPD, os sistemas de armazenamento devem garantir a redundância e disponibilidade, não devendo existir nenhum "*single point of failure*".

[72] CNCS, "Roteiro para as capacidades mínimas de cibersegurança", outubro 2019, p. 33, disponível em: <https://www.cncs.gov.pt/content/files/cncs_roteiro_capacidades_minimas_ciberseguranca.pdf>, acedido a 4/07/2020.

[73] Idem, p.28.

compliance com a comunicação do incidente à autoridade de controlo. É, por sua vez, fundamental que a documentação contenha indicadores relativos à probabilidade do risco e à severidade do mesmo e ao seu potencial impacto nos direitos e liberdades do titular dos dados pessoais, que se pretendem salvaguardar.

Por fim, depois de identificado um incidente, a organização deverá promover uma variedade de medidas de mitigação que passam por mudanças: operacionais, de processo, de sistemas, promoção do treino de pessoas ou até a rescisão de contratos com trabalhadores e subcontratados. As organizações deverão tomar medidas para futuros incidentes, nas quais se incluem a discussão de lições aprendidas de forma a promover alterações, a monitorização e a utilização de métricas (devem ser revistas todas as provas que foram coletadas e a atuação dos colaboradores para identificar padrões e vulnerabilidades), bem como a apresentação de estudos para explicar o impacto na organização e a definição de soluções para estarem preparadas para o próximo ataque.

Para finalizar entende-se que para a fiabilidade de um reporte de incidente é necessário que a organização tenha um plano de gestão de crise alargado a todos os colaboradores para que, em caso de ataque, não fiquem a aguardar que a tecnologia os suporte. Tem-se como um dos maiores obstáculos à exatidão de um reporte de incidente, que reflita o mais aproximadamente o que aconteceu, o nível de conhecimento em Cibersegurança dos seus intervenientes o que desvirtua, atualmente, o seu propósito que é assegurar a proteção dos dados pessoais.

Mais do que reportar um incidente, é necessário saber que medidas se devem tomar e dessa forma atenuar os danos sofridos pelos titulares, podendo ser uma atenuante na aplicação de uma coima[74] que constitui uma contraordenação grave no ordenamento português[75].

Convém, ainda, referir, que a adoção de medidas de proteção adequadas ainda que possa evitar que se tenha de comunicar ao titular de dados pessoais a referida violação, conforme dispõe o n.º 3 do art. 34.º do RGPD, não estará a ter em conta de um Ciberataque, atendendo às suas caraterísticas e ao facto inerente de ter uma abrangência maior, dada a amplitude do ciberespaço, ser "suscetível" de aumentar o risco para os

---

[74] Alínea c) do n. º 2 do art. 83.º e considerandos 85, 87 e 88 do RGPD.

[75] Alínea j) do n.º 1 do art. 38.º da Lei nº 58/2019.

direitos e liberdades das pessoas singulares irremediavelmente, o que lhe deveria conferir de forma imediata, no nosso entendimento, um caráter de obrigação de comunicação, nos termos do n.º 1 do art. 34.º do RGPD.

Tratando-se de um Ciberataque não podemos deixar de fazer referência, no que diz respeito ao reporte de incidentes de Cibersegurança *tout court,* que a Diretiva UE 2016/1148, de 6 de julho de 2016, encorajou as organizações a pensar de uma forma holística sobre a notificação de incidentes, não incidindo unicamente em incidentes financeiros e a colocar os dados pessoais na ordem do dia[76]. Através da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, e transpôs a referida Diretiva, identificaram-se setores e subsetores de operadores de serviços essenciais como fazendo parte do seu âmbito, porém excluiu-se a obrigação da notificação de um incidente por parte da maioria do tecido económico português, limitando-a à notificação voluntária em caso de incidente[77], retirando, desde logo, responsabilidade a quem sofre um Ciberataque aos dados pessoais que trata. Tanto a Diretiva (UE) 2016/1148 como o RGPD representaram um papel importante na obrigação dos atores do ciberespaço aprimorarem as competências em Cibersegurança[78], ainda que peque por defeito pela abrangência reduzida e que poderia ter servido para alavancar a inclusão da Cibersegurança na Proteção de Dados Pessoais, e não ficar reduzido a uma putativa cooperação entre as duas.[79]

Saber como responder a um incidente e qual o passo seguinte é primordial para estabelecer um reporte de incidente fidedigno das possíveis consequências para os dados pessoais.

---

[76] United States Chamber of Commerce and Hunton Andrews Kurth "Aligning Data Breach Notification Rules Across Borders", 2019, p. 12, disponível em: <https://www.huntonprivacyblog.com/2019/04/04/hunton-partners-with-the-u-s-chamber-of-commerce--on-seeking-solutions-aligning-data-breach-notification-rules-across-borders/>, acedido a 3/4/2020.

[77] Art. 20.º Lei n.º 46/2018, de 13 de agosto.

[78] ENISA "Study on CSIRT landscape and IR capabilities in Europe 2025", fevereiro 2019, p.5, disponível em: <https://www.enisa.europa.eu/publications/study-on-csirt-landscape--and-ir-capabilities-in-europe-2025>, acedido a 19/04/2020.

[79] N. º 8 do Art. 7.º da Lei nº 46/2018 de 13 de agosto e Considerando 63 da Diretiva (EU) 2016/1148 de 6 de julho de 2016.

Conclusão

Ao longo deste artigo, pretendeu-se sublinhar a importância que a Cibersegurança deve ter na proteção dos dados pessoais, atendendo a que o RGPD serviu para colocar a Cibersegurança na agenda e para que dependa desta para a sua efetiva execução. Por esse motivo, o RGPD poderá ser o impulsionador que faltava para a implementação da Cibersegurança como parte integrante da proteção de dados pessoais e estabelecer-se como uma prioridade do responsável pelo tratamento, mas também do titular dos dados. Se é evidente que a violação de dados pessoais implica consequências para o titular dos mesmos, consequentemente, a entidade responsável pelo tratamento será responsabilizada em razão disso, com repercussões tanto na reputação, como na continuidade da atividade, em coimas, em prejuízos financeiros, ou em termos legais, fatores que podem ser a pedra de toque para a inclusão da Cibersegurança na proteção de dados pessoais, conferindo-lhe um papel diferenciador e que será aproveitado pelos titulares dos dados, em resultado disso.

O objetivo da inclusão da Cibersegurança na proteção de dados pessoais só pode ser concretizado se os responsáveis pelo tratamento dos dados forem suficientemente "incentivados", através de meios jurídicos ou da ponderação dos riscos reputacionais e financeiros (podendo ser estes últimos a motivação que faltava), a tomar as medidas necessárias para assegurar que esta proteção seja colocada em prática.

No que se refere aos meios jurídicos, as autoridades de controlo de proteção de dados estão no centro do sucesso ou do falhanço da execução do RGPD mas se não possuírem os recursos adequados para aplicar a lei, as organizações acabarão por ignorá-la pelo facto de não ser executada ou ser executada de forma lenta, com repercussões para os titulares dos dados pessoais.

Retira-se ainda do exposto ao longo do artigo que, não é pelo facto de a legislação ser executada que os dados pessoais não deixam de estar em risco. De realçar que se a preocupação de uma organização for apenas cumprir o RGPD, já falhou em grande parte, pois a proteção de dados pessoais, sendo um imperativo legal, deverá ter, impreterivelmente, acoplada uma responsabilidade ética que vai para além de qualquer diploma. Ainda que seja tentador, e nos transmita algum conforto, limitar o cumprimento do art. 32.º do RGPD à avaliação (insuficiente) realizada

por uma autoridade de controlo traduz-se num risco, no estado atual do ciberespaço.

Mais do que ver a proteção dos dados pessoais como uma obrigação legal e percecionando-a apenas com uma visão burocrática, de simples cumprimento de alguns artigos de um determinado regulamento, seja através da criação de politicas de privacidade ou da celebração de acordos de subcontratação com parceiros, por exemplo, deverá ser encarada como a obrigação de estar em *compliance* não apenas com a legislação, mas com a proteção de dados pessoais por si só.

Certamente que o titular dos dados quer que se cumpra a lei, mas, acima de tudo, que se protejam os seus dados pessoais.

O aparente cumprimento que é transmitido pelos documentos em dia, a ficha de atividade de tratamento de dados pessoais, a atribuição de um Encarregado de Proteção de Dados (EPD), etc. (que não são devidamente acompanhadas pelas medidas de segurança) e que, ainda assim, para a autoridade de controlo possa ser suficiente para demonstrar *accountability* e ficar imunes às possíveis coimas, é uma visão simplista do que é a proteção de dados pessoais. Para se cumprir esse propósito é primordial um programa de Cibersegurança de acordo com a realidade atual, não se limitando a medidas avulsas que nos garantam o cumprimento legal mas não possuam a eficácia necessária, dado que a produção legislativa e a sua execução dificilmente acompanharão o ritmo da evolução tecnológica. Porém, não significa que, por essa razão, se deva diabolizar a tecnologia e o ciberespaço, pois retroceder à era do analógico poderá ser um sinal de desistência em acompanhar a evolução, com efeitos irreversíveis para os dados pessoais.

Esta permanente revolução tecnológica e sociológica que vivemos, vem retirar qualquer fé que se possa ter numa lei atualizada e que é potenciada pelos anacronismos de leis avulsas desadequadas à realidade da época que vivemos, cumprindo ao Direito, sem abdicar dos princípios fundamentais do ordenamento jurídico, tentar acompanhar a (inevitável) inovação tecnológica, aproveitando-a em seu favor sem que isso signifique uma "servidão" tecnológica que estimule a isenção de responsabilidade.

Igualmente, os próprios titulares não se podem eximir da obrigação de proteger os seus próprios dados, não devendo jamais desconsiderar estes em detrimento de outros interesses, sendo importante a consciencialização

das pessoas do valor que têm os seus próprios dados e dos que a elas lhes são confiados e que fortalecerá o grau de exigência.

Tendo em conta que os dados pessoais só terão relevância se permanecerem seguros, significa que a Cibersegurança não deve estar em segundo plano, nem ter um caráter facultativo, só podendo alcançar a sua plenitude através de um grau de usabilidade acessível a quem trata dados pessoais, ficando intrinsecamente dependente da existência de uma *firewall* humana robusta. Entendendo-se que para a efetiva execução do RGPD em consonância com a Cibersegurança o responsável pelo tratamento ter-se-á de colocar no lugar tanto de autoridade de controlo, como de um *hacker* malicioso, mas sobretudo do titular dos dados, para dessa forma avaliar onde se está mais exposto garantindo a segurança dos dados pessoais.

Pese embora não exista uma fórmula mágica, a implementação da Cibersegurança na proteção de dados pessoais depende das organizações que os tratam, bem como, ainda que com menor influência, das legislações existentes, mas sobretudo da sensibilização da sociedade civil.

Seria importante para os nossos dados pessoais que depois do advento da implementação do RGPD não viessem a ser negligenciados, não só pelas organizações, mas por cada um de nós, o que dependerá do nível de consciencialização que se venha a ter sobre o assunto, tendo como finalidade evitar o darwinismo da proteção de dados pessoais em que só sobrevivem os mais aptos e que resulta na exclusão da premissa de ter os dados seguros.

O objetivo deste artigo não é fazer juízos críticos sobre oportunidades perdidas com a legislação implementada, mas sim prever soluções para a segurança (Cibersegurança) dos dados pessoais chegando-se, a duas opções claras, ficar-se reduzido à legislação estando à mercê da inércia e descoordenação do legislador e do menor grau de exigência das autoridades de controlo em relação à Cibersegurança ainda que cumprindo a *accountability* ou ter uma atitude proativa de melhorar a Cibersegurança dos nossos dados pessoais e perceber que o propósito é proteger dados pessoais independentemente do que estabeleçam as regras legais e que possam pecar por defeito.

Deste modo, a chamada "autorregulação", com maior ou menor participação legislativa, tem no que concerne à Cibersegurança e à proteção de dados pessoais um papel decisivo, em especial na perspetiva

das organizações que querem preservar o bom nome, a reputação e a confiança do titular dos dados pessoais.

Tem-se por fundamental que a proteção de dados pessoais e a Cibersegurança tenham sempre por base os direitos fundamentais de cada indivíduo dado que qualquer sociedade terá de ter sempre espaço para a autonomia individual e para os direitos fundamentais de cada um e tal depende muito de cada um de nós e não apenas de qualquer lei ou regulamento. A era digital não pode, em momento algum, deixar-nos cair numa letargia em relação aos nossos direitos fundamentais, os quais são requisitos essenciais para o desenvolvimento de qualquer sociedade.

Posto isto, preconiza-se como política sensata em qualquer ciência que se deve procurar a explicação mais simples que for possível para qualquer problema que estejamos a tentar resolver por isso, implementar a proteção de dados pessoais sem a Cibersegurança parece algo desfasado com a era digital da vida social e laboral atual e que revela a dimensão do perigo por um lado e, por outro, a incapacidade dos meios para o neutralizar e que levou a escrever sobre o tema.

Integrar a Cibersegurança na Proteção de Dados Pessoais não é uma opção, é um imperativo na era digital.

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, consequentemente, 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"[1]. 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.[2-3] Ao recorrer às técnicas enunciadas, a inteligência artificial consegue gerar uma análise preditiva de comportamento[4], sendo este o modelo predominantemente empregue no tratamento

---

[1] V. Morais Carvalho, Jorge, *Manual de Direito do Consumo*, 6ª edição, Almedina, 2019, p. 51.

[2] 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*.

[3] Sobre esta temática, confira-se Flach, Peter, *Machine Learning, The Art and Science of Algorithms that Make Sense of Data*, Cambrigde University Press, 2012.

[4] 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[5]. 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[6].

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, consequentemente, 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

---

[5] 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.

[6] Neste sentido, Domingos, Pedro, *A revolução do algoritmo mestre: como a aprendizagem automática está a mudar o mundo*, Letras & Diálogos, 2017.

ou deslocações"[7]. 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[8]. 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[9]. 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

---

[7] Este processo, nos termos do RGPD, traduz-se no tratamento de dados, estipulado no seu art. 4.º, n.º 4.

[8] 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.

[9] 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[10].

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[11].

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

---

[10] Igualmente, Morais Carvalho, Jorge, *op. cit.*, p. 52.

[11] Neste sentido, "Data Brokers: A Call for Transparency and Accountabily", *Federal Trade Commision*, 2014, pp. 1-110.

clientes ou até mesmo para aperfeiçoar o seu público-alvo[12]; (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[13]. 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[14].

---

[12] 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.

[13] 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.

[14] 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"[15]. 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.

---

[15] 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 encarregue 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[16].

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[17], 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.

---

[16] 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.

[17] 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 despender 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.[18]

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.

---

[18] 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 despender 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[19].

---

[19] 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[20].

---

[20] 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.º retira-se uma obrigação de resultado: a empresa a quem os dados pessoais foram fornecidos terá que eliminá-los[21]. 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.º 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[22]. 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 consequente 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[23].

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.

---

[21] Também no sentido de o art.17.º 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.

[22] Também assim, Palmela Fidalgo, Vítor, *op. cit.*, p. 189.

[23] Elencando também estes obstáculos face à obrigação de apagar os dados pessoais nos termos do artigo 17.º 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 fáctica, 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[24] e as variadas legislações que proíbem e sancionam a discriminação. Referimos discriminação porque, compreendendo que os algoritmos agem

[24] 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[25].

Tendo o ordenamento jurídico consagrado a proibição de discriminação, tanto na Constituição da República Portuguesa, no seu art. 26.º, como em legislação avulsa[26], 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[27]. Chegados aqui, é possível avaliarmos que ambas as situações são passíveis de ocorrem nos contratos acima identificados.

---

[25] Igualmente, Morais Carvalho, Jorge, *op. cit.*, p. 52.

[26] Tal como a Lei n.º 14/2008, Lei n.º 93/2017 e Lei n.º 46/2006.

[27] 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[28].

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[29]. 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[30] 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

---

[28] 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.

[29] Neste sentido, *idem, ibidem*, p. 43.

[30] 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 subjugados 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.[31] Concluindo, um fiduciário de informações é uma pessoa (singular ou coletiva) que, pela sua relação com uma outra, obteve informações sensíveis sobre esta, detendo, consequentemente, 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[32].

---

[31] V. Balkin, Jack, *op. cit.*, pp. 1205-1209.

[32] 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 estádio, 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 estádio, 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, conjetura potencialmente mais perigosa ainda, não compreenderem a extensão das consequências que poderão advir desse mesmo tratamento. A generalidade dos indivíduos não perceciona 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.

Cremos, 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.

Índice Geral