REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

LISBON LAW REVIEW

Número Temático: Tecnologia e Direito

ANO LXIII 2022 NÚMEROS 1 E 2

REVISTA DA FACULDADE DE DIREITO
DA UNIVERSIDADE DE LISBOA
Periodicidade Semestral
Vol. LXIII (2022) 1 e 2

LISBON LAW REVIEW

PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade – 1649-014 Lisboa – Portugal

EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO
LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

ISSN 0870-3116 Depósito Legal n.º 75611/95

Data: Outubro, 2022

ÍNDICE 2022

LIVROS & ARTIGOS

Reconhecimento facial (FRT) e direito à imagem

Facial recognition (FRT) and image rights

José A. R. Lorenzo González*

Resumo: A videovigilância constitui, só por si, uma séria ameaça de intrusão ilícita nos direitos à imagem e à intimidade de cada indivíduo. Se lhe estiver associado um sistema automatizado de reconhecimento facial (FRT), os perigos envolvidos incrementam-se incomensuravelmente. Primeiro, devido à forma, quase descontrolada, como a base de dados se constrói e construirá, sem possibilidade prática de os titulares dos direitos às imagens que a compõem se pronunciarem sobre o uso que se lhes dá. Segundo, em flagrante violação da regra da igualdade, por assim se potenciarem fenómenos de discriminação negativa sempre que as FRT não assentem em bases de dados confiáveis (enviesamento algorítmico). O reconhecimento facial automatizado veio, porém, para ficar. Até porque inegavelmente apresenta, em alguns casos, óbvia utilidade social. Pelo que não é juridicamente concebível a sua interdição. Ao Direito caberá, isso sim, fixar os limites dentro dos quais ele se poderá legitimamente empregar.

Palavras-chave: Inteligência artificial (IA); Reconhecimento facial; Direito à imagem; Igualdade.

Abstract: Video surveillance composes, just by itself, a serious threat of unlawful intrusion on some rights of each individual: image and privacy, mainly. If an automated facial recognition system (FRT) is associated with it, the dangers involved increase immensely. Firstly, due to the way in which the database will be built in an almost wild way, with no practical possibility for the holders of the rights to the images that compose it to consent on the use that is given to them. Secondly, because negative discrimination is enhanced in flagrant violation of the equality rule if the FRT is not grounded on a reliable database (algorithmic bias). However, automated facial recognition is here to stay. Even because it undeniably presents, in some cases, clear social benefit. Therefore, its ban is not legally conceivable. Rather, it will be up to the Law to set the limits within which it can legitimately be used.

Keywords: Artificial intelligence (IA); Facial recognition technologies (FRT); Right to image; Equality.

* Professor Associado com Agregação da Faculdade de Direito da Universidade Lusíada. Centro Universitário de Lisboa.

Sumário: 1. O direito à imagem no Código Civil. 2. A jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH). 3. Inteligência Artificial? 4. O perigo de enviesamento (*algorithtmic bias*) no campo do reconhecimento facial. 5. Licitude das FRT. 6. Conclusões.

1. O direito à imagem no Código Civil

O retrato equivale, no Código Civil, a qualquer forma de representação figurativa de uma pessoa (fotografia, pintura, *cartoon*, caricatura, escultura, filmagem sobre qualquer suporte, vídeo, etc.), dado que a finalidade, quer desta disposição, quer daquela que constitui o seu reflexo constitucional (artigo 26º, n.º 1, Constituição), se consubstancia no reconhecimento do grau máximo de intangibilidade da imagem individual. Ainda que, no que toca ao preceito contido no artigo 79.º do Código Civil, o que sobretudo esteja em causa seja o direito de "controlar a captação, recolha e utilização de sinais visualmente identificadores da pessoa"[1], enquanto pela disposição constitucional o que se tutela seja, principalmente, o direito de cada qual adotar a imagem que entender[2].

Naturalmente, o retrato de uma pessoa não pode ser obtido e/ou difundido sem o respetivo consentimento[3]. Este há de valer e ser eficaz dentro dos parâmetros

---

[1] Acórdão do Tribunal Constitucional n.º 81/07, de 06/02/2007, Proc. n.º 05/0871 – DR n.º 56, série II, de 20/03/2007.

[2] Não falta quem considere que "a imagem pessoal não se restringe à figura, à fisionomia da pessoa, ao corpo que aparece no mundo real e sensível. A imagem pessoal é composta não apenas pelo corpo, por todo o corpo da pessoa humana, mas também pela sua personalidade, pelo seu conhecimento, pela sua educação, pela sua vida enquanto ser humano, pela sua idade, pelo seu aspeto estético, pela sua profissão, pelos seus gostos, pela sua vida social, pela sua sabedoria, pela sua inteligência, pela sua integração na sociedade, na família, na cultura, pela sua sensibilidade humana e profissional, etc." (Adalberto Costa, *O Direito à Imagem*, Revista da Ordem dos Advogados, 2012, Ano 72, vol. IV, 1351). A ser assim, porém, a imagem individual incorporará, não só a aparência física, como ainda muitos outros bens da personalidade – o bom nome, a reputação, a honra, a consideração social, etc. –, numa amálgama que gera indeterminação. Afigura-se mais acertada, por isso, uma conceção restrita do objeto do direito à imagem que apenas alcance a forma externa do ser humano. Até por carecer de sentido a aplicação de qualquer das exceções que o n.º 2 do artigo 79.º do Código Civil institui à necessidade de consentimento para a captação e difusão da imagem individual quando esta se entenda naquele sentido amplo (cf. Gomes Canotilho – Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. I, Artigos 1.º a 107.º, 4.ª edição revista, Coimbra Editora, Coimbra, 2007, 467).

[3] Cf. Acórdão do Supremo Tribunal de Justiça de 07/06/2011, Proc. n.º 1581/07.3TVLSB.L1.S1: "I – Não obstante o direito à imagem ser um direito indisponível, no plano constitucional, a lei

estabelecidos pelos artigos 81.º ou 340.º do Código Civil[4]. E, sobretudo, tendo em consideração o efeito para o qual foi concedido[5].

Em contrapartida, não se pode descartar, porém, a regra *dominus membrorum suorum nemo videtur*. O que significa que nem qualquer consentimento é válido ou, que é o mesmo, que nem todo o consentimento legitima a intervenção na esfera jurídica de quem em tal assentiu.

De acordo com o conteúdo que se extrai do preceito encerrado no artigo 81.º do Código Civil, o consentimento daquele que autolimita algum direito de personalidade não valida a ingerência de terceiro na sua esfera jurídica se for contrário a "princípios de ordem pública"[6]. Tratando-se de um limite de difícil materialização, outro remédio não resta a não ser aquele que passa pelo recurso, como sempre sucede no preenchimento de conceitos abertos ou indeterminados, a casos concretos[7].

O consentimento previsto no artigo 81.º do Código Civil distingue-se daquele outro a que o artigo 340.º do mesmo diploma se reporta. Neste, ele funciona como causa de exclusão da ilicitude, justificando a conduta de quem *a priori* estaria a praticar um ato ilícito e, por isso, a incorrer em responsabilidade civil aquiliana nos termos gerais do n.º 1 do artigo 483.º do Código Civil. De todo o modo, que é o ponto mais saliente, aquele que produz a lesão não tem o direito de a provocar; apenas beneficia da tolerância daquele outro que a sofre.

Na hipótese do artigo 81.º, o consentimento para a restrição resulta tipicamente de um contrato celebrado entre quem a autoriza e quem a causa. Como qualquer

---

permite, dentro de determinados limites, a captação, reprodução e publicitação da imagem, desde que o titular do direito anua ou consinta essas atividades. (...) IV – Se alguém aceita, ainda que de forma tácita, ser fotografado para um determinado fim, não podem as imagens ser utilizadas para fim diverso, sem que para este específico fim tenha sido obtido prévio consentimento do titular ou pelo menos que, aquando da captação de imagens, não tivesse sido adquirido um sentido inequívoco de que o titular do direito permitiria na utilização das imagens captadas para esse específico fim. V – Para que ocorra uma situação de consentimento tácito, significação externa de autorização para a captação, reprodução e publicitação da imagem de quem quer, torna-se necessário que os sinais (significantes ou exteriorizáveis) do titular do direito se revelem ou evidenciem como inequívocos ou desprovidos de qualquer dúvida". Cf. Cláudia Trabuco, *Dos contratos relativos à imagem*, Revista "O Direito", Ano 133, 2001, II., 433.

[4] De harmonia com a máxima *volenti non fit iniuria*, admite-se que o titular de algum direito de personalidade possa dar consentimento a que uma conduta alheia suscetível de o lesar, efetivamente sobrevenha, legitimando assim, através da autolimitação permitida, o comportamento de quem produzir uma intromissão na sua esfera jurídica.

[5] Ver acórdão da Relação de Lisboa de 22/09/2005, R. 5011/2004, Col. de Jur., 2005, IV, 105.

[6] Cf. acórdão do Supremo Tribunal de Justiça n.º 03B2361, de 25/09/2003.

[7] Ver, por exemplo, acórdão da Relação de Évora n.º 2788/04-3, de 24/02/2005.

contrato, sujeita-se à regra *pacta sunt servanda*. De onde decorre que a parte que beneficia do consentimento tem o direito de exigir que a outra suporte os efeitos jurídicos e factuais associados à sua execução[8].

Atendendo, contudo, ao facto de estar em causa matéria dotada de importância transcendente, como é aquela que respeita à tutela da personalidade humana, abriu-se uma importante exceção à regra contida no n.º 1 do artigo 406.º do Código Civil: o consentimento em causa é sempre (não admitindo, pois, cláusula em sentido inverso) livremente revogável. Significando isto, portanto, que o titular do direito de personalidade autolimitado pode, a todo o tempo e discricionariamente, pôr termo ao consentimento antes concedido[9]. Uma aplicação desta ideia encontra-se inscrita no n.º 6 do artigo 8.º da Lei n.º 12/93, de 22 de abril: "o consentimento do dador" (de órgãos e tecidos de origem humana) "ou de quem legalmente o represente é sempre prestado por escrito, sendo livremente revogável".

Não é impossível que a limitação emergente do assentimento do próprio titular de algum direito de personalidade se funde em simples ato unilateral da sua autoria[10]. Nesta hipótese não se concebe, porém, o surgimento a favor de outrem de "legítimas expectativas" carentes de tutela (por via de ressarcimento ou por outra).

Aquele que revogar a permissão anteriormente conferida fica obrigado, todavia, a "indemnizar os prejuízos causados às legítimas expectativas da outra parte".

Qualquer que seja a melhor interpretação a dar a este segmento normativo, uma coisa afigura-se certa: não pode o montante da indemnização em causa ser tão alto que, na prática, inviabilize o exercício do direito de livre revogação. Por isso, é de excluir de imediato a possibilidade de a referida compensação poder abranger tanto os danos emergentes como os lucros cessantes (tal qual sucederia como se em causa estivesse uma pura obrigação de indemnizar nos termos gerais do n.º 1 do artigo 564.º do Código Civil).

Note-se, suplementarmente, que os prejuízos a reparar são aqueles que atingirem as "legítimas expectativas" da outra parte e não os que resultarem da violação de direitos alheios (*v.g.* artigo 483.º, n.º 1, Código Civil). Ora, a expectativa é, reconhecidamente, algo menos do que um direito subjetivo (com maior rigor, é uma situação jurídica que pode desembocar num direito, mas ainda não o é).

Pelo que, em conclusão, admitindo-se a justeza do direito à atribuição da compensação em causa, impõe-se que esta apenas se destine a cobrir as despesas que a "outra parte" fez, mas não teria feito se o consentimento jamais tivesse sido

---

[8] Ver acórdão do Supremo Tribunal de Justiça de 25/10/2005, Proc. n.º 05A2577.
[9] Cf. acórdão da Relação do Porto de 06/01/2014, Proc. n.º 1007/11.8TBMCN.P1.
[10] Ver acórdão da Relação de Lisboa de 14/04/2016, Proc. n.º 1454/09.5TVLSB.L1-8.

outorgado. Quer isto dizer, no fundo, que por conta daquele que se aproveita da autolimitação outorgada pelo titular do direito de personalidade é que deve correr o risco de este o revogar quando entender. O que tendo em conta que retira benefícios que, em princípio, lhe estariam liminarmente vedados, é uma solução razoável[11].

A falta de referência explícita, na lei, à necessidade de consentimento para a captação e eventual posterior difusão da imagem individual não significa que ele não se requeira. Por ser óbvio, apenas se tornou supérflua a sua inclusão[12]. Além disso, como a aquisição da imagem de outrem é diferenciável do momento relativo à sua disseminação, cabe também entender que a anuência para a primeira não envolve forçosamente a permissão para a segunda. O que parece ser especialmente importante acentuar no que toca ao uso das FRT.

O preceito contido no artigo 79.º do Código Civil tem utilidade, mormente, por através dele se manifestar a preocupação de produzir um inventário (ainda que meramente exemplificativo) dos casos em que a captação e/ou a divulgação da imagem alheia não depende do assentimento do seu titular.

---

[11] Cf., neste sentido, Pedro Pais de Vasconcelos, *Direito de Personalidade*, Almedina, Coimbra, 2006, 165 a 168.

[12] Exigir o consentimento da pessoa visada para que a respetiva imagem possa ser captada e divulgada dá implicitamente origem à criação, sobre ela, de um monopólio de uso e exploração a seu favor. Em alguns Direitos da *Common Law* – em particular, no Direito de alguns Estados dos EUA – tal constatação fez despontar o chamado *right to publicity*: direito de propriedade intelectual que protege cada sujeito contra a apropriação indevida do seu nome, da sua imagem ou de outros elementos da sua identidade pessoal – como o apelido, o pseudónimo, a voz, a assinatura – para benefício económico de outrem. Tal como se de uma *trademark* se tratasse (cf., por exemplo, Stacey Dogan, *What the Right of Publicity Can Learn from Trademark Law*, Stanford Law Review, vol. 58, 2006, 1190). Qualquer que seja o melhor enquadramento a dar-lhe, é indisputável *v.g.* que: *(i)* "É proibida... a publicidade que: e) Utilize, sem autorização da própria, a imagem ou as palavras de alguma pessoa" (artigo 7.º, n.º 2, Decreto-Lei n.º 330/90, de 23 de outubro – Código da Publicidade); *(ii)* "Todo o praticante desportivo tem direito a utilizar a sua imagem pública ligada à prática desportiva e a opor-se a que outrem a use para exploração comercial ou para outros fins económicos" (artigo 14.º, n.º 1, Lei n.º 54/2017, de 14 de julho – regime jurídico do contrato de trabalho do praticante desportivo).
O *right to publicity*, na visão comum da doutrina dos EUA, busca o seu alicerce no *right of privacy* (Randall T.E. Coyne, *Toward a Modified Fair Use Defense in Right of Publicity Cases*, William & Mary Law Review, vol. 29, 1988, 782). Historicamente, a respetiva autonomização fundou-se, sobretudo, em razões de índole económica: a imagem – ao menos, a das pessoas "famosas" – é um bem capaz de proporcionar avultados benefícios patrimoniais, ao próprio ou a terceiros. Entendendo-se que a sua exploração assenta numa espécie de *property right* (artigo 1303.º, Código Civil), torna-se relativamente simples justificar, por esta via, a licitude do estabelecimento de "limitações voluntárias a direitos de personalidade" (artigo 81.º, Código Civil) a título oneroso (cf. Menezes Cordeiro, *Tratado de Direito Civil Português*, I, Parte Geral, tomo III, Pessoas, 2004, Almedina, Coimbra, 195).

Podem agrupar-se tais hipóteses em três classes:

– numa, são razões atinentes à própria pessoa retratada que justificam a desnecessidade de consentimento (notoriedade, cargo que desempenha, etc.);

– noutra, estão em causa razões ligadas à finalidade da captação/divulgação do retrato (exigências de polícia ou de justiça, intuitos científicos, didáticos ou culturais);

– na última, por fim, é a própria natureza do contexto em que a pessoa é retratada que funda a superfluidade do consentimento (imagem enquadrada na de lugares públicos, na de factos de interesse público ou que hajam decorrido publicamente).

A notoriedade pessoal (que tipicamente dá origem ao aparecimento da chamada figura pública) tem contornos muito imprecisos. O critério geral para a sua definição há de passar, hoje em dia, pela frequência com que certa pessoa surge (ao que parece, seja por que razão for) nos meios de comunicação social e, designadamente, nos *mass media*.

O mesmo se diga no que toca à notoriedade decorrente do exercício de cargos públicos. Embora, nesta hipótese, sempre se deva prevenir que não é certamente qualquer "cargo público" (tal como, por exemplo, a expressão surge utilizada para efeitos do n.º 1 do artigo 50.º da Constituição) que confere notabilidade ao seu titular. O que está aqui em causa – pois só nessa medida se justifica prescindir da autorização da pessoa retratada – é aquele cargo ao qual esteja associada uma certa dose de publicidade, trate-se de cargo verdadeiramente público ou não.

Num caso ou no outro, a inutilidade do consentimento do retratado dá-se dentro do perímetro da sua notoriedade[13]. Fora disso, regressa-se à regra instituída pelo n.º 1 do referido artigo 79.º[14].

As exigências de "polícia ou de justiça" determinam igualmente a superfluidade do consentimento para a obtenção/difusão do retrato. A fórmula usada é, de novo, de alcance dúbio[15]. Parece relativamente assente, todavia, que a exceção ocorrerá para, por exemplo, se conseguir proceder à detenção de algum suspeito da prática

---

[13] Cf. acórdão da Relação de Lisboa de 08/01/2009, R. 6465/2008, Col. de Jur., 2009, I, 88.

[14] Cf. acórdão da Relação de Lisboa de 28/01/1999, R. 6314/98, Col. de Jur., 1999, I, 93. Cf., igualmente, acórdão do Supremo Tribunal de Justiça de 08/11/2001, Proc. n.º 01B2853.

[15] No contexto desta exceção, o Tribunal Constitucional já firmou jurisprudência no sentido de entender que "a manutenção nos autos do retrato do recorrente contra a sua vontade (depois, aliás, de a sua inclusão ter ocorrido também sem consentimento, ou, sequer, conhecimento), configura uma restrição à possibilidade de controlo da utilização do retrato, e, portanto, uma limitação ao direito à imagem" (acórdão n.º 81/07, de 06/02/2007, Proc. n.º 05/0871, DR n.º 56, série II, de 20/03/2007).

de crime (*v.g.* mediante a divulgação de *retrato-robô* ou através do recurso a tecnologias de reconhecimento facial), ou, ainda por exemplo, para efeitos do disposto no n.º 6 do artigo 250.º do Código de Processo Penal[16].

A desnecessidade de consentimento do retratado fundada na publicidade do próprio local ou do evento em que a imagem da pessoa é colhida, supõe, pelo menos, que ela não tenha sido especialmente visada. Pelo que a exceção estará verificada sempre que tal imagem seja captada por razões fortuitas; ou, de outro modo, quando a referida imagem tenha sido apenas intercetada pelo autor do retrato. Assim, por exemplo, se o operador de câmara aponta a objetiva para uma certa pessoa que se encontre sentada numa bancada lotada de um estádio desportivo, apenas a poderá fotografar ou filmar se ela nisso (expressa ou tacitamente) anuir.

Qualquer uma das exceções erguidas pelo n.º 2 do artigo 79.º do Código Civil à necessidade de obtenção de anuência por parte da pessoa retratada deixa de ter aplicação (e, portanto, retorna-se à regra) sempre que a captação ou, sobretudo, a divulgação da imagem ofenda a honra, a reputação ou o decoro da pessoa[17]. Remete-se assim, no fundo, para a indispensabilidade de proteção devida a um outro direito de personalidade: o "bom nome e reputação" (artigo 484.º, Código Civil; artigo 26.º, n.º 1, Constituição).

O problema reside essencialmente, portanto, na definição do âmbito de aplicação das referidas exceções.

Tome-se, como paradigma, o que nestes tempos alegadamente sucederá na Ucrânia, no que respeita à identificação dos cadáveres de (eventuais) soldados russos mortos. Para quantificar o respetivo número, os ucranianos empregarão um *software* de reconhecimento facial concebido por uma empresa privada (Clearview AI) sediada nos EUA. O algoritmo, diz-se, recorrerá a um banco de dados que conterá mais de 20 mil milhões de imagens obtidas e indexadas a partir da Internet.

Como foram estas fotografias obtidas? Como estão a ser usadas? No banco de dados elas encontrar-se-ão identificadas pelo nome ou por qualquer outro método passível de autorizar a individualização dos retratados? Se o problema se colocasse entre nós, o segundo grupo de exceções a que atrás se aludia – exigências de "polícia ou de justiça" – estaria verificado?

---

[16] Cf. acórdão da Relação do Porto de 15/12/2021, Proc. n.º 515/10.2TBGMR-D.P1.

[17] Cf. o exemplo conferido por Pedro Pais de Vasconcelos – Pedro Leitão Pais de Vasconcelos, *Teoria Geral do Direito Civil*, 9.ª edição, Almedina, Coimbra, 2019, 75, nota 79.

2. A jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH)

No dizer do Tribunal Europeu dos Direitos Humanos (TEDH), o direito à proteção da imagem individual compõe um dos principais ingredientes da intimidade pessoal e envolve, forçosamente, o poder de supervisionar a sua utilização (*Reklos e Davourlis v. Grécia*, 2009, §§ 40-43). Exceto quando um indivíduo, consciente ou acidentalmente, permitir que a sua fotografia seja captada num contexto público ou similar, a proteção efetiva da imagem pressupõe, em princípio, a obtenção do consentimento do visado no momento em que ela é obtida e não simplesmente se e quando for publicada. Este princípio, contudo, não é absoluto. *V.g.* a integração de certo indivíduo na categoria de figura pública ou motivos de interesse público podem justificar o registo da imagem sem o seu conhecimento e a ocorrência da respetiva divulgação sem o seu assentimento.

No caso de pessoas detidas, presas ou, pelo menos, alvo de algum processo penal, a utilidade objetiva das imagens captadas pelas autoridades após a detenção de um indivíduo suspeito de cometer um crime é capaz de legitimar a retenção da sua imagem – "necessária numa sociedade democrática" – para fins de combate ao crime (*Suprunenko v. Rússia*, 2018, §§ 63-65). Na verdade, o simples facto de se fotografar um suspeito e incluir a sua imagem numa base de dados não acarreta forçosamente, na interpretação do TEDH, o estigma da culpabilização (ibid., § 64). Justamente por isso, no caso *Murray v. Reino Unido*, 1994 (§§ 92-93), a tomada e manutenção, sem o seu assentimento, da fotografia de uma pessoa suspeita da prática de um crime de terrorismo não foi considerada desproporcionada considerando o objetivo prosseguido: prevenção de atos terroristas.

Diversamente, já entendeu o TEDH, no entanto, constituir uma violação do artigo 8.º da Convenção Europeia dos Direitos do Homem[18] o caso em que a polícia forneceu à imprensa, sem consentimento prévio dos visados, fotografias de indivíduos por ela detidos ou acusados (*Sciacca v. Itália*, 2005, §§ 29-31; *Khoujine v. Rússia*, 2008, §§ 115-118), ou em que convidou equipas de televisão para filmarem um suspeito da prática de um crime na esquadra com a subsequente transmissão das imagens assim obtidas (*Toma v. Roménia*, 2009, §§ 90-93; *Khmel*

[18] "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".

v. Rússia, 2013, § 41), ou ainda no caso em que a exibição da foto de um indivíduo resultou da sua obtenção a partir de uma lista de *most wanted persons* (*Guiorgui Nikolaïchvili v. Geórgia*, 2009, §§ 129-131) elaborada por entidades policiais.

Já, porém, a retenção por tempo ilimitado da fotografia de um indivíduo suspeito de cometer um crime de cuja comissão foi, a final, absolvido, apresentava maior risco de desonra do que a retenção de dados sobre indivíduos que foram condenados por um crime (*S. and Marper v. Reino Unido*, 2008, § 122; *Gaughran v. Reino Unido*, 2020, §§ 82-84).

Especificamente no que toca às técnicas de reconhecimento e mapeamento facial que atualmente se podem aplicar a fotografias contendo retratos de pessoas, por serem cada vez mais complexas, obrigam os tribunais nacionais, no entender do TEDH, a examinar cuidadosamente a necessidade de qualquer interferência sobre o direito à imagem.

Em *Gaughran v. Reino Unido*, 2020 (§§ 97-98), onde as autoridades nacionais decidiram guardar por tempo indeterminado a fotografia de um indivíduo condenado por conduzir com excesso de álcool, além de seu perfil de DNA e das suas impressões digitais, o TEDH entendeu existir uma violação do artigo 8.º. Ao decidir sobre essa retenção de dados pessoais, sem referência à gravidade da infração e na ausência de qualquer possibilidade real de revisão, as autoridades nacionais não conseguiram encontrar, segundo o TEDH, um justo equilíbrio entre o interesse público e o privado.

Num contexto diferente, o Tribunal considerou no caso *Reklos e Davourlis v. Grécia*, 2009 (§§ 41-43), ter havido violação do artigo 8.º a propósito da obtenção, numa clínica, de uma fotografia de um recém-nascido contra a vontade dos pais, de uma forma que permitia a sua identificação e a possibilidade de uso indevido posterior (como efetivamente ocorreu).

De igual modo, considerou-se ter existido violação do artigo 8.º nos casos *Hájovský v. Eslováquia*, 2021 (§§ 46-49), no que respeita à publicação na imprensa de imagens não convenientemente desfocadas do requerente, e *Volodina v. Rússia*, 2021 (§ 68), no que tange à falha das autoridades em proteger uma mulher contra a reiterada *cyber* violência do marido que criou perfis falsos em seu nome e publicou fotos íntimas dela.

Já no caso *Von Hannover v. Alemanha*, 2012 (§§ 114-126), a recusa dos tribunais nacionais em interditar a publicação de uma fotografia de um casal famoso tirada sem o seu conhecimento foi entendida como não constituindo infração do artigo 8.º.

E, em idêntico sentido, no caso *Kahn v. Alemanha*, 2016 (§§ 63-76), o TEDH não encontrou qualquer violação do artigo 8.º no facto de o editor de uma revista não ter sido condenado a pagar qualquer indemnização ao requerente pela infração

de uma proibição de publicação de fotografias de dois filhos de um antigo guarda-redes da seleção alemã de futebol na medida em que outros meios de tutela se encontrassem à sua disposição (*astreintes*, designadamente).

Em processos relativos à tomada pelas autoridades, para fins de prevenção criminal, de impressões digitais, dados biológicos e perfis de DNA de pessoas suspeitas ou condenadas pela prática de crimes, indicou o TEDH que o recurso a modernas tecnologias não pode ser autorizado a qualquer preço (*S. e Marper c. Reino Unido*, 2008, § 112), embora reconhecendo que é de antecipar, tendo em conta o ritmo acelerado dos desenvolvimentos no campo da genética e da tecnologia da informação, a possibilidade de que, no futuro, o direito à vida privada e o direito à informação genética se tornem fortes adversários (ibid., § 71).

Na conceção do TEDH, o desenvolvimento rápido de técnicas cada vez mais inteligentes que tem permitido, entre outras coisas, o desenvolvimento de instrumentos de reconhecimento facial e de mapeamento facial, faz da tomada, armazenamento e divulgação de fotografias um tema muito delicado. Os tribunais nacionais não devem, apesar disso, deixar de levar em conta estas evoluções tecnológicas ao avaliar a necessidade de interferência na vida privada (*Gaughran c. Reino Unido*, 2020, § 70).

Este breve excurso pela recente jurisprudência do TEDH em matéria de direito à imagem, autoriza, de imediato, uma óbvia ilação: nela, a respetiva tutela encontra o seu fundamento na proteção devida à "vida privada e familiar". Tal deve-se certamente à falta de referência autónoma a um direito à imagem no articulado da Convenção Europeia dos Direitos do Homem. Mas, em simultâneo, tal perspetiva permite asseverar que os casos em que a terceiro se autoriza a interferência com o direito à imagem alheia hão de subsumir-se ao n.º 2 do seu artigo 8.º. As alusões que aí se encontram à "segurança nacional", à "segurança pública", à "defesa da ordem" e à "prevenção das infrações penais" podem, no âmbito das FRT, revelar-se particularmente profícuas.

Induz-se ainda, por outro lado, que a jurisprudência do TEDH se dirige por uma linha fortemente protetora do cidadão e dos seus direitos fundamentais. Razão pela qual a ingerência de terceiros – do Estado ou de outros cidadãos – no direito à imagem individual só muito excecionalmente se admite sem assentimento da pessoa afetada.

3. *Inteligência Artificial?*

Antes do mais, a questão posta pela chamada Inteligência Artificial (IA) faz despontar um sério dilema – como tantas vezes sucede com novos problemas – de definição e de demarcação de fronteiras.

Mas, primeiro, pergunta-se: qual a razão que justifica a caracterização da IA como *inteligência*[19]?

Ela parece residir, sobretudo, no facto de a máquina munida de tal aptidão ser capaz de, tal qual os humanos, aprender pelo seu próprio traquejo a lidar com situações para as quais não foi originariamente programada[20]. Isto permite distingui-la dos atuais *robots* que se limitam (somente) a desempenhar funções rotineiras, pré-definidas. A máquina dotada de IA será capaz de, ante uma dificuldade (*dead-end*), aprender, pela experiência anterior (ou seja, em função dos dados anteriormente recolhidos), a superá-la, chegando eventualmente a ultrapassá-la. Por exemplo, a máquina que aparafusa o chassis de um automóvel fá-lo-á enquanto estiver abastecida de parafusos. Assim que, por qualquer razão, o seu abastecimento cessar, ele parará a atividade ou continuará inutilmente a produzir o gesto de aparafusar. A máquina provida de IA, ao invés, recorrendo à sua prática prévia, procurará uma solução que lhe permita eventualmente vencer o obstáculo[21].

---

[19] A transposição da locução "inteligência" (humana) para as "máquinas" não é indisputável. Tratar-se-á, para já, de uma simples afinidade mais ou menos próxima. "The term artificial intelligence can perhaps best be regarded not as derived, by analogy, from the rigorous conceptions of philosophers, psychologists, and linguistic scientists, but as a label used to refer to what it seems that certain computer systems possess to some degree. Such systems, having been so designed and constructed to perform those tasks and solve those problems that together if performed by human beings are taken by us to be indicative of intelligence, can be said to exhibit Artificial Intelligence. On this account, then, the term artificial intelligence connotes a prima facie intelligence and this designation, while perhaps lacking in philosophical rigour, serves simply as an explanatory, and metaphorically framed, classification" (Richard E.Susskind, *Expert systems in Law – a jurisprudential approach to artificial intelligence and legal reasoning*, The Modern Law Review, vol. 49, 1986, pág. 171). "What is AI? There are many ways to answer this question, but one place to begin is to consider the types of problems that AI technology is often used to address. In that spirit, we might describe AI as using technology to automate tasks that «normally require human intelligence»" (Harry Surden, *Artificial Intelligence and Law: An Overview*, Georgia State University Law Review, vol. 35, 2019, pág. 1307). Algum dia – num futuro talvez não muito distante – as máquinas hão de considerar-se "seres". Até lá, apenas por analogia se raciocinará.

[20] O caso *v.g.* do computador da Google denominado *AlphaGo* que, sem nunca ter sido ensinado (programado) para o efeito, foi capaz de vencer diversas partidas do jogo *Go* cujas regras aprendeu, assim como a ganhá-lo, tanto pela observação de outros jogadores como pela prática de milhões de outras partidas.

[21] Isto é o que principalmente caracteriza o algoritmo dito "inteligente" e o separa de qualquer outro. Ao contrário deste, aquele é construído – ao menos em parte – pela própria máquina. "AI is different from conventional computer algorithms. The development of Artificial Intelligence is aimed at making it self-training (the ability to accumulate personal experience) or machine learning. This unique feature enables AI to act differently in the same situations, depending on the actions previously performed. This is very similar to human experience" (Paulius Cerka – Jurgita Grigie – Gintar Sirbikyt, *Liability for damages caused by artificial intelligence*, Computer Law & Security Review, n.º 31, 2015, 378).

A aquisição de conhecimentos através da experiência supõe a repetição de ações e a sua observação. Numa casa dita inteligente, o assistente eletrónico que a administra pode recomendar ao seu dono que, em dada ocasião, não saia de casa sem chapéu de chuva porque verificou que em *X* número de ocasiões anteriores, sempre que choveu, ele somente a abandonou munido desse utensílio. Será assim que, para já, a melhor IA funcionará. Mas, pergunta-se, não é o conhecimento humano igualmente obtido, em grande parte, pela repetição da prática de atos e pela análise dos efeitos deles emergentes?

Machine learning[22] é um ramo da inteligência artificial, que para alguns se confunde com *deep learning* (ou que, pelo menos, constitui um nível anterior a este)[23], embora, para outros, componha um ramo de IA distinto daquele e que se caracteriza por uma menor capacidade da máquina para lidar com problemas novos. Será o subgrupo da inteligência artificial que, para produzir o resultado desejado, envolve algoritmos modificáveis sem intervenção humana, mas sempre supondo que a informação introduzida se encontra categorizada – contendo *v.g.* as características de um cão ou de um gato – de modo que a máquina (em termos binários) proceda à inclusão/exclusão do caso concreto. *V.g.* o algoritmo que identifica e separa o *spam* de entre todo o correio eletrónico recebido.

---

[22] "Aprendizagem automática", no dizer da Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica [2015/2103(INL)]. *OJ C*, 252, 18.7.2018, 239-257.

[23] Assim como a locução "inteligência" suscita dúvidas quando se considera a sua extensão às "máquinas", também o uso da expressão "aprendizagem" ("learning") origina dificuldades similares sempre que se intente expandi-lo às "machines". "It is important to clarify the meaning of the word learning in machine learning. Based upon the name, one might assume that these systems are learning in the way that humans do. But that is not the case. Rather, the word learning is used only as a rough metaphor for human learning. For instance, when humans learn, we often measure progress in a functional sense – whether a person is getting better at a particular task over time through experience. Similarly, we can roughly characterize machine-learning systems as functionally «learning» in the sense that they too can improve their performance on particular tasks over time. They do this by examining more data and looking for additional patterns" (Harry Surden, *Artificial Intelligence and Law: An Overview,* Georgia State University Law Review, vol. 35, 2019, 1311). "«Machine learning» refers to a subfield of computer science concerned with computer programs that are able to learn from experience and thus improve their performance over time. (...) The idea that the computers are «learning» is largely a metaphor and does not imply that computers systems are artificially replicating the advanced cognitive systems thought to be involved in human learning. Rather, we can consider these algorithms to be learning in a *functional* sense: they are capable of changing their behavior to enhance their performance on some tasks through experience" (Harry Surden, *Machine Learning and Law*, Washington Law Review, vol. 89, 2014, 89).

Deep learning é um diferente (superior) ramo da inteligência artificial em que os algoritmos operam de maneira semelhante aos de *machine learning*, mas organizando-se por inúmeras camadas (*multilayer*[24]), cada uma fornecendo uma interpretação diferente dos dados dos quais se alimenta. Essas camadas, numa tentativa de imitar a função das redes neurais humanas (presentes no cérebro), formam uma rede neural artificial[25].

O grande desafio que a inteligência artificial defronta consiste em pô-la a desempenhar tarefas que, sendo de simples execução para o ser humano, são de difícil descrição em termos formais, o que dificulta sobremaneira a transmissão do ensinamento. Como, por exemplo, proceder ao reconhecimento de palavras[26] (especialmente devido à ambiguidade da linguagem natural[27]), sons ou rostos.

---

[24] Por exemplo, para o reconhecimento de imagem, a sequência poderá ser (partindo da base para o topo): *pixel* → *edge* → *texton* → *motif* → *part* → *object*. (Marc'Aurelio Ranzato, *Deep Learning for Object Category Recognition*. AI group).

[25] Uma rede neural artificial – por comparação, de novo, com a rede neural humana – "is like the natural human brain with its biological neurons and synapses, the goal of which is to reproduce the computing power of the human brain. A network of many nodes can exhibit incredibly rich and intelligent behaviors such as ability to learn" (Paulius Cerka – Jurgita Grigie – Gintar Sirbikyt, *Liability for damages caused by artificial intelligence*, Computer Law & Security Review, n.º 31, 2015, 380).

[26] Assim *v.g.* "the symbols A, B, and C can be replaced with sentences without diminishing the deductive capabilities of the system. Suppose, for example, that the following substitutions were to be made:
A = (person is 21 years of age or older);
B = (person is a major);
and C = (person has contractual capacity).
The result would read:
Rule 1, if (person is 21 years of age or older)
then (person is a major).
Rule 2, if (person is a major)
then (person has contractual capacity).
A program that could deduce C when given A in the original example might have little difficulty in deducing «person has contractual capacity» when given that «person is 21 years of age or older». The problem is to make the computer treat expressions like «person is 21 years of age or older» as a unit like A" (Cary Debessonet – George Cross, *An Artificial Intelligence application in the Law: CCLIPS, a computer program that processes legal information*, Berkeley Technology Law Journal, 329, 1986, 332/333).

[27] Daí a dificuldade que todos os algoritmos destinados a traduzir a linguagem humana apresentam. Entoações, sentidos subentendidos, ironias, emoções, etc. só raramente conseguem ser por eles captados. "Tasks involving «common sense» reasoning or perception, such as language understanding, are by far the most difficult for AI. More technical tasks, like solving calculus problems or playing chess, are usually much easier. That is because the latter can be framed in well-defined terms and

Pelo recurso ao *deep learning* (ou *hierarchical learning*), pretende-se que os computadores aprendam a partir do próprio traquejo e compreendam o mundo por intermédio de uma hierarquia de conceitos[28]. Não se tornará então necessário transmitir-lhes todo o conhecimento, dado que eles, em parte, o obterão mediante a sua própria prática. A referida hierarquia de conceitos permitirá ao computador cultivar ideias complexas (mais abstratas), construindo-as a partir de outras mais simples[29].

Como se pode já deduzir a partir do que antecede, a IA apresenta-se, portanto, como uma árvore com muitos ramos.

O que importa sublinhar, contudo, é que as máquinas dotadas de *deep learning* se assemelham, em vários aspetos ligados à racionalidade, ao ser humano. Seja qual for a arquitetura técnica que a engenharia informática adote, faz já parte da realidade, do presente, a existência de máquinas dotadas de *deep learning*. Desde computadores com intervenção em certos modelos de contratação eletrónica até aos veículos automóveis – exemplo, para já, paradigmático – ou navios de condução completamente autónoma[30], passando por sistemas informáticos capazes de atuar como mediadores

---

come from totally black-and-white domains, while the former cannot and do not" (Edwina L. Rissland, *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, The Yale Law Journal, vol. 99, 1990, 1959).

[28] Ver, por exemplo, Cary Debessonet – George Cross, *An Artificial Intelligence application in the Law: CCLIPS, a computer program that processes legal information*, Berkeley Technology Law Journal, 329, 1986, 331.

[29] Cf., a propósito, Yann Lecun – Yoshua Bengio – Geoffrey Hinton, *Deep Learning*, Review. Nature, vol. 521, 2015, 436.

[30] Ver Olivia J. Erdélyi – Judy Goldsmith, *Regulating Artificial Intelligence Proposal for a Global Solution*. 2018 AAAI/ACM Conference on AI, Ethics, and Society (AIES '18), 2018, New Orleans, LA, USA, 1. Com contributos para a problemática da personalidade jurídica de pessoas coletivas e navios *vide* Joshua C. Gellers, *Rights for robots: artificial intelligence, animal and environmental law,* London and NY: Routledge, 2021, 32-36. "The act of anthropomorphizing ships is thus a ritual of identification that crept its way into common-law systems. However, [...], the judges who applied principles that construed seafaring vessels as legal persons did so on the basis of practical expediency, not literal personification derived from religious or cultural beliefs about the ontological status of ships. Ships, therefore, are personified culturally but are determined to possess liability legally. They do not represent the interests of a group, although they have been legalized in ways that shield individuals from responsibility. They are not brought into being purely through state action, although they are recognized as a legal entity for the purposes of engaging in legal relations. Finally, while they are somewhat akin to pre-existing sociological persons, claims of their metaphysical or moral personhood do not form the basis for establishing their legal personhood, which instead relies on a pragmatic approach to resolving legal disputes involving ships. As such, the extension of legal personhood to vessels appears most closely aligned with the unique entity theory of corporate personhood given the fact that ships are neither natural persons nor creations of the state" (35).

em *online dispute resolution*[31] ou como guardas prisionais[32]. E adivinha-se, com alto grau de certeza, que o futuro não muito longínquo há de passar pela ampla utilização destes engenhos[33]. Veja-se *v.g.* a relevância que a seleção e organização elaborada pelas bases de dados de arquivo de jurisprudência vai adquirindo em alguns ordenamentos jurídicos, particularmente, de *Common Law* e os desafios resultantes do domínio da linguagem[34].

Um dos principais desafios da IA reside na transmissão do conhecimento, ou seja, na suscetibilidade e capacidade de vida em relação (pelo menos como a conhecemos entre seres humanos[35]) essencial para o reconhecimento de palavras, sons, rostos[36]. Já em Aristóteles se fazia referência à relevância da dimensão social, da voz e da fala enquanto características do ser humano[37]. Verdadeiramente,

---

[31] Ver, a propósito, Davide Carneiro – Paulo Novais – Francisco Andrade – John Zeleznikow – José Neves, *Online dispute resolution: an artificial intelligence perspective*, Artificial Intelligence Review, 41, 2014, 230.

[32] Cf. Melanie Reid, *Rethinking the Fourth Amendment in the Age of Supercomputers, Artificial Intelligence, and Robots*, West Virginia Law Review, vol. 119, 2017, 865.

[33] Inclusivamente no campo das profissões jurídicas (cf. Edwina L. Rissland, *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, The Yale Law Journal, vol. 99, 1990, 1961 a 1979). Como afirma Harry Surden (*Machine Learning and Law*, Washington Law Review, vol. 89, 2014, 105): "Attorneys combine their judgment, training, reasoning, analysis, intuition, and cognition under the facts to make approximate legal predictions for their clients. To some extent, machine learning algorithms could perform a similar but complementary role, only more formally based upon analyzed data". Daí que, "artificial intelligence can now engage in legal reasoning, because a well-designed program can tell a lawyer, or even a judge, what cases are really closest to the case at hand, and what cases are properly distinguished from it" (Cass R. Sunstein, *Of Artificial Intelligence and Legal Reasoning*, Public Law & Legal Theory Working Papers, n.º 18, University of Chicago, 2001, 5).

[34] Salwa Hoque, *Law and IA technologies: mediating "Islamic" piety and "secular" reasoning in Bangladesh courts*, Chicago/Virtual, Law and Society Association Annual Meeting, 29th May 2021, Presentation in CRN 37 session: "Social and legal perspectives on speech, regulation and privacy". Refere a autora o potencial discriminatório que pode advir da utilização de arquivos digitais nos tribunais do Bangladesh pela incapacidade de tradução exata de expressões complexas que designam diversas realidades, dando como exemplo a dificuldade de tradução da expressão «uthai nawa» উঠায় নওেয়া".

[35] Ainda que de uma forma muito incipiente, e além das novas tecnologias líticas (*v.g.* bifaces, raspadores, etc.), pode falar-se de vestígios conducentes à caracterização de comportamentos sociais já no Acheulense (Paleolítico Inferior)*, vide* Armando Coelho Ferreira da Silva, *et al. Pré-história de Portugal*, Lisboa: Universidade Aberta, 1993, 41-94.

[36] Changyu Deng, *et al., Integrating machine learning with Human knowledge*, IScience, vol. 23, n.º 11, 1-27. Também Edwina L. Rissland, *Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning*, The Yale Law Journal, vol. 99, 1990, 1959.

[37] Maria Helena da Rocha Pereira, *Hélade: antologia da cultura grega,* 7.ª edição, Coimbra, Faculdade de Letras da Universidade de Coimbra, Instituto de estudos clássicos, 1998, *Política*, Aristóteles

não se poderá excluir a dimensão orgânica do ser humano – enquanto ser vivo dotado de uma mente complexa – da dimensão de vida em relação porquanto a transmissão de conhecimento entre mentes (*v.g.* por processos de imitação e de aprendizagem) constitui uma característica identificadora dos primatas antropoides[38]. A aptidão para o desenvolvimento da linguagem nos seres humanos, permanece um fator individualizador[39] que não poderá ignorar o elemento fundamental da relação interindividual e da função simbólica, traduzida na diferenciação de significantes e significados[40]. A própria definição da palavra *imagem* reconduz-nos à formulação latina *imitari*[41] e a uma ponderação sobre a mensagem por ela transmitida na medida em que, para a elaboração do seu significante e significado[42], a dimensão relacional, a criatividade, a imaginação e o pensamento

---

(1253ª): "[...] o homem é um animal sociável [...]. A fala, [...], destina-se a declarar o que é útil e o que é prejudicial, assim como o que é justo e o que é injusto. Essa característica é própria do homem, perante os outros animais; consiste em ser o único que tem o sentimento do bem e do mal, da justiça e da injustiça, e assim por diante" (438).

[38] W.G. Runciman, *O animal social,* trad. Isabel Mafra, Lisboa, Temas e debates, 2001, 11 ss.

[39] W.G. Runciman, *O animal social,* trad. Isabel Mafra, Lisboa, Temas e debates, 2001, 14 ss.

[40] Jean Piaget, *Seis estudos de psicologia*, trad. Nina Constante Pereira, 10.ª edição, Lisboa, Dom Quixote, 1990, 119-133. "[...] o próprio da função simbólica consiste numa diferenciação dos significantes (sinais e símbolos) e dos significados (objetos ou acontecimentos, ambos esquemáticos ou conceptualizados" (pág. 123); "A linguagem é assim uma condição necessária, mas não suficiente, para a construção das operações lógicas. É necessária, pois sem o sistema de expressão simbólica que constitui a linguagem as operações permaneceriam no estado de ações sucessivas, sem nunca se integrarem em sistemas simultâneos ou englobando simultaneamente um conjunto de transformações solidárias. Sem a linguagem, por outro lado, as operações permaneceriam individuais e ignorariam, por conseguinte, essa regulação que resulta da troca interindividual e da cooperação. É no duplo sentido da condensação simbólica e da regulação social que a linguagem é, portanto, indispensável à elaboração do pensamento. Entre a linguagem e o pensamento existe assim um círculo genético, de tal modo que um dos dois termos se apoia necessariamente no outro, numa formação solidária e numa perpétua ação recíproca. Mas ambos dependem, no fim de contas, da própria inteligência, que, essa sim, é anterior à linguagem e independente dela" (133).

[41] António Gomes Ferreira, *Dicionário de Latim-Português,* Porto, Porto Editora, 1997. *Imitari*: "[...] 1. Imitar, reproduzir por imitação, copiar, 2. Simular, fingir, afetar. 3. [...] apresentar, exprimir, representar.", 566.

[42] Roland Barthes, *The rhetoric of the image*, in Ann Gray – Jim McGhigan, ed., *Studying culture: an introductory reader,* 2nd ed., London, Arnold, 1997. Sobre a mensagem linguística, a mensagem icónica codificada e não codificada transmitidas pela imagem, *vide* págs. 15-27. "It is certain that the distinction between the two iconic messages is not made spontaneously in ordinary reading: the viewer of the image receives *at one and the same time* the perceptual message and the cultural message [...]. The distinction, however, has an operational validity, analogous to that which allows the distinction in the linguistic sign of a signifier and a signified (even though in reality no one is

crítico desempenham papéis preponderantes[43]. Pense-se, a propósito, *v.g.* na complexidade que a questão da linguagem põe para a IA (justamente na compreensão do significante e do significado) no caso de um algoritmo que removeu vídeos de lutas entre *robots* por considerar que correspondiam a demonstrações de crueldade contra animais[44].

A complexidade da temática dos direitos dos não-humanos conduz a ponderações, também, no domínio digital, problematizando-se *v.g.* a fundamentação da personalidade jurídica da IA[45] na tentativa de alcançar uma proposta para a miríade de questões suscitadas neste âmbito[46].

---

able to separate the 'word' from its meaning except by recourse to the metalanguage of a definition)" (18).

[43] Roland Barthes, *The rhetoric of the image*, in Ann Gray – Jim McGhigan, ed., *Studying culture: an introductory reader,* 2nd ed., London, Arnold, 1997. Changyu Deng *et al., Integrating machine learning with Human knowledge*, IScience, vol. 23, n.º 11, 2020, 1-27. "Machine learning has been heavily researched and widely used in many areas from object detection (Zou et al., 2019) and speech recognition (Graves et al., 2013) to protein structure prediction (Senior et al., 2020) and engineering design optimization (Deng *et al.*, 2020; Gao and Lu, 2020; Wu *et al.,* 2018).

[44] A. Cuthbertson, *YouTube Is Deleting Videos of Robots Fighting Because of "Animal Cruelty",* The Independent (20/08/2019).
Também Joshua C. Gellers, *Rights for robots: artificial intelligence, animal and environmental law,* London and NY: Routledge, 2021. "[...], in 2019, YouTube's algorithm began removing robot combat videos on the grounds that they ran afoul of community standards prohibiting depictions of animal cruelty (Cuthbertson, 2019). Although the robots featured in these videos did not look much like quadrupedal domesticated animals, the controversy highlighted concerns about how humans identify and treat nonhumans, even those of the zoomorphic mechanical kind" (160). Mas sobre as possibilidades da comunicação entre máquinas, *vide* Aline F.S. Borges *et. al., The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions*, International Journal of Information Management, vol. 57, 2021.

[45] Propondo mapas metodológicos e de enquadramento da problemática da personalidade jurídica, inteligência artificial, animais e meio ambiente *vide* Joshua C. Gellers, *Rights for robots: artificial intelligence, animal and environmental law,* London and NY, Routledge, 2021.

[46] *Vide* n.º 70-71 da Proposta de Resolução do Parlamento Europeu que contém recomendações à Comissão sobre o enquadramento posto pelos aspetos éticos à inteligência artificial, à robótica e às tecnologias conexas [2020/2012(INL)]: "[...] [70.] convicto de que o progresso tecnológico não deve conduzir à utilização da inteligência artificial, da robótica e das tecnologias conexas para tomar autonomamente decisões do setor público que tenham um impacto direto e significativo nos direitos e obrigações dos cidadãos; [...]"; e que "[...] a IA jamais deverá substituir os seres humanos na emissão de decisões judiciais; considera que decisões como a de colocar em liberdade sob caução ou liberdade condicional, que são tomadas em tribunal, ou as decisões baseadas unicamente no tratamento automatizado que produzam efeitos jurídicos relativamente a pessoas ou que as afetem de forma significativa devem implicar sempre uma avaliação profunda e uma decisão por um ser humano; [...]". Atendendo aos incontáveis e multidisciplinares desafios colocados

Por outro lado, a concessão *v.g.* de direitos humanos e personalidade jurídica à montanha Taranaki, pela Nova Zelândia, fundamentando-se na relação entre os povos indígenas e a montanha (considerada como antepassado e família), traduz-se na tutela do património natural e cultural, promovendo a sustentabilidade e a biodiversidade, dimensões que integram e fundamentam, *de per se*, a dignidade humana, viabilizando-a[47]. O que demonstra que também a IA pode ser usada como instrumento de preservação e proteção do ambiente, da sustentabilidade e da neutralidade climática, procurando minimizar e reparar eventuais danos causados a tais bens[48].

Mesmo a apregoada aproximação entre certos animais não humanos e animais humanos assente na natureza senciente de ambos parece não ser única. Com efeito, há já notícias – entretanto desmentidas, mas de forma que mais avoluma a suspeita – de que um dos chamados *chatbots* (programa de computador que simula uma conversa com um ser humano) da Google se terá igualmente tornado senciente, "ou seja, dotado da capacidade de expressar sentimentos e pensamentos"[49].

4. O perigo de enviesamento (*algorithtmic bias*) no campo do reconhecimento facial

O recurso à Inteligência Artificial apresenta óbvios benefícios. Mas os riscos e perigos envolvidos no seu uso são enormes[50]. O que é particularmente sensível

---

pela IA, talvez nos situemos, atualmente, no que sugerimos designar de Paleolítico Inferior da Era Digital, considerando, por comparação, os desenvolvimentos da história humana durante o Paleolítico Inferior (*vide* Armando Coelho Ferreira da Silva, *et al. Pré-história de Portugal,* Lisboa, Universidade Aberta, 1993, 41-94). Salientando, os desafios éticos, atuais e futuros, colocados pela utilização da IA, *vide* Vincent C. Müller, *Ethics of Artificial Intelligence and Robotics*, in Edward N. Zalta (ed.) – *The Stanford Encyclopedia of Philosophy (Summer 2021 Edition)*, forthcoming, 2020/2021.

[47] Boaventura Sousa Santos, *Direitos Humanos, democracia e desenvolvimento*, in Martins, Bruno Sena – Boaventura Sousa Santos, coord., *O pluriverso dos direitos humanos: a diversidade das lutas pela dignidade*, Lisboa, Edições 70, 2019, 41-66 e 59-60, nota 15. Também Eleanor Ainge Roy, *New Zealand gives Mount Taranaki same legal rights as a person*, *The Guardian* (22/12/2017).

[48] N.º 51-62 da Proposta de Resolução do Parlamento Europeu que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

[49] Jornal digital "Observador" de dia 13/0672022, *https://observador.pt/2022/06/13/google-suspende-engenheiro-que-afirmou-que-inteligencia-artificial-da-empresa-ganhou-vida/*.

[50] Como, por exemplo, salientam Ninareh Mehrabi – Fred Morstatter – Nripsuta Saxena – Kristina Lerman – Aram Galstyan (*A Survey on Bias and Fairness in Machine Learning*, 2019, 1): "There

nos casos em que ela se usa para reconhecimento facial (FRT – *Facial Recognition Technology*)[51/52].

Para proceder ao reconhecimento facial, é necessário, primeiro, que o computador aprenda o que é um rosto. Isto, em geral, obtém-se "treinando" um algoritmo – normalmente uma rede neural profunda – através do fornecimento de um grande número de fotografias (retratos) contendo rostos de diferentes pessoas em situações típicas. Cada vez que uma imagem é apresentada ao algoritmo, ele estima a localização do rosto. De início, faltará "pontaria". Mas, com a repetição, o algoritmo melhorará a sua fineza (acerto) e acabará por dominar a arte de *detetar* uma face humana.

Surge, em seguida, a parte do *reconhecimento* propriamente dito. Pode operar de diversas maneiras, mas é comum usar uma segunda rede neural à qual se fornece uma multiplicidade de retratos. Ante eles, os algoritmos mapearão cada rosto, *v.g.* medindo as distâncias entre os olhos, nariz e boca e assim por diante. A rede gera

---

are clear benefits to algorithmic decision-making; unlike people, machines do not become tired or bored, and can take into account orders of magnitude more factors than people can. However, like people, algorithms are vulnerable to biases that render their decisions «unfair». In the context of decision-making, fairness is the absence of any prejudice or favoritism toward an individual or a group based on their inherent or acquired characteristics. Thus, an unfair algorithm is one whose decisions are skewed toward a particular group of people".

[51] O reconhecimento facial é uma modalidade avançada de reconhecimento biométrico. Como, por exemplo, referem Marcus Smith – Seumas Miller (*The ethical application of biometric facial recognition technology*, AI & Society, 2022, vol. 37, 167/168): "Biometric facial recognition is a form of AI that involves the automated extraction, digitisation and comparison of the spatial and geometric distribution of facial features to identify individuals. Using a digital photograph of a subject's face, a contour map of the position of facial features is converted into a digital template, using an algorithm to compare an image of a face with one stored in a database".

[52] Segundo o European Data Protection Board (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted on 12 May 2022, n.os 1 e 2) "Facial recognition technology (FRT) may be used to automatically recognise individuals based on his/her face. FRT often is based on artificial intelligence such as machine learning technologies.

A great deal of the increased interest in FRT is based on the efficiency and scalability of FRT. With these come the disadvantages inherent to the technology and its application – also on a large scale. While there may be thousands of personal data sets analysed at the push of a button, already slight effects of algorithmic discrimination or misidentification may create high numbers of individuals affected severely in their conduct and daily lives. The sheer size of processing of personal data, and in particular biometric data, possible is a further key element of FRT, as the processing of personal data constitutes an interference with the fundamental right to protection of personal data according to Article 8 of the Charter of Fundamental Rights of the European Union (the Charter)".

um vetor para cada rosto – uma sequência de números que o identifica de forma única entre todos as demais[53].

O desempenho ótimo depende de condições ideais: uma foto nítida e clara integrada num banco de dados que integra muitíssimas outras fotografias (*big data*) de alta qualidade. Mesmo nesse contexto, porém, a tecnologia apresenta, para já, grandes dificuldades em lidar, por exemplo, com gémeos ou com pessoas com rostos de geometria aproximada, confundindo-os.

Juridicamente, o recurso às FRT apresenta perigos com os quais não será fácil lidar. A possibilidade de o reconhecimento facial ser utilizado (deliberadamente ou

---

[53] Assim, por exemplo:

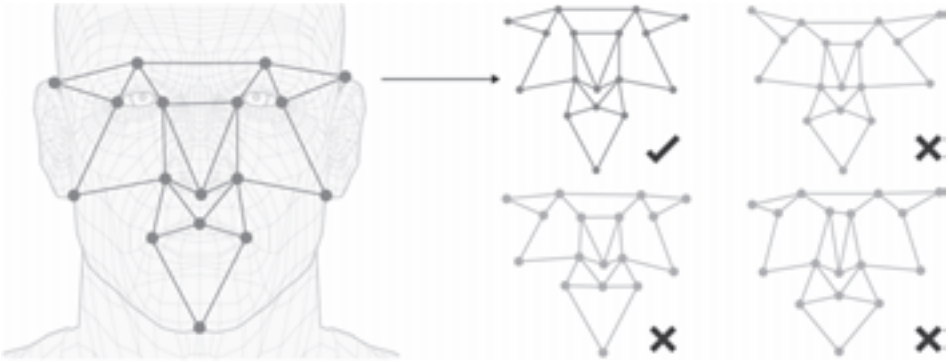

Figura obtida em *https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it*.

Ainda de acordo com o European Data Protection Board (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted on 12 May 2022), "FRT falls into the broader category of biometric technology. Biometrics include all automated processes used to recognise an individual by quantifying physical, physiological or behavioural characteristics (fingerprints, iris structure, voice, gait, blood vessel patterns, etc.). These characteristics are defined as "biometric data", because they allow or confirm the unique identification of that person.

This is the case with people's faces or, more specifically, their technical processing using facial recognition devices: by taking the image of a face (a photograph or video) – called a biometric «sample» it is possible to extract a digital representation of distinct characteristics of this face (this is called a «template»).

A biometric template is a digital representation of the unique features that have been extracted from a biometric sample and can be stored in a biometric database. This template is supposed to be unique and specific to each person and it is, in principle, permanent over time. In the recognition phase, the device compares this template with other templates previously produced or calculated directly from biometric samples such as faces found on an image, photo or video. «Facial recognition» is therefore a two-step process: the collection of the facial image and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates".

não) de forma capaz de afetar a imagem, a intimidade privada ou a igualdade, é um problema de apreciável dimensão. Quer ele se destine (meramente) à autenticação (*one-to-one comparison*[54]) ou se dirija à identificação de pessoas (*one-to-many comparison*[55])[56], trata-se de hipótese não despicienda, nem extraordinária, nem nova[57]. Basta que as redes neurais tenham sido preparadas (alimentadas) sobre desiguais qualidades e quantidades de dados[58]: por exemplo, diferente número de faces de diversos grupos sociais. Se *v.g.* um sistema for treinado sobre milhões de rostos masculinos brancos e apenas milhares de rostos de mulheres[59] ou de pessoas de outras raças, ele será evidentemente menos preciso em relação a estes dois últimos grupos[60]. E menor precisão significa, claro, maior possibilidade de erro na identificação. A isto se chama *enviesamento algorítmico* – ou seja, enviesamento inerente ao conjunto de dados subjacentes[61] – ou

[54] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 7: "It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown on the two images is the same person".

[55] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 7: "Identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his or her image is stored there. The facial recognition technology returns a score for each comparison indicating the likelihood that two images refer to the same person".

[56] Ainda que, evidentemente, a ameaça seja maior quando se use para a segunda finalidade (cf. European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 8).

[57] Neste sentido, David Leslie, *Understanding bias in facial recognition technologies: an explainer*, The Alan Turing Institute, 2020, 13, *https://zenodo.org/record/4050457#.Yp9LixrMK3A*.

[58] Cf. Tom C.W. Lin, *Artificial Intelligence, Finance, and the Law*, Fordham Law Review, vol. 88, 2019, 536.

[59] Como, por exemplo, refere Susan Leavy (*Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning*, GE'18, May 28, 2018, Gothenburg, Sweden): "the over-representation of men in the design of these technologies could quietly undo decades of advances in gender equality. (...) Gender balance in machine learning is therefore crucial to prevent algorithms from perpetuating gender ideologies that disadvantage women".

[60] Cf. *v.g. Ewert v. Canada* (2018 SCC 30): *Ewert* cumpria pena de prisão perpétua. Pertencia aos *Métis*, um dos povos aborígenes do Canadá. O Correctional Service of Canada – instituição responsável pela administração das prisões –, usava, na altura, ferramentas de IA para avaliar o risco de reincidência e a saúde mental dos presidiários. *Ewert* argumentou, ante o Supreme Court of Canada, que o referido Correctional Service confiava em "instrumentos desenvolvidos e testados em populações predominantemente não indígenas e que não houve pesquisas confirmando que eles eram igualmente válidos quando aplicados a indígenas". O Supreme Court aceitou a alegação, reconhecendo a discriminação negativa ilegítima.

[61] N.º 27 da Proposta de Resolução do Parlamento Europeu que contém recomendações à Comissão sobre o quadro dos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

algorithmic bias[62]. Para mitigar, tanto quanto possível, estas (maiores ou menores) inexatidões e as possíveis discriminações delas emergentes[63], estabelece a Carta Portuguesa de Direitos Humanos na Era Digital que "as decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei" (artigo 9.º, n.º 2, Lei n.º 27/2021, de 17/05). Resta saber, claro, o que cabe entender por "decisões com impacto significativo"!

Se o reconhecimento facial estiver *v.g.* a ser usado num aeroporto, para monitorização de passageiros clandestinos ou de suspeitos da prática de crimes, a imprecisão do sistema de reconhecimento facial aí implantado pode, com facilidade, gerar situações de (profundo) tratamento desigual fundadas em certas características raciais[64]. No acesso a algo tão simples como um telemóvel que se obtenha também mediante reconhecimento facial, a errada identificação, pode, também por exemplo, autorizar o acesso de estranhos às informações pessoais nele contidas ou constituir uma fonte de discriminações em razão do sexo ou da raça. "Facebook's facial recognition uses a machine learning algorithm to automatically identify and tag friends when uploading a photo"[65], o que permite facilmente gerar, em caso de errada identificação facial, ingerências ou associações não desejadas. Confira-se

---

[62] Quanto às diversas formas que este enviesamento pode assumer, cf. *v.g.* Ninareh Mehrabi – Fred Morstatter – Nripsuta Saxena – Kristina Lerman – Aram Galstyan, *A Survey on Bias and Fairness in Machine Learning*, 2019, 4 a 7.

[63] Com efeito, tal como se diz em Susan Leavy – Barry O'Sullivan – Eugenia Siapera (*Data, Power and Bias in Artificial Intelligence*, 2020, 1), "artificial Intelligence has the potential to exacerbate societal bias and set back decades of advances in equal rights and civil liberty. Data used to train machine learning algorithms may capture social injustices, inequality or discriminatory attitudes that may be learned and perpetuated in society".

[64] Joseph J. Avery, *An uneasy dance with data: racial bias in Criminal Law*, Southern California Law Review Postscript, vol. 93:PS28, 2020, 30/31: "The use of predictive analytics in the law can be bifurcated into two subsets. One involves policing, where what is being predicted is who will commit future crimes. Embedded in this prediction is the question of where those crimes will occur. In theory, these predictions can be used by police departments to allocate resources more efficiently and to make communities safer. (...) The second subset primarily involves recidivism. Here, we have bail decisions in which predictions about who will show up to future court dates are made. Embedded in these predictions is the question of who, if released pretrial, will cause harm (or commit additional crimes). This subset also includes sentencing, such that judges may receive predictions regarding a defendant's likelihood of recidivating". Se estes prognósticos assentarem também em reconhecimento facial, alarga-se a possibilidade de replicar e multiplicar preconceitos ou pré-julgamentos.

[65] Adrienne Yapo – Joseph Weiss, *Ethical Implications Of Bias In Machine Learning*, in Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, 5366.

ainda o exemplo, segundo relatos ocidentais[66], do reconhecimento facial extraordinariamente intrusivo a que, em Xinjiang, se diz se encontra submetida a minoria Uighur muçulmana. Ou, por fim, o caso sucedido em 2015 quando a aplicação *Google Photos* etiquetou dois rostos de pessoas de raça negra como "gorilas"[67].

Os perigos de intromissão desnecessária e desproporcionada em «direitos, liberdades e garantias» / «direitos de personalidade» oferecidos pelo enviesamento são, portanto, imensos[68/69]. Quando certo é que "a utilização da inteligência artificial deve ser orientada pelo respeito dos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência e da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação" (artigo 9.º, n.º 1, Lei n.º 27/2021, de 17/05 – Carta Portuguesa de Direitos Humanos na Era Digital).

5. Licitude das FRT

Embora tenha vindo para ficar (especialmente por razões ligadas à prevenção criminal), o reconhecimento facial executado por algoritmos apresenta, antecipa-se, três fortes perigos (para além dos que, em geral, respeitam a qualquer fenómeno de processamento de dados[70] e dos que, em especial, se ligam aos sistemas de identificação biométrica[71]).

---

[66] *V.g.* "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.*

[67] "Google apologises for Photos app's racist blunder", *https://www.bbc.com/news/technology-33347866.*

[68] Adrienne Yapo – Joseph Weiss, *Ethical Implications Of Bias In Machine Learning*, in Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, 5365: "The accelerated advances in AI, especially related to machine learning algorithms, are having far-reaching and profound consequences on our lives. Ethical considerations for consumers, society, public policy, laws, and regulation are beginning to form".

[69] Assim, por exemplo, "half of American adults are currently in a law enforcement facial recognition network. As the use of body-worn camera («BWC») technology by law enforcement increases, the demand for facial recognition technology likewise accelerates. (...) Anyone passing a police officer equipped with this technology may be scanned, identified, and cataloged in a facial-recognition database without being suspected of any crime or even communicating with the officer" (Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, Virginia Law Review, vol. 105, 2019, 57/58). Cf., entre nós, o disposto nos artigos 9.º e 10.º da Lei n.º 95/2021, de 29 de dezembro.

[70] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted on 12 May 2022, 7-8: "(...) the facial recognition techniques used are based on an estimated match between templates: the one being compared and the baseline(s).

O primeiro, relaciona-se com a indispensável implementação da base de dados à qual o algoritmo há de acudir para proceder a comparações (e para, na sequência, obter um eventual *match*)[72]. Pode assumir-se que toda a fotografia colocada na *internet* é suscetível de apropriação por quem controla aquele algoritmo? Mesmo aquela que lá se encontre arquivada contra a vontade da pessoa retratada? Mesmo quando ela tenha sido colocada para efeito completamente distinto[73]? "Uma vez na *net*, para sempre na *net*"? Seja para que destino for? A resposta a estas questões há de forçosamente ser negativa quando se considerem os moldes em que o direito à imagem se encontra reconhecido pelo preceito contido no artigo 79.º do Código Civil, bem como atendendo à natureza de Direito, Liberdade e Garantia pessoal que a Constituição lhe reconhece (artigo 26.º, n.º 1)[74].

O segundo – que desponta em relação a qualquer base de dados, mas que aqui adquire especial acuidade tendo em conta o modo geralmente descontrolado como ela surge, se constitui e se compõe – concerne ao seu destino: na essência, *(i)* quem tem legitimidade para aceder e *(ii)* que uso lhe está permitido dar? Em especial quando se reconheça a existência de um *right to publicity*, justificar a

---

From this point of view, they are probabilistic: from the comparison, it is deduced a higher or lower probability that the person is indeed the person to be authenticated or identified; if this probability exceeds a certain threshold in the system, defined by the user or the developer of the system, the system will assume that there is a match. While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data".

[71] Artigo 3.º, n.º 36, *Proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União* [2021/0106 (COD) – 21/04/2021: «Sistema de identificação biométrica à distância» é o "sistema de IA concebido para identificar pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que o utilizador do sistema de IA saiba antecipadamente se a pessoa em causa estará presente e pode ser identificada".

[72] Como diz Elizabeth A. Rowe (*Regulating Facial Recognition Technology in the Private Sector*, Stanford Technology Law Review, n.º 24, 2020, 25): "One of the biggest areas of concern for consumers relates to the collection of the photos and biometric data used to create the various databases and algorithms used with facial recognition technology. Many worry that without privacy regulations, companies are free to collect photos and create large databases that can be shared with other companies".

[73] Cf. acórdão do Supremo Tribunal de Justiça de 07/06/2011, Proc. n.º 1581/07.3TVLSB.L1.S1.

[74] Não admira, por isso, com base em semelhante fundamentação, que o *Information Commissioner's Office* (organismo público que, na Grã-Bretanha, tutela, no interesse público, os direitos de e à informação), tenha multado "a facial recognition database company Clearview AI Inc" em "£7.5m and orders UK data to be deleted" [*https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/*].

utilização de imagens alheias sem o devido consentimento do seu titular não só infringirá um direito de personalidade, como transgredirá também um monopólio de exploração económica de que ele juridicamente goza[75].

O terceiro, atinente ao defeituoso ou imperfeito funcionamento do sistema. Em suma, o relativo à sua fiabilidade. Uma errada identificação (seja um falso positivo, seja um falso negativo, embora a ameaça apresente uma óbvia maior dimensão na primeira hipótese) pode contender profundamente com direitos fundamentais e com princípios jurídicos elementares. O *risco* de a base de dados não se encontrar devidamente construída – por *v.g.* não ser suficientemente representativa da realidade que intenta espelhar – deve correr por conta de quem[76]?

Do ponto de vista legal e jurisprudencial, a questão não parece poder ser ultrapassada, para já, a não ser casuisticamente, através, por exemplo, do recurso ao "three data protection «tests»" extraíveis a partir do n.º 2 do artigo 8.º da Convenção Europeia dos Direitos do Homem (ao enumerar as condições de que depende a legítima ingerência no gozo de um direito protegido através dele)[77]: *(i) the purpose test; (ii) the necessity test; (iii) the balancing test*[78]. Ou, entre nós, mediante o manuseio

---

[75] O que se apresenta como argumento não desprezível quando se tome em consideração que a coisificação da imagem proporcionada pelo *right to publicity* – tendo em vista reservar para o seu titular eventuais benefícios económicos que ela seja suscetível de lhe proporcionar – colide com o aproveitamento que terceiros dela queiram tirar sempre que a usem, com intuito lucrativo, para efeitos de reconhecimento facial.

[76] Não parece apresentar novidade jurídica o recurso a qualquer base de dados cuja construção, disponibilização ou utilização assente em alguma forma de conduta dolosa ou descuidada. Daí despontará a aplicação das regras (normais) de responsabilidade civil e/ou penal. O perigo especificamente posto pelo emprego de uma base de dados indevidamente erigida conexiona-se com a respetiva necessidade social: considerando-se útil que, para certo efeito, dela alguém se socorra, há um risco de enviesamento que cabe distribuir. Por quem? Pelo utente? Pelo beneficiário (se for pessoa diferente daquela)? Pela sociedade em geral? E, em qualquer caso, associando-lhe a obrigação de indemnizar (objetivamente) por eventuais danos?

[77] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted on 12 May 2022, 11 a 17.

[78] *V.g.* TEDH, *Uzun v. Germany,* 2010: "The applicant, suspected of involvement in bomb attacks by a left-wing extremist movement, complained in particular that his surveillance via GPS and the use of the data obtained thereby in the criminal proceedings against him had violated his right to respect for private life. The Court held that there had been no violation of Article 8 of the Convention. The GPS surveillance and the processing and use of the data thereby obtained had admittedly interfered with the applicant's right to respect for his private life. However, the Court noted, it had pursued the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime. It had also been proportionate GPS surveillance had been ordered only after less intrusive methods of investigation had proved insufficient, had been carried out for a relatively short period (some three months), and had affected the applicant only when he was

dos princípios orientadores contidos nos n.os 2 e 3 do artigo 18.º da Constituição[79]. Com especial ênfase, na necessidade, na proporcionalidade e na adequação da restrição (ao direito à imagem, no caso). No futuro, o rigor requererá, no entanto, maior concretização. Os tremendos perigos envolvidos exigem-na.

No quadro da exceção à necessidade de consentimento do titular para a captação e difusão da sua imagem fundada em "exigências de polícia ou de justiça" (artigo 79.º, n.º 2, Código Civil), e no que especificamente respeita à "utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som", existe já a Lei n.º 95/2021, de 29 de dezembro. Ainda que, no essencial, ela remeta para a aplicação dos referidos princípios (artigo 4.º) e se estabeleça no n.º 1 do artigo 16.º que "o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados", logo se acrescenta que "não é permitida a captação e tratamento de dados biométricos"[80]. Assim, ao menos do ponto de vista legal, a captação de imagem não pode destinar-se ao reconhecimento facial.

Em geral, a constituição de uma base de dados supõe que os seus titulares os cedam à entidade que os gere, para um certo efeito. A construção de uma base de fotos destinada às FRT não pode, pela sua própria natureza, dar-se do mesmo modo. Se por outra razão não for, em virtude de tal se mostrar verdadeiramente impraticável ou inexequível. Resta assim pretender que a lei, quando decidir intervir, o faça para fixar em termos precisos e rigorosos os fins a que as FRT se podem destinar.

A *Proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União* [2021/0106 (COD) – 21/04/2021] proíbe explicitamente "a utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem

---

travelling in his accomplice's car. The applicant could not therefore be said to have been subjected to total and comprehensive surveillance. Given that the investigation had concerned very serious crimes, the applicant's surveillance by GPS had thus been necessary in a democratic society".

[79] Cf. acórdão do Tribunal Constitucional n.º 81/2007, de 06/02/2007, Proc. n.º 871/2005.

[80] Artigo 3.º, n.º 35, *Proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União* [2021/0106 (COD) – 21/04/2021]: "Um sistema de IA concebido para identificar pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que o utilizador do sistema de IA saiba antecipadamente se a pessoa em causa estará presente e pode ser identificada".

pública". Salvo se "essa utilização for estritamente necessária para alcançar um dos seguintes objetivos: i) a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas, ii) a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista, iii) a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho" [artigo 5.º, n.º 1, alínea d)]. Distingue ainda entre sistemas de inteligência artificial de risco elevado, de risco de limitado e de risco mínimo. Em relação aos primeiros, entre outros, destaca-se a imposição aos seus operadores dos seguintes deveres: *(i)* criação de um sistema de gestão de risco (artigo 9.º); *(ii)* conceção da capacidade para o registo automático de eventos (artigo 12.º); *(iii)* transparência e prestação de informações aos utilizadores (artigo 13.º); *(iv)* supervisão humana (artigo 14.º); *(v)* informação sobre o funcionamento do sistema às pessoas "a ele expostas" (artigo 52.º, n.º 2). Também entre outros, consideram-se sistemas de inteligência artificial de risco elevado os que, designadamente, se destinem à "identificação biométrica e categorização de pessoas singulares", possibilitando-a "à distância «em tempo real» e «em diferido»" [Anexo III da referida Proposta, 1, a)].

6. Conclusões

Não se afigura exequível pretender que a composição da base de dados que o recurso às FRT pressupõe deva assentar na permissão dos titulares dos direitos à imagem afetados. Exigir o contrário significará inviabilizar o seu emprego. Pelo que, portanto, o primeiro dilema a pôr-se ao legislador será fruto desta constatação elementar: conceder prevalência ao direito à imagem com a consequente necessidade de obtenção de consentimento do seu titular para a respetiva captação, acarreta tornar impraticável o recurso às tecnologias de reconhecimento facial.

Por outro lado, admitindo-se existir interesse, proveito e conveniência no emprego das FRT, torna-se indispensável, de seguida, fixar-lhe estritos limites para prevenir abusos. Mediante, pelo menos, a demarcação dos fins para os quais elas se hão de encontrar autorizadas. Para tanto, a enumeração a que procede o n.º 2 do seu artigo 8.º da Convenção Europeia dos Direitos do Homem mostra-se particularmente profícua.

Fechar, de todo, a porta à utilização das FRT não é solução.