UNIVERSIDADE D
COIMBRA

Sandra Raquel Amaral da Silva

RECONHECIMENTO FACIAL
UMA REFLEXÃO À EVENTUAL ADMISSIBILIDADE NO PROCESSO PENAL

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pelo Professor Doutor Nuno Fernando Rocha Almeida Brandão e apresentada à Faculdade de Direito da Universidade de Coimbra.

Janeiro de 2023

Sandra Raquel Amaral da Silva

RECONHECIMENTO FACIAL, UMA REFLEXÃO À EVENTUAL ADMISSIBILIDADE NO PROCESSO PENAL

FACIAL RECOGNITION, A REFLECTION ON ITS POSSIBLE ADMISSIBILITY IN CRIMINAL PROCEDURE

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Especialização em Ciências Jurídico-Forenses, orientada pelo Professor Doutor Nuno Fernando Rocha Almeida Brandão.

Coimbra, 2023

AGRADECIMENTOS

Primeiramente, tenho de agradecer ao Exmo. Senhor Doutor Nuno Fernando Rocha Almeida Brandão pela sua simpatia e disponibilidade para orientar a elaboração da presente dissertação.

Agradeço aos meus pais, irmão e à Laura, por me terem proporcionado as possibilidades de aqui chegar, por me acompanharem ao longo destes anos, por sempre acreditarem em mim, reconfortarem e, sobretudo, pelo incentivo que me deram, sem a ajuda deles não seria possível concluir esta etapa.

Não posso, ainda, deixar de mencionar todos os familiares e amigos que estiveram ao meu lado durante este meu longo percurso.

Por fim, gostaria de agradecer à Ilustre Advogada, Exma. Senhora Dr.ª Márcia Lemos, minha Patrona e, ainda, à Ilustre Advogada, Exma. Senhora Dr.ª Neide Rodrigues Vaz, por terem estado ao meu lado ao longo da elaboração desta dissertação, sempre com uma palavra de incentivo, tendo-me dado forças para completar esta jornada.

Com esta dissertação dou por terminado um percurso longo, difícil, mas, acima de tudo enriquecedor e recompensador, deixo, portanto, um agradecimento a todas as pessoas que me apoiaram e ajudaram a aqui chegar.

RESUMO

A sociedade atual está marcada por um progresso tecnológico significativo, nomeadamente no que diz respeito à Inteligência Artificial, em específico, o reconhecimento facial. Se por um lado, pontos negativos se apontam ao reconhecimento facial, tendo em conta, principalmente, a sua falta de precisão. Por outro lado, surgem associadas ao reconhecimento facial largas vantagens, principalmente, no que toca a uma mais valia na sua utilização no sistema jurídico português, em específico no direito processual penal.

A possibilidade do reconhecimento facial ter um papel importante no reconhecimento dos cidadãos é, com certeza atrativo para o processo penal, de forma a auxiliar decisivamente na realização da justiça e na descoberta da verdade material, principalmente quando se fala no uso deste como prova.

Contudo, a inexistência de qualquer regulamentação sobre o seu uso pelo direito processual penal leva a que não sejam admitidas como meio probatório, uma vez que o uso de tecnologias de reconhecimento facial está em contante contacto com direitos fundamentais. Tem-se por fundamental, atualmente, perceber se o uso destas não restringe de forma inadmissível os direitos fundamentais, como o direito à reserva da intimidade da vida privada, o direito à imagem, a proibição de tratamento informático de dados referentes à vida privada, entre outros.

A verdade é que, existe uma ingerência muito grande nos direitos fundamentais elencados, que associado ao leque de desvantagens existente leva a que não se possa admitir o uso das tecnologias de reconhecimento facial no âmbito da prova em processo penal.

PALAVRAS-CHAVE: Reconhecimento facial, Admissibilidade da Prova, Proibições de Prova, Direitos Fundamentais, Restrição de Direitos Fundamentais, Direito à Reserva da Intimidade da Vida Privada, Direito à Imagem

ABSTRACT

Technological progress is leaving its mark on today's society, especially when considering Artificial Intelligence and facial recognition. While we highlight the lack of precision as one of the negative aspects of facial recognition, many of its advantages also come into play, especially regarding how much it can add to the Portuguese legal system, particularly to de Criminal Procedure Law.

The possibility of facial recognition playing a crucial role in identifying citizens is attractive for criminal proceedings, as it can decisively aid in carrying out justice and discovering the material truth, especially when considering its use as evidence.

However, the lack of regulations on its use under the Criminal Procedure Law dictates it not to be admissible as means of evidence since the use of technologies that facilitate facial recognition often borders with fundamental rights. At this time, it is crucial to understand whether the use of these technologies does not inadmissibly restrict fundamental rights, such as the right to privacy, the right to personal portrayal, the prohibition of computer processing of personal data, and others.

The bottom line is that many of the fundamental rights abovementioned are substantially interfered with. Furthermore, combined with a vast range of existing downsides, facial recognition technologies cannot be admitted as evidence in criminal proceedings.

KEY WORDS: Facial Recognition, Admissibility of Evidence, Prohibitions of Evidence, Fundamental Rights, Limitations of Fundamental Rights, Right to Privacy, Right to Personal Portrayal

SIGLAS E ABREVIATURAS

Ac. – Acórdão

Art./Arts. – Artigo/Artigos

CC – Código Civil

Cfr. – Conforme

Coor – Coordenação

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

CEDH – Convenção Europeia dos Direitos do Homem

DIR - Dirigido

DUDH – Declaração Universal dos Direitos Humanos

IA – Inteligência Artificial

LPDP – Lei da Proteção de Dados Pessoais

N.º - Número

Ob. cit. – Obra citada

P./PP. – Página/Páginas

PIDCP – Pacto Internacional sobre os Direitos Civis e Políticos

PROC. - Processo

SS. – Seguintes

STJ – Supremo Tribunal de Justiça

TC – Tribunal Constitucional

TRL – Tribunal da Relação de Lisboa

UE – União Europeia

Vol. - Volume

“Conheça todas as teorias, domine todas as técnicas, mas ao tocar uma alma humana seja apenas outra alma humana.”

CARL G. JUNG

ÍNDICE

INTRODUÇÃO

A presente Dissertação insere-se no âmbito do Mestrado em Ciências Jurídico-Forenses, tendo como principal objetivo a investigação do tema das tecnologias de reconhecimento facial e a sua possível utilização no processo penal português.

A capacidade para reconhecer rostos é inata aos seres humanos, sendo que *"a identificação é o ato mais frequente e elementar da vida social"*[1]. Não obstante, com o aumento da população, assim como das deslocações, houve uma crescente necessidade de documentar os cidadãos[2], tendo-se ao longo dos tempos procurado diferentes formas de se proceder ao reconhecimento destes.

Foi então que, na década de 60, se deram os primeiros passos no tema do reconhecimento facial, por Woodrow W. Bledsoe, Helen Chan Wolf e Charles Bisson, enquanto se focavam no estudo de tecnologias de reconhecimento de padrões.[3] Na sequência das suas descobertas, Bledsoe desenvolveu um sistema que era capaz de identificar rostos, baseando-se para isso numa base de dados repleta de fotografias.[4] Consequentemente, em virtude desta descoberta, e com o passar do tempo, foram surgindo novos sistemas de reconhecimento facial.[5]

---

[1] Expressão proferida pelo médico e antropólogo Federico Olóriz Aguilera, cfr. ARAÚJO, Marcos Elias Cláudio de, e PASQUALI, Luiz, "*Histórico dos Processos de Identificação*", p. 2, disponível em https://doczz.com.br/doc/7242/cap%C3%ADtulo-i---hist%C3%B3rico-dos-processos-de-identifica%C3%A7%C3%A3o, consultado a 11 junho 2022.

[2] DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. e VU, B., "*A Technological and Ethical Analysis of Facial Recognition in the Modern Era.",* 7 de dezembro de 2018, Engineering 183EW – Engineering and Society, pp. 9-12, disponível em https://www.academia.edu/38066258/A_ , consultado a 4 de outubro de 2021.

[3] *Ibidem*; LIBBY, C. e EHRENFELD, J., *"Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare*. Journal of Medical Systems", 2021, disponível em https://doi.org/10.1007/s10916-021-01723-w, consultado a 20 de fevereiro de 2022.

[4] Woodrow acabou por ser contratado pelo governo dos EUA para desenvolver o sistema com o propósito de melhorar a segurança. Cfr. DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., "*A Technological and Ethical Analysis of Facial Recognition …",* ob. cit., pp. 9-11; LIBBY, C. & EHRENFELD, J., *"Facial Recognition Technology in 2021 …",* ob. cit.

[5] Em 1970, Goldstein, Harmon e Lesk implementaram um sistema de reconhecimento facial que aumentava a especificidade da tecnologia. Em 1988 foi desenvolvida uma nova técnica por Sirovich e Kirby, denominada por Eigenfaces, ideia esta, mais tarde desenvolvida por Turk e Pentland. Cfr. DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., *"A Technological and Ethical Analysis of Facial Recognition …",* ob. cit., pp. 9-11; ABREU, Viviana Rubina Gonçalves, *"Reconhecimento Facial – Comparação do Uso de Descritores Geométricos Heurísticos e Aprendizagem Profunda"*, 2021, Dissertação no âmbito do Mestrado Integrado em Engenharia Electrotécnica e de Computadores, Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra, pp.18-19; SIROVICH, L. KIRBY, M., *"Low-dimensional procedure for the characterization of human faces"*, Journal of the Optical Society of America. A, Optics and image science, Vol.4, 1987, p.519 disponível em: https://www.researchgate.net/publication/19588504_Low-

Pode, portanto, inferir-se que o reconhecimento facial não é propriamente recente, este surgiu acompanhando o avanço tecnológico, o surgimento da Inteligência Artificial e a crescente necessidade de um sistema eficiente e seguro, fazendo hoje parte do quotidiano da generalidade das pessoas.

No entanto, após a descoberta do reconhecimento facial e das suas vantagens, foi pensado o seu uso e aplicação nas mais diversas áreas, tanto no setor público, como forma de garantir a segurança das sociedades, podendo ser empregues nos aeroportos, no controlo de fronteiras, ou, até mesmo, na via pública, tornando mais eficiente a procura por fugitivos e na procura de pessoas desaparecidas[6], assim como para a descoberta da verdade material. Sob outra perspetiva temos a sua utilização no setor privado, a título de exemplo, nos diversos dispositivos móveis que nos permitem o acesso através do reconhecimento facial.[7] Esta sua atratividade tem levado a frequentes debates por todo o Mundo.

Acontece que, atualmente, vivemos num tempo que começa a assemelhar-se à sociedade descrita por George Orwell, na sua obra "1984", onde se relatava uma sociedade em que os indivíduos eram constantemente observados e controlados, como dizia Orwell *"Havia que viver – e vivia-se, graças a um hábito que se fazia instintivo – no pressuposto de que cada som emitido estaria a ser escutado e, salvo na escuridão, cada movimento, vigiado"*.[8] Poderá a nossa realidade estar efetivamente a aproximar-se da descrita na obra supramencionada?

A verdade é que a existência do reconhecimento facial já não é recente, no entanto, a inexistência de regulamentação do seu uso é, de certa forma, preocupante, propiciando a um errado uso destas tecnologias, podendo, inclusive, estar em causa a violação de Direitos Fundamentais.

Dimensional Procedure for the Characterization of Human Faces, consultado a 7 de março de 2022; TURK, Matthew e PENTLAND, Alex, "*Eigenfaces for Recognition",* Massachusetts Institute of Technology, Journal of Cognittive Neuroscience, Volume 3, number 1, disponível em https://www.face-rec.org/algorithms/PCA/jcn.pdf, consultado a 7 de março de 2022.

[6] DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., *"A Technological and Ethical Analysis of Facial Recognition …",* ob. cit., p. 16; AKHTAR, Marya, *"Police use of facial recognition technology and the right to privacy and data protection in Europe"*. Naveiñ Reet: Nordic Journal of Law and Social Research, n.º 9, 2019, pp. 325-326, disponível em https://tidsskrift.dk/nnjlsr/article/view/122165/169414, consultado a 16 de setembro de 2021.

[7] RODRIGUES, Sara Raquel dos Santos, *"Desenvolvimento de um Sistema de Reconhecimento Facial"*, 2020, Dissertação do Mestrado em Engenharia Eletrónica e de Computadores, Departamento de Engenharia Eletrotécnica, Instituto Superior de Engenharia do Porto, p. *iii*.

[8] ORWELL, George, "*1984"* (Ana Luísa Faria, Trad.). Coleção Mil Folhas, PUBLICO, 2002, ISBN 84-8130-562-6, p. 9.

Com o presente estudo, pretende-se, num primeiro momento conhecer melhor as tecnologias de reconhecimento facial, bem como fazer uma pequena menção da sua utilização no contexto internacional. Num segundo momento, o estudo será centrado na temática da admissibilidade das tecnologias de reconhecimento facial como prova no processo penal português, abordando ainda, num terceiro momento, os direitos fundamentais, tendo em conta os problemas que podem surgir quanto à relação entre as tecnologias de reconhecimento facial e os direitos fundamentais.

Para tal propósito, a presente dissertação tocará nas possíveis vantagens que estas tecnologias têm para a nossa sociedade, bem como, nos possíveis obstáculos ao uso das mesmas, como por exemplo, potenciais ofensas a direitos fundamentais, como o direito à reserva da intimidade da vida privada e familiar, o direito à imagem, o direito à proteção legal contra qualquer forma de discriminação, etc..

Pelo exposto, percebe-se a atualidade e pertinência deste estudo reflexivo, num momento em que muito se discute o surgimento e desenvolvimento da Inteligência Artificial, associando ao facto de a sociedade estar mais ciente dos seus direitos, em especial, prezando pela sua privacidade.

Esta discussão atravessa, atualmente, todo o Mundo, sendo, por isso, de especial importância contextualizar e concretizar a possibilidade da admissibilidade das tecnologias de reconhecimento facial no sistema jurídico português, em especial no direito processual penal, nunca esquecendo que, também, suscita pertinentes questões a nível constitucional.

Ora, terá sido George Orwell um visionário em relação a este tema? Ou pelo contrário, as ofensas aos direitos fundamentais fazem com que seja inadmissível o uso de tecnologias de reconhecimento facial no processo penal português?

A questão em causa é, poderão efetivamente ser utilizadas estas tecnologias como prova no processo penal? Poderá o Estado controlar toda esta informação sem incorrer em violações aos direitos fundamentais dos cidadãos? Assim como, será esta tecnologia suficientemente precisa e rigorosa? Que passos se poderão tomar para serem protegidos os direitos fundamentais em causa?

CAPÍTULO I
RECONHECIMENTO FACIAL

1. Considerações iniciais

É notório que, ao longo dos tempos, a tecnologia tem sofrido um grande desenvolvimento a nível global, consequentemente assistimos a uma substancial mudança no nosso quotidiano devido ao impacto causado por este, acabando por influenciar todas as áreas da vida social.[9] Perante este desenvolvimento, o direito penal e processual penal não podem ficar alheios, tendo, efetivamente, que ir respondendo às questões e aos problemas trazidos por estes avanços tecnológicos[10].

O desenvolvimento que se refere, deve-se, principalmente, aos avanços na área da Inteligência Artificial (IA)[11] e do *big data.*[12]

---

[9] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", *in: A Inteligência Artificial no Direito Penal*, coord: Anabela Miranda Rodrigues, Almedina, 2022, p. 130.

[10] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal – a Justiça Preditiva entre a Americanização e a Europeização", Almedina, 2022, p.12

[11] "A inteligência artificial (IA) é a capacidade que uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade. A IA permite que os sistemas técnicos percebam o ambiente que os rodeia, lidem com o que percebem e resolvam problemas, agindo no sentido de alcançar um objetivo específico. O computador recebe dados (já preparados ou recolhidos através dos seus próprios sensores, por exemplo, com o uso de uma câmara), processa-os e responde. Os sistemas de IA são capazes de adaptar o seu comportamento, até certo ponto, através de uma análise dos efeitos das ações anteriores e de um trabalho autónomo, cfr., "O que é a inteligência artificial e como funciona?", Parlamento Europeu, disponível em https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona, consultado a 16 de setembro de 2021. John McCarthy (conhecido pelos seus estudos no campo da IA) define esta como a ciência que constrói máquinas, algo parecido com a tarefa de usar computadores para perceber a inteligência humana e por vezes envolvendo a sua simulação, mas também o estudo dos problemas que o mundo coloca à inteligência humana. Cfr. MCCARTHY, John, "*WHAT IS ARTIFICIAL INTELLIGENCE?"*, Computer Science Department Stanford University, Stanford, CA 94305, pp. 2-8, disponível em http://jmc.stanford.edu/articles/whatisai/whatisai.pdf, consultado a 16 de setembro de 2021. FRA – European Union Agency For Fundamental Rights, "*Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*", Luxembourg, Publications Office, junho 2019, p. 2, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf, consultado a 16 de setembro de 2021.

[12] Trata-se de desenvolvimentos tecnológicos na área do armazenamento e do processamento de dados, possibilitando o tratamento de aumentos no volume e variedade de dados em curtos espaços de tempo, crf. SCHERMANN, M. HEMSEN, H. BUCHMÜLLER, C. BITTER, T. KRCMAR, H. MARKL, V. e HOEREN T., "*Big Data, Na Interdisciplinary Opportunity for Information Systems Research*", Business & Information Systems Engineering 6, 2014, pp. 261-266, disponível em https://link.springer.com/article/10.1007/s12599-014-0345-1, consultado a 16 de setembro de 2021; "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.", cfr. GARTNER, "*What is Big Data?"* – Gartner IT Glossary – Big Data, 2018, disponível em http://www.gartner.com/it-glossary/big-data, consultado a 16 de setembro de 2021; "Vast amounts of data are being collected, analysed and used, at an ever increasing pace – a phenomenon referred to as Big Data. Often, but not exclusively, data are gathered over the internet and smartphones. Such data are considered an important asset that provides the basis for many AI applications and

Sendo que, à medida que se avançava na área da IA e do *big data*, também se desenvolvia o reconhecimento facial.[13]

Urge, em primeira linha, esclarecer o que é o reconhecimento facial. Michael O'Flaherty refere, de uma forma simplificada, que se trata de tecnologias que tornam possível a comparação de duas imagens de forma a saber se se trata ou não de imagens da mesma pessoa[14], da mesma forma, Verónica Orvalho define esta como "tecnologia capaz de identificar uma pessoa a partir de uma imagem digital ou de um vídeo".[15] Mais detalhadamente temos a definição publicada pelo *Data Protection Working Party* «is the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals"».[16]

Apesar da atualidade deste tema, existe um Ac. do STJ de 27-09-2017 que se refere ao reconhecimento facial, definindo este como o "*emprego de técnicas de fotografia forense avançadas que incluem identificação de padrões faciais, elaboração de um perfil antropométrico único e comparação com os padrões que não oferecem dúvidas. Por meio de software de edição fotográfica determina-se a correcção a aplicar sobre a imagem para, deste modo, poder precisar a localização dos pontos de referência. Por meio de negatoscopio digital pode-se realizar sobreposições entre as imagens que oferecem dúvidas e as isentas de dúvidas, analisando a correspondência entre os pontos de referência*".[17]

progress in the field" cfr. FRA – European Union Agency For Fundamental Rights," *Data quality and artificial intelligence…" ob. cit.*, p. 4.

[13] NEGRI, Sérgio; OLIVEIRA, Samuel e COSTA, Ramon, *"Proteção de Dados e Inteligência Artificial: Persptivas Éticas e Regulatórias. O Uso de Tecnologias de Reconhecimento Facial baseadas em Inteligência Artificial e o Direito à Proteção de Dados"*, RDP, Brasília, Volume 17, n.º 93, maio/junho 2020 pp. 83-84, disponível em https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740/Negri%3B%20Oliveira%3B%20Costa%2C%202020, consultado a 24 de outubro de 2021.

[14] O'FLAHERTY, Michael, "*Facial Recognition Technology and Fundamental Rights*. Opinions", European Data Protection Law Review (EDPL), Vol. 6, Issue 2 (2020), p. 170, disponível em HeinOnline https://heinonline.org/HOL/Page?public=true&handle=hein.journals/edpl6&div=29&start_page=170&collection=journals&set_as_cursor=13&men_tab=srchresults, consultado a 12 de outubro de 2021.

[15] Excerto retirado de ORVALHO, Verónica, *"Reconhecimento Facial",* Ver. Ciência Elem., Casa das Ciências, 2019, disponível em http://doi.org/10.24927/rce2019.073, consultado a 16 de setembro de 2021.

[16] Article 29 Data Protection Working Party (2012), "*Opinion 02/2012 on facial recognition in online and mobile services"*, 00727/12/EN, WP 192, Bruxelas, 22 Março 2012, p.2, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, consultado a 13 de novembro de 2021.

[17] Ac. do STJ, Proc. n.º 427/14.0JACBR.C1, de 27-09-2017, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/79760e66f0bf4ba4802581bb003b2bd8?OpenDocument

No que diz respeito ao seu funcionamento, o reconhecimento facial faz uso de dados biométricos, que comportam características únicas de cada pessoa[18], podendo, de certa forma, comparar-se a uma impressão digital.[19] Ou seja, estes sistemas operam mediante o uso de biometria, esquematizando as características faciais de uma pessoa, presentes numa fotografia ou vídeo. Recolhidas estas informações, são depois comparadas com as informações armazenadas num banco de dados, isto é, com rostos conhecidos, com o intuito de encontrar uma correspondência. [20]

Um sistema de reconhecimento facial é constituído por etapas (algumas das quais comuns aos diferentes sistemas). Regra geral, primeiramente tem de se detetar o rosto na fotografia/vídeo, sendo que desta imagem vão extrair-se as características com maior interesse[21], após esta etapa temos o reconhecimento do rosto, sendo aqui que se compara o rosto detetado com imagens de rostos já pertencentes a uma base de dados, verificando-se as semelhanças.[22]

Comummente o reconhecimento facial é utilizado para verificação da identidade, onde o que se procura é apenas a confirmação de que aquele indivíduo é quem diz ser, que é o que acontece com muitos *smartphones* atuais, por exemplo, e com dispositivos de

---

[18] "«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos", cfr. art. 3.º, al. o) da Lei n.º 59/2019, de 08 de agosto e art. 4.º, n.º 14 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[19] A biométrica analisa características físicas do ser humano, características estas singulares, como as impressões digitais e padrões do rosto, possibilitando a identificação de um indivíduo, que, à partida, tem características físicas diferentes, cfr. RODRIGUES, Sara Raquel dos Santos, *"Desenvolvimento de um Sistema de Reconhecimento Facial"*, ob. cit., p. 1; Article 29 Data Protection Working Party, "*Opinion 4/2007 on the concept of personal data*", junho, 01248/07/EN WP136, p.8, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, consultado a 13 de novembro de 2021.

[20] Cfr. WECHSLER, Harry – "Reliable Face Recognition Methods, System Design, Implementation and Evaluatio", George Mason University, USA, Springer, pp.97-118 disponível em https://link.springer.com/content/pdf/10.1007/978-0-387-38464-1.pdf, consultado a 3 de dezembro de 2021.

[21] É certo que o rosto apresenta características variáveis em cada pessoa, contudo, existem certas combinações que não se alteram, como é o caso da distância entre os olhos, cfr. CONCEIÇÃO, Valdir Silva, NUNES; Edna Maria e ROCHA, Ângela Machado, *"O reconhecimento facial como uma das vertentes da Inteligência Artificial (IA): um estudo de prospeção tecnológica"*, Cadernos de Prospecção – Salvador, v. 13, n. 3, junho, 2020, pp.746-747, disponível em http://dx.doi.org/10.9771/cp.v13i3.32818, consultado a 16 de novembro de 2021.

[22] ABREU, Viviana Rubina Gonçalves, "*Reconhecimento Facial – Comparação do Uso de Descritores Geométricos Heurísticos e Aprendizagem Profunda*", ob. cit., pp.18-19; RODRIGUES, Sara Raquel dos Santos, "*Desenvolvimento de um Sistema de Reconhecimento Facial*", ob. cit. pp. 49-52.

controlo de entradas. Isto é o que se chama de comparação de "um para um" ("*one-to-one*").[23]

Todavia, o reconhecimento facial pode ter ainda como propósito a identificação de uma pessoa, ou seja, parte-se de uma imagem de um rosto desconhecido, e compara-se este com uma base de dados com imagens de rostos conhecidos, a fim de se determinar a identidade da pessoa, de se encontrar uma correspondência, também designada de "um para vários" ("*one-to-many*"). Findo este procedimento, é dada uma percentagem de probabilidade de se tratar da mesma pessoa, nunca dando lugar a uma certeza, isto é, nunca nos dá um resultado definitivo e absoluto, apenas uma mera probabilidade de se tratar da mesma pessoa.[24]

Acontece que, estes sistemas trazem consigo inúmeras vantagens, contudo, há vários fatores que influenciam o correto uso destes, podendo ser verdadeiros obstáculos, como, por exemplo, a iluminação, a idade, o género, a cor da pele, o uso de óculos, chapéus e demais acessórios, entre outros.[25] Esta questão será abordada mais detalhadamente nos pontos seguintes deste Capítulo.

A verdade é que estas tecnologias podem levar a uma substancial alteração ao modo como a investigação em processo penal é realizada, assim como relativamente aos meios admissíveis de prova, especialmente nesta sua vertente de identificação.

1.1. Vantagens na utilização do reconhecimento facial

As tecnologias de reconhecimento facial possuem um sem número de vantagens, tornando-as seriamente cativantes.

---

[23] RODRIGUES, Sara Raquel dos Santos, "*Desenvolvimento de um Sistema de Reconhecimento Facial*", ob. cit., p. 49-52; AKHTAR, Marya, *"Police use of facial recognition technology and the right to privacy and data protection in Europe",* ob. cit., pp. 328-332; FRA – European Union Agency For Fundamental Rights, *"Facial recognition technology: fundamental rights considerations in the context of law enforcement"*, novembro 2019, pp. 7-10, disponível em https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law, consultado a 13 de novembro de 2021.

[24] *Ibidem*.

[25] FRA – European Union Agency For Fundamental Rights, "*Facial recognition technology: fundamental rights considerations…",* ob. cit., pp. 9-10; LI, Stan Z. e JAIN, Anil K., *"Handbook of Face Recognition"*, 2005 Springer Science+Business Media, Inc., pp. 4-7, disponível em https://link.springer.com/content/pdf/10.1007/b138828.pdf, consultado a 20 de setembro de 2021.

A vantagem primordial destas é a inegável contribuição para a realização da justiça e para a descoberta da verdade material.[26] Pensando, por exemplo, numa sua utilização no processo penal, poderá auxiliar na investigação criminal, identificando os autores da prática do ilícito típico criminal.

Ademais, e sendo um fator a favor da utilização destas tecnologias, está o facto de os dados biométricos serem intransmissíveis de pessoa para pessoa, uma vez que assim é, é muito difícil que estes sejam imitados. Destarte, torna-se este um procedimento mais seguro do que o uso de palavras-passe e códigos de acesso, que podem ser perdidos, esquecidos e usados por outrem que não o seu titular.[27]

É certo que, o reconhecimento facial não é o único procedimento que faz uso de dados biométricos, mas a verdade é que se trata do procedimento que os captura com mais facilidade, sem haver necessidade de uma cooperação direta da pessoa em questão, ao contrário do que acontece, a título de exemplo, com as impressões digitais, onde é necessário que a pessoa em questão participe ativamente na recolha destes dados. Ora, no reconhecimento facial não é isso que acontece, por vezes a pessoa nem se apercebe que estão a ser recolhidos os seus dados, sendo difícil evitar que estes dados sejam capturados num local público.[28]

Clive Norris acrescenta que esta 'forma de vigilância' torna-se mais democrática, uma vez que todos ficam igualmente sujeitos à vigilância, livre de restrições temporais como no caso da presença humana.[29]

Não se pode, também, olvidar o potencial efeito preventivo que podem ter estas tecnologias, uma vez que, sabendo-se que se está a ser "vigiado" poderá o número de crimes cometidos baixar, isto por receio de que através dos sistemas de reconhecimento facial facilmente se venha a descobrir a identidade do autor.[30]

---

[26] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo"*, ob. cit, p. 130.
[27] RODRIGUES, Sara Raquel dos Santos, "*Desenvolvimento de um Sistema de Reconhecimento Facial*", ob. cit., pp. 66-67.
[28] FRA – European Union Agency For Fundamental Rights*, "Facial recognition technology: fundamental rights considerations…",* ob. cit., p. 5.
[29] NORRIS, Clive, "From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control", *in "Surveillance as Social Sorting. Privacy, risk, and digital discrimination*", Routledge, David Lyon, 2003, ISBN 0-203-99488-4, pp. 263-266, disponível em https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf, consultado a 15 de setembro de 2021.
[30] *Ibidem*.

A aditar a este leque de vantagens, sendo também de extrema importância, é o caso das crianças desaparecidas, que, apesar das dificuldades no reconhecimento destas, através do uso destes sistemas afigura-se que seja mais fácil de as identificar e localizar.[31]

Em termos práticos, acrescenta-se o facto de que com estas tecnologias existe uma desnecessidade de mobilização de um grande número de agentes, sendo estes substituídos por câmaras e tecnologias capazes proceder à identificação das pessoas[32], o que é positivo uma vez que os agentes quando se encontram a patrulhar não conseguem estar constantemente a vigiar o mesmo local.[33] Acontece, também, que se for utilizado um algoritmo que seja operado por uma pessoa, a quantidade de dados que conseguirá operar é pequena, sendo que para isso necessitará de muito tempo, acabando por fornecer poucos *outputs*.[34] Contrariamente, se for utilizado um computador que realize esta tarefa de forma automática já se conseguirá operar um grande número de dados num curto espaço de tempo, fornecendo uma quantidade enorme de *outputs*, economizando também o tempo.[35]

Posto isto, facilmente se compreende a tentação de implementação destas tecnologias. No entanto, contrapondo com estas sedutoras vantagens, existe ainda um leque de problemas que podem surgir, igualmente numeroso, que se passa a nomear e analisar.

1.2. Problemas proporcionados pelo reconhecimento facial

Relativamente aos problemas trazidos pelas tecnologias em questão é preciso tomar muita atenção, uma vez que estes são fulcrais para uma possível aceitação da utilização destes no processo penal português.

---

[31] Relativamente às crianças, há que ter em atenção a sua vulnerabilidade, assim sendo, a coleta e o processamento dos seus dados deve ser feito muito restritamente, assim como, com o seu crescimento o rigor dos dados anteriormente adquiridos diminui, aumentando assim o risco de uma errada identificação, cfr. FRA – European Union Agency For Fundamental Rights*, "Facial recognition technology: fundamental rights considerations…",* ob. cit., p. 18.

[32] NISSENBAUM, Helen e INTRONA, Lucas D., "*Facial Recognition Technology. A survey of Policy and Implementation Issues*", The Center for Catastrophe Preparedness and Response, pp.20-21, disponível em https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues, consultado a 19 de dezembro de 2021.

[33] *Ibidem*.

[34] RODRIGUES, Anabela Miranda, "*A Inteligência Artificial no Direito Penal*", ob. cit., p. 23; FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit, p. 130.

[35] *Ibidem.*

Primeiramente, e um dos maiores problemas que pode surgir é a errada identificação de uma pessoa, isto porque se trata de uma tecnologia que não é perfeita e que está em constante desenvolvimento.[36] Havendo, inclusive, algumas formas de defraudar o resultado, como é o caso do uso de maquilhagem, óculos, cirurgias estéticas e, ainda, o caso de se tratar de gémeos, entre outros.[37] Pode acontecer ainda que, a variação da luz e o ângulo das imagens possa interferir no resultado, podendo conduzir a um resultado erróneo.[38] Ou seja, se não se conseguir garantir a qualidade e fiabilidade das imagens, pode, de facto, comprometer-se a exatidão dos resultados alcançados.[39] Ora, a qualidade de imagens retiradas de câmaras de vigilância está longe de ser de fácil controlo, podendo também constituir um sério risco para o rigor dos resultados que se pretende com o uso do reconhecimento facial, uma vez que a má qualidade pode conduzir a uma incorreta identificação de um indivíduo.[40] Nestes casos a "fidedignidade depende da exatidão dos meios tecnológicos usados".[41]

Acontece que, analisando-se os resultados que têm sido obtidos com estas tecnologias é notório que existe um menor rigor quando se trata de mulheres e pessoas com aparência não ocidental, diminuindo, assim, a efetividade da tecnologia e levando a resultados tendenciosos.[42] O perigo aqui em causa são os resultados discriminatórios, logo

---

[36] DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., *"A Technological and Ethical Analysis of Facial Recognition …",* ob. cit., pp. 13-15.

[37] RODRIGUES, Sara Raquel dos Santos, "Desenvolvimento de um Sistema de Reconhecimento Facial", ob. cit., pp. 49-52.; ORVALHO, Verónica, Reconhecimento Facial, ob. cit.; GALBALLY, J.;FERRARA, P.; HARAKSIM, R.; PSYLLOS, A. e BESLAY, L., "*Study on Face Identification Technology for its Implementation in the Schengen Information System*", EUR 29808 EN, Publication Office of the European Union, Luxemburg, 2019, ISBN 978-92-76-08843-1, doi:10.2760/661464, JRC116530, pp. 38-41 disponível em https://op.europa.eu/en/publication-detail/-/publication/dd473249-adbf-11e9-9d01-01aa75ed71a1/language-en, consultado a 5 de janeiro de 2022.

[38] SANTOS, Hugo Luz dos, "Inteligência Artificial e Processo Penal", Braga: Nova Causa, Edições Jurídicas, 2022, ISBN 9789899026308, pp. 163-165.

[39] Article 29 Data Protection Working Party*, "Opinion 3/2012 on developments on biometric technologies",* 27 de abril de 2012, 00720/12/EN, WP193, p. 6, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, consultado a 13 de novembro de 2021.

[40] FRA – European Union Agency For Fundamental Rights*, "Facial recognition technology: fundamental rights considerations…", ob. cit.*, p. 10.

[41] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", ob. cit., p. 142.

[42] Isto acontece porque o desenvolvimento/treino destes softwares é, maioritariamente, feito com imagens de homens brancos, *cfr.* FRA – European Union Agency For Fundamental Rights*, "Facial recognition technology: fundamental rights considerations…",* ob. cit., p. 10. Para uma melhor compreensão deste risco, cfr. Buolamwini, Joy e Gebru, Timnit*, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*", *Proceedings of Machine Learning Research* 81: 1-15, Conference on Fairness, Accountability, and Transparency, disponível em http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, consultado a 6 de setembro de 2022.

aqui se percebe que é necessário garantir primeiro uma certa eficácia nestas tecnologias para não se dar lugar a condutas discriminatórias.[43]

A razão por detrás deste acontecimento é, basicamente, a forma como estas tecnologias são 'treinadas', isto é, depende dos dados que são usados no desenvolvimento destas. Para uma maior exatidão nos resultados, é necessário haver um "treino" com uma grande variedade de dados, de forma a ser o mais representativo possível de todos os cidadãos, o mais abrangente possível. Caso contrário, por exemplo, um sistema "treinado" só com dados de homens, mas a população, onde realmente é testado o sistema, é composta também por mulheres, acabará por ter maus resultados quando se tratar da identificação destas.[44]

Não obstante, com o avanço dos anos, tem havido um maior rigor nestas tecnologias, sendo que o risco de erro tem vindo a diminuir.[45]

Como supramencionado, na operação de reconhecimento facial são reunidos e armazenados dados biométricos, mas é preciso ter em conta que, com o passar dos anos, as

---

[43] AKHTAR, Marya – *"Police use of facial recognition technology and the right to privacy…", ob. cit.*, pp. 332-333; contrapondo o entendimento da maioria, há quem defenda que o risco de discriminação existe tanto com a implementação do reconhecimento facial, como quando o reconhecimento está a ser feito pelas autoridades competentes, cfr. *FRA – European Union Agency For Fundamental Rights, "Facial recognition technology: fundamental rights considerations…", ob. cit.,* pp. 27-28. Porém, houve, inclusivemente, um alerta do Parlamento Europeu para existir o máximo cuidado possível de forma a prevenir a discriminação, cfr. FRA – European Union Agency For Fundamental Rights*, "#BigData: Discrimination in data-supported decision making",* 2018, ISBN 978-92-9474-069-4, doi:10.2811/343905, p.2, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf, consultado a 16 de novembro de 2021; existe também quem defenda que, apesar de tudo, este sistema é menos discriminatório do que quando a identificação se faz por um agente da autoridade 'físico', ou seja, que as máquinas têm um menor risco de discriminação. Contudo, seria sempre necessário tomar medidas que prevenissem a discriminação e existir o dever de os agentes da polícia verificarem os resultados antes de agirem, cfr. Eu-LISA, *"Smart Borders Pilot Project Technical Report Annexes Volume 2*", European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 2015, ISBN 978-92-95203-95-2 doi:10.2857/898335, pp. 330-331, disponível em https://home-affairs.ec.europa.eu/system/files/2020-09/smart_borders_pilot_-_technical_report_annexes_en.pdf, consultado a 8 de fevereiro de 2022.

[44] GALBALLY, J.;FERRARA, P.; HARAKSIM, R.; PSYLLOS, A. e BESLAY, L., *"Study on Face Identification Technology"*, ob. cit., p. 66. No entanto, é preciso atentar que uma maior base de dados pode levar a um maior número de falsos positivos, cfr. POGO – Project on Government Oversight, *"Facial Recognition Facing the Future of Surveillance"*, Task Force on Facial Recognition Surveillance, 4 de março de 2019, pp. 31-33, disponível em https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance, consultado a 18 de outubro de 2021; BUOLAMWINI, Joy, "*how I'm fighting bias in algorithms",* produção de TedxBeaconStreet, 2016, vídeo, disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms, consultado a 8 de fevereiro de 2022; FRA- European Union Agency For Fundamental Rights, "*Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*", ob cit., pp. 8-10.

[45] FRA – European Union Agency For Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", ob. cit., pp. 33-34.

características biométricas vão-se degradando, vão-se alterando, sendo que após cinco anos será mais difícil de obter resultados exatos diminuindo, portanto, a precisão destes.[46]

Também não se pode descorar que doenças, acidentes, cirurgias, entre outros, influenciam a capacidade destas tecnologias fazerem o seu reconhecimento, compreendendo-se desta forma a importância da manutenção e atualização da base de dados.[47]

No que concerne às crianças existem questões pertinentes, como: quando é que se pode justificar a recolha e armazenamentos dos seus dados antes de atingirem a idade legal? Há quem responda dizendo que isto apenas seria permitido nos casos de desaparecimentos de crianças.[48] Para além disso, as características faciais destas são as que mais se vão alterando com o passar dos anos.

À parte destes riscos técnicos, por assim dizer, mais complexo e crucial é o constante sentimento de que se está a ser vigiado[49], uma vez que se trata de imagens que podem ser capturadas à distância, sem o conhecimento e consentimento das pessoas.[50] Ou seja, a maior adversidade ao uso destas tecnologias é uma potencial violação da privacidade[51], sendo afetadas inúmeras pessoas, mesmo nada tendo feito de errado.[52] A

---

[46] *Ibidem*, pp. 28-29.

[47] RODRIGUES, Sara Raquel dos Santos, "Desenvolvimento de um Sistema de Reconhecimento Facial", ob. cit., p. 67; AKHTAR, Marya – *"Police use of facial recognition technology and the right to privacy…", ob. cit.*.

[48] FRA – European Union Agency For Fundamental Rights, *"The revised Visa Information System and its fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights",* Viena, 30 de agosto de 2018, pp. 67-69, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-visa-information-system-02-2018-corr_en.pdf, consultado a 16 de novembro de 2021.

[49] AKHTAR, Marya – *"Police use of facial recognition technology and the right to privacy…", ob. cit.;* "Como os nossos rostos são tão individualistas quanto as nossas impressões digitais, a tecnologia de reconhecimento facial dita que a privacidade termina no momento em que saímos de casa", cfr. ORAVALHO, Verónica, Reconhecimento Facial, *ob. cit.*.

[50] Article 29 Data Protection Working Party, *"Opinion 3/2012 on develoments on biometric technologies",* ob. cit., p. 5.

[51] Em jeito de exemplo temos um caso na Suécia em que foi usado o reconhecimento facial para monitorizar a presença de alunos numa escola. Após avaliar a situação a Autoridade Sueca de Proteção de Dados concluiu que violaria a privacidade dos alunos, havendo meios menos intrusivos para controlar a presença dos alunos, acabando por multar a escola em questão. Cfr. European Data Protection Board, *"Facial recongnition in school render Sweden's first GDPR fine"*, 22 de agosto de 2019, disponível em https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv, consultado a 15 de novembro de 2021. À mesma conclusão chegou a Autoridade Francesa de Proteção de Dados, cfr. CNIL, *"Expérimentation de la reconnaissance facial edans deux lycées: la CNIL precise sa position",* 29 de outubro de 2019, disponível em https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position, consultado a 18 de novembro de 2021.

[52] O Professor Christopher Slobogin falou deste problema, referindo que estas técnicas seriam invasivas, e que se trataria de uma "public surveillance gap" referindo ainda o direito ao anonimato, cfr. RUBINSTEIN, Ira S., Privacy Localism, Washington Law Review, Volume 93, Issue 4, 2018, pp. 1974-1980, disponível em

acrescer temos a eventual intromissão no direito à liberdade de reunião e manifestação, isto acontece porque as pessoas sabendo que estão a ser constantemente monitorizadas, acabam por se comportar de maneira diferente.[53]

Há quem considere, também, que estas tecnologias sendo uma intromissão na vida dos cidadãos, podem tornar-se, efetivamente, numa ferramenta para a opressão, pois os governos podem fazer uso destas da maneira que mais lhes aprouver, podendo, inclusive, ser uma ameaça à existência da democracia.[54]

Outra questão pertinente tem, de facto, a ver com a proteção dos dados, uma vez que estas tecnologias fazem uso de dados pessoais, que são os dados biométricos, haverá intromissão no direito à proteção de dados?[55] Podendo ainda surgir um risco de manipulação dos dados armazenados, um risco de estes serem comprometidos.[56]

Verdadeiramente não se pode esperar que o nosso rosto não seja visto quando estamos em público, contudo, será que se deve esperar que a mera vista do nosso rosto fique instantaneamente disponível para quem esteja no lado recetor das câmaras?[57]

---

https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4083&context=wlr, consultado a 17 de setembro de 2021.

[53] Nlets – the International Justice and Public Safety Network, *"Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field",* 30 de junho de 2011, pp. 18-19, disponível em https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf, consultado a 23 de outubro de 2021; Human Rights Council, *"Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression",* 28 de maio de 2019, disponível em https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement, consultado a 9 de novembro de 2021.

[54] WHITTAKER, M.; CRAWFORD, K.; DOBBE, R.; FRIED, G.; KAZIUNAS, E.; MATHUR, V.; WEST, S.; RICHARDSON, R.; SCHULTZ, J. e SCHWARTZ, O., *"AI Now Report 2018",* AI Now Institute, New York University dezembro 2018, p.17, disponível em https://ainowinstitute.org/AI_Now_2018_Report.pdf, consultado a 31 de outubro de 2021. Como é o caso de Jonathan Frankle, um investigador na área da IA no Instituto de Tecnologia de Massachusetts. Cfr. MOZUR, Paul, *"One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", The New York Times*, 2019, disponível em https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html, consultado a 14 de novembro de 2021.

[55] Nlets – the International Justice and Public Safety Network, *"Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field", ob.cit*, pp. 18-19; Human Rights Council, *"Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression",* ob. cit., p.5.

[56] DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., "*A Technological and Ethical Analysis of Facial Recognition …",* ob. cit., pp. 13-15; RODRIGUES, Sara Raquel dos Santos, *"Desenvolvimento de um Sistema de Reconhecimento Facial"*, ob. cit., p. 67; GALBALLY, J.;FERRARA, P.; HARAKSIM, R.; PSYLLOS, A. e BESLAY, L., "*Study on Face Identification Technology for its Implementation in the Schengen Information System"*, ob. cit., pp. 38-41.

[57] WIEHL, Tom, *"Human and Computerized Facial Recognition: comparison and constitutional analysis",* Northwestern Interdisciplinary Law Review, Vol. VI. No. 1, 2013, pp. 123-124, disponível em https://heinonline.org/HOL/LandingPage?handle=hein.journals/nwilr6&div=9&id=&page=, consultado a 17 de outubro de 2021.

Daqui se retira que as tecnologias de reconhecimento facial apresentam um leque variado de vantagens, assim como de desvantagens, sendo que não há ainda qualquer legislação relativamente ao tema, regulamentação esta que, a existir, terá de ser minuciosa para prevenir todos os riscos enumerados.[58]

Desta feita, primeiramente é necessário uma abordagem ao tema da prova e da sua admissibilidade no processo penal português, percorrendo um pouco pelos direitos fundamentais afetados pela utilização do reconhecimento facial. A verdade é que, se se concluir que é possível uma futura admissibilidade destas tecnologias como prova, é fundamental que se alcance uma regulamentação que proteja os direitos fundamentais, evitando todos os riscos que foram supramencionados.[59]

2. Panorama Internacional

A questão da possibilidade do uso de tecnologias de reconhecimento facial tem sido colocada a nível internacional, sendo que em alguns países efetivamente já se usa, noutros ainda está a ser testada a possibilidade do seu uso, enquanto há países que apenas hipoteticamente colocam a questão sem realizar qualquer teste.

Um dos países em que o uso destas tecnologias tem sido mais questionado é nos Estados Unidos da América, que efetivamente já fizeram uso destas. Contudo, alguns dos Estado acabaram por colocar barreiras ao seu uso.

A verdade é que nos EUA faz-se uso do reconhecimento facial para detetar suspeitos e terroristas em grandes eventos[60], como por exemplo, em eventos desportivos e concertos, assim como para identificar abusadores sexuais. Acontece que, em 2019, ocorreu um dos casos mais marcantes em relação às tecnologias de reconhecimento facial. Portanto,

---

[58] Sendo este mesmo o motivo por no Canadá não se considerar o uso desta tecnologia seguro, cfr. MCSORLEY, Tim, *"The Case for a Ban on Facial Recognition Surveillance in Canada"*, International Civil Liberties Monitoring Group, Canada, Surveillance & Society, 19(2), pp. 250-254, disponível em https://doi.org/10.24908/ss.v19i2.14777, consultado a 9 de janeiro de 2022.

[59] "Greater accuracy is not the point. We need strong legal safeguards that guarantee civil rights, fairness and accountability. Otherwise, this technology will make all of us less free", cfr. *"Regulate facial-recongition technology",* Springer Nature Limited, Vol. 572, 2019, p.565, disponível em https://media.nature.com/original/magazine-assets/d41586-019-02514-7/d41586-019-02514-7.pdf, consultado a 25 de novembro de 2021.

[60] Isto aconteceu principalmente após os atentados terroristas de setembro de 2001, de forma a garantir a segurança dos cidadãos, tentando que não se volte a repetir a mesma situação, cfr. NEGRI, Sérgio; OLIVEIRA, Samuel & COSTA, Ramon, "Proteção de Dados e Inteligência Artificial…", ob. cit. p. 86.

nesse ano, para se identificar um abusador sexual de crianças, que tinha filmado o abuso, fez-se uso de uma aplicação denominada de "Clearview AI". A aplicação acabou por encontrar uma correspondência, que se veio a comprovar correta, uma vez que no decorrer da investigação o suspeito confessou o crime, vindo a ser condenado[61]. Após se descobrir o efetivo uso desta aplicação e do seu funcionamento (uma vez que fazia uso de uma base de dados que continha imagens retiradas de páginas da Internet e posteriormente associava a imagem ao link da página da qual tinha sido retirada) as pessoas revoltaram-se, empresas como o Facebook, LinkedIn, Venmo e Google enviaram cartas à empresa criadora da aplicação em questão informando da violação dos seus termos de uso e exigindo que parassem de usar as fotografias das suas plataformas.[62] Sucede-se que, foi criado um alarido tal que acabou por ser banido o uso destas tecnologias pela polícia, por exemplo, em São Francisco[63], Boston e Minneapolis; outras cidades, ao invés de banirem, apenas limitaram o seu uso, como foi o caso de Washington e Massachusetts que declararam a necessidade de haver primeiro uma autorização do juiz para depois se poder fazer uso da aplicação; em Illinois e Texas estabeleceu-se que a empresa teria de ter o consentimento dos seus residentes para usarem os seus dados biométricos.[64]

Não obstante toda a polémica causada e todas as queixas feitas contra a "Clearview AI", esta não foi processada, nem extinta, continuando em atividade. Assim como também não houve qualquer legislação para controlar o seu uso.

Apesar do grande alarido causado e da revolta contra estas tecnologias de reconhecimento facial, mais recentemente começou a mudar-se de ideias, isto aconteceu quando houve a invasão ao Capitólio dos Estados Unidos em 2021, sendo que nesse caso

---

[61] HILL, Kashmir, *"Your Face Is Not Your Own. When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.",* The New York Times Magazine, 2021, disponível em https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html, consultado a 9 de janeiro de 2022.

[62] *Ibidem*.

[63] São Francisco foi a primeira cidade dos Estados Unidos da América a proibir o uso de tecnologias de reconhecimento facial pela polícia, com receio que os EUA se dirigissem para um estado opressivo, cfr. CONGER, K., FAUSSET, R., KOVALESKI, S.F., *"San Francisco Bans Facial Recognition Technology",* The New York Times Magazine, 14 de maio de 2019, disponível em https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html, consultado a 27 de setembro de 2021.

[64] HILL, Kashmir, *"Your Face Is Not Your Own. When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.",* ob. cit.

equacionaram o uso destas tecnologias e efetivamente fizeram uso delas para identificar as pessoas presentes no motim.[65]

Uma vez surgido este tema, foi efetuada uma pesquisa pelo *Pew Research Centre*, com a qual se descobriu que a maioria dos americanos (56%) confia no uso responsável de tecnologias de reconhecimento facial pelas autoridades, já menos pessoas confiam no seu uso por empresas de tecnologia (36%) ou para fins publicitários (18%).[66]

Um dos países em que o uso das tecnologias de reconhecimento facial já faz parte do quotidiano dos seus cidadãos é a China. Onde existem mais de 200 milhões de câmaras de vigilância por todo o país com o objetivo de vigiar a população e assegurar o cumprimento da lei e das normas sociais[67], prevenir crimes violentos, identificar ladrões, fugitivos, ou até mesmo para apanhar os estudantes que estão a dormir nas salas de aulas, entre outras situações.[68]

Porém, tem sido levantado um problema quanto ao uso pela China destas tecnologias, sendo este preocupante, que é o facto de, através destas se estar a categorizar etnias, estando a ser utilizadas para localizar e controlar os Uighurs (minoria muçulmana), encaminhando muitos deles para campos de reeducação.[69]

---

[65] *Ibidem.*

[66] SMITH, Aaron, *"More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recogniion Responsibly",* Pew Research Center, 2019, disponível em https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/, consultado a 1 de outubro de 2021.

[67] HILL, Kashmir, *"Your Face Is Not Your Own. When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.", ob. cit.*.

[68] LENTINO, Amanda. *"This Chinese facial recogniton start-up can identify a person in seconds*". CNBC Disruptor 50, 2019, disponível em https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html, consultado a 1 de outubro de 2021.

[69] MOZUR, Paul. *"One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority"*, ob. cit.; HILL, Kashmir, *"Your Face Is Not Your Own, When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.", ob. cit.;* PHILLIPS, Tom. *"China testing facial-recognition surveillance system in Xinjiang – report",* The Guardian, 2018, disponível em https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report, consultado a 1 de outubro de 2021; *"China: Big Data Fuels Crackdown in Minority Region. Predictive Policing Program Flags Individuals for Investigations, Detentions",* Human Rights Watch, 2018, disponível em https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region, consultado a 1 de outubro de 2021;*"Eradicating Ideological Viruses. China's Campaign of Repression. Against Xinjiang's Muslims",* Humam Rights Watch, 2018, ISBN: 978-1-6231-36567, pp.10-25, disponível em https://www.hrw.org/sites/default/files/report_pdf/china0918_web.pdf, consultado a 1 de outubro de 2021.

Houve, igualmente, um aumento substancial do uso destas em tempos de pandemia, tendo sido usadas para identificar indivíduos potencialmente infetados com base na sua temperatura corporal.[70]

Também na Rússia, em 2016 uma empresa, designada NTechLab desenvolveu uma aplicação chamada "FindFace" que retirava fotos de perfis da plataforma VK. No entanto, começou a verificar-se um uso deturpado desta aplicação, estando a ser usada, entre outros propósitos, para identificar protestantes. Não obstante, a aplicação em causa, similar ao que aconteceu com a 'Clearview AI', passou a ser providenciada ao governo, tendo em 2019 sido introduzida nas câmaras de segurança espalhadas por Moscovo, com o objetivo de ajudar a encontrar suspeitos de crimes. Sendo que, tal como na China, foi útil em tempos de pandemia, porém, na Rússia estas serviram para identificar pessoas que não estavam a respeitar a quarentena.[71]

Diversos países fazem, também, uso destas tecnologias como forma de dinamizar e tornar mais célere o procedimento de entrada nos aeroportos, como é o caso do Dubai, da Alemanha, por exemplo, no aeroporto de Frankfurt.[72] No caso do Dubai, aqui também se faz uso destes mecanismos como postos de controlo.[73]

No Brasil também se faz uso das tecnologias de reconhecimento facial, como é exemplo o programa Rio+Seguro.[74]

Por último é pertinente referir o Reino Unido, país este onde vários testes e sondagens têm sido efetuadas relativamente ao uso de tecnologias de reconhecimento facial.

---

[70] MARASCIULO, Marília, "Reconhecimento facial: prós e contras da tecnologia que veio para ficar", GALILEU, junho de 2020, disponível em https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html, consultado a 18 de setembro de 2021.

[71] HILL, Kashmir, *"Your Face Is Not Your Own, When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.",* ob. cit..

[72] *"Cognitec awarded contract by German federal criminal police office",* SOURCESecurity.com, making the world a better place, disponível em https://www.sourcesecurity.com/news/co-2232-ga.837.html, consultado a 1 de outubro de 2021.

[73] ONG, Thuy *"Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints".* The Verge, 2017, disponível em https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium, consultado a 1 de outubro de 2021.

[74] As imagens são captadas por câmaras espalhadas em pontos estratégicos e também acompanhadas em tempo real pelos agentes do Núcleo de Videopatrulhamento, que funciona no Centro de Operações Rio. Cfr. *"Prefeitura lança programa Rio+Seguro",* Prefeitura da Cidade do Rio de Janeiro, 2017, disponível em http://www.rio.rj.gov.br/web/guest/exibeconteudo?id=7505084, consultado a 1 de outubro de 2021.

Apesar disto, existem campanhas para se acabar com o reconhecimento facial dado que se trata de um ataque à privacidade das pessoas.[75]

Algo com que nos deparamos mais recorrentemente, é o uso de sistemas de reconhecimento facial nas redes sociais, como é o caso do Facebook, que permite aos utilizadores identificarem amigos nas suas fotos automaticamente, não sendo necessário introduzir manualmente a sua identificação.[76] Existe, ainda, o exemplo dos telemóveis em que para os desbloquear é necessário a identificação da pessoa titular através dos seus dados biométricos, do seu reconhecimento facial.

Conclui-se, portanto, que de uma maneira ou de outra já se faz uso destas tecnologias por todo o Mundo, contudo, de forma menos controversa através dos dispositivos tecnológicos, como é o caso dos telemóveis.

O Instituto *Ada Lovelace* realizou um estudo, tendo concluído que 70% das pessoas pensa que deveria ser permitido o uso do reconhecimento facial nas investigações criminais, sendo que a maioria (55%) apoia que o governo limite o uso a específicas circunstâncias, 54% admitiam o seu uso para sistemas de desbloqueio de dispositivos, 50% como substituto dos passaportes para uso nos aeroportos, 80% admite como sistema de policiamento pelo benefício que seria para a segurança da sociedade.[77]

A verdade é que esta tecnologia está em constante desenvolvimento e o seu uso em contante crescimento.

---

[75] Big Brother Watch, *"Stop Facial Recognition",* disponível em https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/, consultado a 27 de outubro de 2021.

[76] BUCKLEY, Ben, HUNTER, Matt*, "Say cheese! Privacy and facial recognition",* Computer Law & Security Review 27 (2011), Linklaters LLP., publicado por ELSEVIER, pp. 637-640, disponível em https://www.sciencedirect.com/science/article/pii/S0267364911001567, consultado a 17 de dezembro de 2021; SIMONITE, Tom, *"Facebook Can Now Find Your Face, Even When It's Not Tagged",* Wired, 19 de dezembro de 2017, disponível em https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/.

[77] ADA LOVELACE INSTITUTE, *"Beyond face value: public attitudes to facial recognition technology"* September 2019, disponível em https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/, consultado a 27 de outubro de 2021.

CAPÍTULO II
ADMISSIBILIDADE DA PROVA

1. Considerações Iniciais

É certo que a par com o desenvolvimento da IA houve um desenvolvimento probatório que trouxe consigo associado novas formas de investigação, contudo, o quadro legal tradicional mostra-se insuficiente, não estando reguladas as possíveis conflitualidades que estes desenvolvimentos vêm fazer surgir, principalmente relacionadas com a temática da privacidade.[78]

É certo que o processo penal tem como finalidades essenciais a realização da justiça e a descoberta da verdade material, a proteção perante o Estado dos direitos fundamentais das pessoas e, ainda, o restabelecimento da paz jurídica, porém, por vezes não é alcançável a harmonização destas.[79] Como pode acontecer, por exemplo, quando se fala em reconhecimento facial, podemos estar perante uma conflitualidade entre a descoberta da verdade material e a proteção dos direitos fundamentais, matéria esta particularmente sensível.[80]

Tendo em conta a dificuldade mencionada há que, segundo Figueiredo Dias, se "*operar a concordância prática das finalidades em conflito; de modo a que de cada uma se salve, em cada situação o máximo conteúdo possível, otimizando os ganhos e minimizando as perdas axiológicas e funcionais*"[81], isto é, deve proceder-se a uma "*mútua compressão das finalidades em conflito por forma a atribuir a cada uma a máxima eficácia possível*".[82]

Desta feita, perante uma situação de conflito o aplicador terá de efetuar, portanto, uma ponderação dos valores em conflito, optando pelo valor que se considere dominante, não rejeitando o outro, mas, pelo contrário, tentando salvar a sua efetividade na medida do possível.[83] Isto, após verificação de existência de lei que já realize esta ponderação e tendo

---

[78] RODRIGUES, Anabela Miranda, "*A Inteligência Artificial no Direito Penal* …", ob. cit., pp.11-13.
[79] ANTUNES, Maria João, "*Direito Processual Penal*", 2ª Edição, Almedina, 2019, ISBN 978-972-40-7350-7 p. 14.
[80] *Ibidem*, p.113.
[81] Dias, Jorge Figueiredo, "*O Novo Código de Processo Penal*", p. 13 *apud* ANTUNES, Maria João, "*Direito Processual Penal*", ob. cit., p. 15.
[82] DIAS, Jorge Figueiredo, "Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)", *in* Revista de Legislação e de Jurisprudência, Coimbra, ISSN 0870-8487. A 146, N.º 4000 (2016), p. 9.
[83] *Ibidem, p. 9-11*.

por base o limite absoluto da dignidade da pessoa humana[84], ou seja, nem sempre é possível proceder à concordância uma vez que é necessário respeitar o limite da dignidade da pessoa humana, tratando-se esta de um direito absoluto.[85]

Pelo que se deduz a necessidade de alcançar uma verdade "processualmente válida".[86]

O direito processual penal é verdadeiramente direito constitucional aplicado, assim como mencionado por Figueiredo Dias, uma vez que os fundamentos daquele são, concomitantemente, os alicerces constitucionais do Estado, deve conformar-se jurídico-constitucionalmente a regulamentação de particulares problemas processuais, o que, por vezes, passa pela restrição de direitos fundamentais, envolvendo o regime de restrição dos mesmos previsto na Constituição.[87]

O surgimento de novas tecnologias é, efetivamente, cativante para o processo penal, como mencionado *supra*, contudo, tendo em conta as conflitualidades entre as finalidades do processo penal, há que tentar alcançar a concordância prática entre estas, salvaguardando a efetividade dos bens em causa.[88]

De facto, quando se fala em reconhecimento facial estamos perante um confronto entre duas das finalidades do processo penal, de um lado, a descoberta da verdade material e, do outro, a proteção perante o Estado dos direitos fundamentais dos cidadãos. Acontece que a função primordial destes mecanismos tratar-se-ia de alcançar a verdade, a realidade dos factos, ou seja, estaríamos perante prova.[89] Contudo, é necessário refletir sobre a sua admissibilidade, reforçando a ideia de que a prova tem também um papel importante na garantia da realização de um processo justo, não se podendo alcançar a verdade através de

---

[84] *Ibidem*. No mesmo sentido vai o Ac. do TC n.º 607/2003, proc. n.º 594/03: "*deve afirmar-se que a validade de uma ponderação prudencial suscitada neste domínio, ainda que balanceando a tutela da intimidade com o contrapeso do premente interesse público na realização da justiça, não pode excluir a inviolabilidade inerente à dignidade da pessoa humana*", disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20030607.html.

[85] DIAS, Jorge Figueiredo, "Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal …", ob. cit., p. 13.

[86] DIAS, Jorge Figueiredo, "Direito Processual Penal I", Primeiro Volume, Coimbra Editora, 1974, p. 194.

[87] DIAS, Jorge Figueiredo, "Direito Processual Penal", Lições coligidas por Maria João Antunes, Secção de textos da Faculdade de Direito da Universidade de Coimbra, 1988-89, §3 *apud*, ANTUNES, Maria João, "Direito Processual Penal", ob. cit., pp. 16-18.

[88] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", ob. cit., p. 130.

[89] Sendo esta a função da prova, como se pode conferir pelo art. 341.º do CC.

meios ilícitos.[90] Tal como é referido por Amelung, quando nos diz que o Estado não pode recorrer a um ilícito criminal, caso contrário estaremos perante uma contradição que poderá comprometer a legitimação da pena que for aplicada.[91] Segundo o mesmo autor "*o sistema não pode superar os seus problemas à custa do desrespeito do valor autónomo da pessoa*."[92]

No que concerne à matéria da atividade probatória, podemos estar perante um meio de prova ou um meio de obtenção de prova, distinção esta cada vez mais difícil de se fazer. Para todos os efeitos, seguindo-se de perto a distinção feita por Germano Marques da Silva, sabe-se que os meios de prova são obtidos através dos meios de obtenção de prova, sendo através dos primeiros que se forma a convicção das autoridades judiciárias, uma vez que estes têm aptidão para fundamentar um juízo, enquanto os meios de obtenção de prova não são "*de per si fonte de convencimento, mas permitem obter coisas ou declarações dotadas de aptidão probatória*", "*a expressão de meios de obtenção de prova refere precisamente à actividade de recolha de meios de prova*".[93]

No que toca ao reconhecimento facial, a função desta tecnologia é auxiliar na identificação de uma pessoa, sendo que o resultado probabilístico que nos é oferecido por este mecanismo irá auxiliar as autoridades competentes a prosseguir a investigação, desta forma, crê-se que estamos perante um meio de obtenção de prova, pois ele, por si só não irá ser fonte de convencimento das autoridades judiciárias, nem fundamento de decisão judicial.

Em virtude da necessidade de melhor compreensão das tecnologias de reconhecimento facial, tem-se por fundamental, ainda, haver uma intervenção de um perito que, "*em virtude dos seus conhecimentos técnicos e científicos, encontrar-se-á em posição de produzir um juízo de valor em relação ao material probatório recolhido*", portanto, é necessário ser explicado o resultado obtido.[94]

---

[90] SILVA, Germano Marques da, "Curso de Processo Penal", Volume II, 4ª Edição, 2008, pp. 110-111; *"o direito processual penal num Estado de direito democrático, como o nosso (...) não se compadece com a realização da justiça e a descoberta da verdade material, a qualquer custo, pois estes fins para serem atingidos, como deve ser, têm de o ser através do respeito e a garantia dos direitos fundamentais da pessoa, com vista a alcançar a almejada paz jurídica. (...) Por tudo isto, o arguido não pode ser tratado como objecto"*, cfr. Ac. TRL de 03-05-2006, proc. n.º 872/2006-4, disponível em http://www.dgsi.pt/jtrl.nsf/0/2ee49abdddb1339480257 17f0042790b?OpenDocument.

[91] AMELUNG, *"Informationsbeherrschungsrechte"*, p. 22 *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", Gestlegal, 2ª edição, março 2022, p.17.

[92] AMELUNG, *Rechtsgüterschutz*, p.385 *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p. 124,

[93] SILVA, Germano Marques da, "*Curso de Processo Penal*", ob. cit., pp. 113.

[94] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 142.

Neste momento, já referido o modo de funcionamento das tecnologias de reconhecimento facial, as suas vantagens e problemas associados e a eventual necessidade de um perito para explicar o resultado probabilístico oferecido por estas, cabe agora prosseguir refletindo acerca da admissibilidade no processo penal.

2. Admissibilidade da atividade probatória

Como supramencionado, a obtenção da verdade material nunca pode ser à custa da dignidade do homem, daí existirem proibições de prova, que asseguram que a obtenção de prova não se faz através meios ilícitos, isto é, não se procura a verdade a todo o custo.[95] Desta feita, a descoberta da verdade material é limitada por um conjunto de regras legais, regras estas que confrontam a prova e que estão presentes no CPP, assim como em legislação extravagante.[96]

No que concerne à admissibilidade da prova, há que previamente se delimitar o objeto desta – *thema probandum* (art. 124.º do CPP)[97], devendo ser utilizadas técnicas e fontes de conhecimento idóneas e úteis à verificação deste[98], como nos é indicado pelo artigo 340.º do CPP, que consagra o princípio da investigação.[99]

Na verdade, o CPP oferece uma 'lista' de meios probatórios, acontece que, segundo o princípio da legalidade, previsto no art. 125.º do CPP, "são admissíveis as provas que não forem proibidas por lei", ou seja, a 'lista' de meios probatórios tipificados não é taxativa, sendo admissíveis outros, desde que não sejam proibidos, isto é, são admitidos meios

[95] DIAS, Figueiredo, "*Direito Processual Penal I*", ob.cit., p. 194; SILVA, Germano Marques da, "*Curso de Processo Penal*", ob. cit., pp. 110-111.
[96] SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", in Revista Portuguesa de Ciência Criminal, Ano 21, n.º4, 2011, Coimbra Editora, pp. 545-546. Na mesma obra, Sandra Oliveira e Silva refere que estas regras legais "*exprimem uma opção valorativa perante os interesses conflituantes, quer dizer, espelham a estrutura íntima do processo penal na multiplicidade dos seus princípios conformadores e condensam os cânones que a experiência histórica de dois séculos demonstrou serem indispensáveis para se pode afirmar a fiabilidade da prova*", p. 554.
[97] *Ibidem*, pp. 550-551.
[98] "não deverá estar em contraste com o acervo de conhecimentos lógicos e científicos da época histórica (*verosimilhança*)", cfr. *Ibidem*, p.552.
[99] De acordo com este "o tribunal ordena oficiosamente a produção de todos os meios de prova cujo conhecimento se lhe afigurar necessário à descoberta da verdade e à boa decisão da causa", assim como, "investiga o facto sujeito ou a sujeitar a julgamento, independentemente dos contributos da acusação e da defesa, construindo autonomamente as bases da sua decisão", cfr. ANTUNES, Maria João, "*Direito Processual Penal*", *ob. cit*., p. 171-172.

atípicos.[100] Como afirma Pedro Soares de Albergaria a "liberdade da prova tem assim um claro sentido de *abertura* do sistema", isto acontece porque não consegue antecipar todos os desenvolvimentos que poderão ter impacto na procura da verdade material, especialmente no que toca a desenvolvimentos técnico-científicos[101], o que não indica que sejam aceites todos os métodos científicos[102]. Este princípio deve ser entendido no contexto da estrutura acusatória do processo penal português (art. 32.º, n.º 5 da CRP), procurando a verdade material, "com respeito pela pessoa do arguido e pela validade epistemológica das provas".[103] Não se tomando o devido respeito pelo princípio da legalidade, em consequência considerar-se-ão nulas as provas obtidas por métodos proibidos, não se podendo utilizar estas (arts. 32.º/8 CRP e 126.º e 128.º CPP).[104]

No seguimento do que foi referido, *prima facie*, levar-nos-ia a pensar que uma vez que não é proibido por lei o reconhecimento facial, este seria admitido. Porém, para que possa ser admissível o seu uso, é necessário que se preencham certos requisitos, sendo estes: a "ausência de uma expressa proibição normativa" e a "falta de um meio probatório tipificado adequado a produzir o mesmo resultado cognoscitivo", "não deve confundir-se a liberdade de prova com uma completa fungibilidade" dos meios de prova e, ainda, ter em atenção que há meios de prova que são proibidos precisamente porque não estão previstos na lei.[105]

2.1. Os três corolários na admissibilidade da prova

O primeiro corolário trata-se da ideia de que a admissibilidade da prova atípica[106] pressupõe a "ausência de uma expressa proibição normativa", assim como "a falta de um

[100]SILVA, Germano Marques da, "*Curso de Processo Penal*", ob. cit., pp. 136-137; SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p. 560-562.
[101] ALBERGARIA, Pedro Soares de, "Artigo 125.º - Legalidade da Prova", *in:* Comentário Judiciário do Código de Processo Penal, tomo II, Coimbra: Edições Almedina, 2019, pp. 29-30.
[102] "Cuidados terão de tomar-se logo em tratando-se de novos métodos técnico-científicos", cfr. *Ibidem*, pp. 30-31.
[103] SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p. 562.
[104] ANTUNES, Maria João, "*Direito Processual Penal*", ob. cit., p. 174.
[105] SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., pp. 563-576, no mesmo sentido cfr. ALBERGARIA, Pedro Soares de, "Artigo 125.º - Legalidade da Prova", ob. cit., p.31.
[106] Isto é, instrumento probatório não previsto pelo legislador, cfr. SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p. 564.

meio probatório tipificado adequado a produzir o mesmo resultado cognoscitivo".[107] Isto é, estando prevista uma prova idónea a atingir o fim pretendido, deverá ser essa prova utilizada, não podendo optar-se por uma prova atípica. Concluindo, as autoridades judiciárias só podem recorrer a provas não tipificadas na falta de um meio probatório típico idóneo a produzir o resultado pretendido.[108] É isto que acontece, em regra, "nas situações em que o progresso tecnológico se adianta à capacidade de previsão do legislador".[109]

Por outro lado, o legislador não pré-determina os meios probatórios específicos para a demonstração dos factos, isto significa que a aquisição da prova não tem de ser feita mediante certos meios específicos de acordo com o facto que se pretende provar, existe liberdade para se escolher o meio probatório a utilizar.[110] No entanto, isto não significa que as autoridades judiciárias tenham total liberdade na escolha, havendo, inclusive, exceções em que a prova tem de ser feita por meios de prova específicos. Desta forma se vê que "a liberdade de meios de prova não deve confundir-se com uma completa "*fungibilidade*" das formas probatórias", pois é certo que há casos em que a comprovação de determinados factos tem de ser feita através de meios específicos.[111]

Para além dos supramencionados, temos ainda um terceiro corolário, que nos diz que há meios de prova que são proibidos precisamente porque não estão previstos e disciplinados na lei.[112] É o que, por norma, acontece com os meios que impliquem uma restrição de direitos fundamentais. Sendo, nestes casos, necessário haver uma lei que regule a restrição desses direitos, referindo, inclusive, os métodos admissíveis para a sua compressão.[113] Daqui se retira que não é por a Constituição não proibir um certo meio probatório que ele será considerado legítimo, portanto, fica vedado ao aplicador do direito a consideração de uma prova que restrinja de forma relevante os direitos fundamentais.[114] É de notar, que também se aplica aos meios de obtenção de prova inominados as "exigências constitucionais de reserva formal de lei restritiva".[115] Portanto, tratando-se de um meio inominado de obtenção de prova é necessário saber se existe um meio típico capaz de gerar

[107] Excertos retirados de SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p.563.
[108] *Ibidem*, p.569.
[109] *Ibidem*.
[110] *Ibidem*, p. 561.
[111] *Ibidem*, p. 570.
[112] ALBERGARIA, Pedro Soares de, "Artigo 125.º - Legalidade da Prova", ob. cit., p.31.
[113] *Ibidem*.
[114] *Ibidem*, pp.31-32.
[115] *Ibidem*.

um mesmo resultado, e não havendo temos de questionar se está em causa a constrição sensível de um direito fundamental. Contudo, há que ter em atenção que mesmo não estando em causa meios que restrinjam direitos fundamentais ou apenas o façam num grau mínimo, a admissibilidade destes está, também, condicionada.[116]

3. Proibições de Prova

Em virtude do conflito entre a finalidade da descoberta da verdade material e a da proteção dos direitos fundamentais, proíbem-se determinados meios de prova, de forma a preservar a dignidade da pessoa humana, à inobservância destes limites seguir-se-á a nulidade das provas obtidas com a consequente proibição de valoração destas.[117] Constituindo estas um verdadeiro limite à descoberta da verdade.[118] Nas palavras de Gössel são "barreiras colocadas à determinação dos factos que constituem objeto do processo". [119] Dizendo Rogall que se trata do "instrumento de defesa dos direitos individuais contra a actividade estadual de perseguição criminal".[120]

É, portanto, inegável que se trata de uma das áreas mais complexas e propensas a controvérsias, uma vez que em relação a esta muitas dúvidas se levantam.[121]

Ora, a regular esta matéria temos dois preceitos fundamentais, como é o caso do art. 32.º, n.º 8 da CRP e do art. 126.º CPP, nestes referem-se as provas proibidas tipificadas, que são as obtidas mediante tortura, coação, ofensa à integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas

[116] *Ibidem*, pp. 32-33.
[117] ANTUNES, Maria João, "*Direito Processual Penal*", ob. cit., pp. 15 e 174. Como referido por Pedro Soares de Albergaria, "*o respeito pela proibição é critério da verdade validamente adquirida no processo",* cfr. ALBERGARIA, Pedro Soares de, "Artigo 126.º - Métodos Proibidos de Prova", *in:* Comentário Judiciário do Código de Processo Penal, tomo II, Coimbra: Edições Almedina, 2019, p.38.
[118] Sendo estes "limites intransponíveis à prossecução da verdade em processo penal", cfr. ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.87 e 123.
[119] GÖSSEL, "*Bockelmann-Fs*", p.801 e, do mesmo autor "*NJW*" 1981, p.649 e "*Strafverfahrensrecht*", II, p.95 *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.87 e 123.
[120] ROGALL, "*NStW*" 1979, p. 9, *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p. 35.
[121] ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", *in* Revista Jurídica da Universidade Portucalense, N.º 13 (2008), ISSN 0874-2839, p. 143.

telecomunicações sem o consentimento do respetivo titular.[122] Tendo o legislador constitucional chamado a si "*a conformação normativa e directa dos aspetos mais decisivos da tramitação, em que avulta com particular destaque a disciplina dos métodos proibidos de prova.*"[123]

Como referido *supra*, neste regime jurídico está em causa a tutela dos direitos fundamentais, em especial, a dignidade da pessoa humana, contrapondo estes com a descoberta da verdade, isto é, "com as instituições basilares do Estado de direito democrático."[124] Portanto, a Constituição tutela os direitos fundamentais impondo-os às instâncias de processo penal, emergindo como a "fonte normativa privilegiada das proibições autónomas de valoração".[125]

Estando em causa os direitos fundamentais, fala-se obrigatoriamente da dignidade da pessoa humana (previsto no art. 1.º da CRP), assim como, na integridade moral (art. 25.º da CRP).[126] A verdade é que a dignidade da pessoa humana[127] é, como acentua Costa Andrade, um valor "irredutível, indisponível, e subtraído a toda a forma de ponderação, relativização ou funcionalização".[128] Não se desatendendo, contudo, aos demais direitos fundamentais, em especial, direitos, liberdades e garantias, como é o caso do direito à imagem, à reserva da intimidade da vida privada, entre outros.[129] A verdade é que, como

[122] As proibições de prova estão consagradas também em legislação internacional, como é o caso da DUDH, nos seus artigos 5.º e 12.º, na CEDH, nos seus artigos 3.º e 8.º e, ainda, no PIDCP, no seu artigo 7.º.
[123] SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p. 576-577.
[124]ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", ob. cit., p. 143. Segundo o mesmo autor, na mesma obra, trata-se de "*instrumentos de garantia e tutela de valores ou bens jurídicos distintos – e contrapostos – dos representados pela procura da verdade e pela perseguição penal*", p.203.
[125] ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", ob. cit., p.144.
[126] ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.14-15.
[127] "Valor supremo da axiologia constitucional", cfr. ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", ob. cit., p.144.
[128] *Ibidem*. No mesmo sentido Wolter refere que "*em todos os casos que contendam com a dignidade humana, não poderão ser chamados à ponderação os interesses por uma justiça penal eficaz. Quem o fizesse não tomaria a sério nem a inviolabilidade da dignidade humana nem um processo penal vocacionado para a protecção dos direitos fundamentais. Pois, nas situações de criminalidade mais grave, uma tal ponderação de interesses redundaria sistematicamente na frustração da tutela dos direitos fundamentais*", "*a procura da verdade material e de uma decisão justa, os esforços pela punição e reparação dos danos não são apenas relativizados pela garantia da dignidade humana, mas por ela inteiramente bloqueados*", cfr. WOLTER, "*Aspekte",* p.26 e 23, *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal",* ob. cit., p.40.
[129] ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.16.

refere Figueiredo Dias deve dar-se predominância absoluta à garantia da dignidade da pessoa humana, uma vez que não é possível qualquer transação com este valor.[130]

É também pertinente referir que o catálogo das proibições de prova não é taxativo, sendo que poderão ser reconhecidas novas proibições.[131]

4. Considerações Finais

Atualmente, com o desenvolvimento da IA e a sua utilização no domínio da prova foram criadas novas formas de processar e analisar informação, como é o caso do reconhecimento facial.[132] Nesta senda, torna-se importante a análise da sua possível utilização pelo processo penal português.

Em primeiro lugar, há que notar a completa ausência de lei no que toca aos mecanismos de reconhecimento facial, o que *prima facie*, segundo o primeiro corolário levaria a que se pensasse que não estando proibida, seria, à partida admissível. Não estando, também, previsto outro meio idóneo a produzir o resultado proposto por estes mecanismos. Assim sendo, da análise do exposto no presente capítulo conclui-se que quando a prova intervenha com direitos fundamentais é necessário a sua "legitimação legal".[133] Tendo-se por proibida, precisamente porque não está prevista.

Apesar de não haver lei que proíba expressamente a prova através de mecanismos de reconhecimento facial, existem leis que referem a captação e tratamento de dados biométricos, como é o caso da Lei n.º 95/2021 de 29 de dezembro[134], no entanto, de acordo com esta "não é permitida a captação e tratamento de dados biométricos".[135] Os dados

---

[130] Figueiredo Dias, "*Para uma reforma*", p.207 *apud A*NDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., pp. 124-125.
[131] SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p.589.
[132] DUPONT, Benoît, STEENS, Yuan, WESTERMANN, Hannes, JOYCE, Michael, "*Artificial Intelligence in the Context of Crime and Criminal Justice",* Korean Institute of Criminology – International Center for Comparative Criminology, 2018, p.67,86 e ss. *apud* FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 131,
[133] Como se pode comprovar pelo preceituado no art. 34.º, n.º4 que confia ao legislador ordinário a conformação definitiva da proibição, cfr. ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p. 24 e 27.
[134] Esta Lei veio regular a 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, revogando a Lei n.º 1/2005 de 10 de janeiro que regulava a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum.
[135] Art. 16.º Lei n.º 95/2021, de 29 de dezembro.

biométricos são, ainda, referidos pela Lei 59/2019, de 8 de agosto[136], que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais. Esta é aplicada ao tratamento de dados pessoais[137] por meios automatizados, fazendo referência à possibilidade de utilização de dados biométricos para identificação no seu art. 6.º, dizendo que só pode ser efetuado o tratamento destes se for estritamente necessário e se se garantir a proteção dos direitos e liberdades do titular dos dados, sendo necessário autorização da lei, que proteja os interesses vitais do titular dos dados ou de outra pessoa singular e, ainda, tem de estar relacionado com dados manifestamente tornados públicos pelo titular dos dados.

É justamente neste contexto de ausência de lei que se discute a possibilidade da utilização de mecanismos de reconhecimento facial como meio de obtenção de prova. Poderá vir a ser regulado este uso? Ou, pelo contrário, levaria a uma restrição inadmissível dos direitos fundamentais?

Ou seja, quando estão em causa os direitos fundamentais, assim como o surgimento de novas formas de agressão aos mesmos devido ao progresso tecnológico, é fulcral a existência de uma lei que legitime a sua utilização.[138] Ou seja, uma restrição destes no âmbito da descoberta da verdade material está sempre dependente de intervenção legislativa.[139]

Efetivamente estes desenvolvimentos tecnológicos no âmbito da IA aplicados ao meticuloso campo da obtenção de prova no processo penal, trazem inúmeras vantagens como já expostas e analisadas no presente estudo, contudo, o recurso às mesmas gerará um impacto nefasto nos bens jurídicos penais protegidos configurando uma ofensa aos mesmos, como será agora aludido e explanado.

---

[136] Transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
[137] Art. 3.º, al. c): "«Dados pessoais», informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»)".
[138] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*", *apud* SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p. 590.
[139] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*", a reforma do Código de Processo Penal. Observações críticas sobre uma lei que podia e devia ter sido diferente, Coimbra: Coimbra Editora, 2009, p.149, 150 e 157 *apud* FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 141.

CAPÍTULO III
DIREITOS FUNDAMENTAIS

1. Considerações Iniciais

É inegável a importância de uma análise dos direitos fundamentais para se indagar da possibilidade de o nosso sistema processual penal admitir o uso de tecnologias de reconhecimento facial.

A verdade é que, como menciona Anabela Miranda Rodrigues a "*investigação criminal é tradicionalmente uma área de conflito por excelência entre perseguição penal e direitos fundamentais das pessoas (…), mas os desafios que o progresso tecnológico atual coloca são, em muitos casos, de dimensão difícil de alcançar*".[140]

Assim se percebe que é necessário atentar sobre os desenvolvimentos tecnológicos na área da IA, especialmente relacionados com o reconhecimento facial, e o impacto que podem ter sobre os direitos fundamentais.[141]

Acontece que, tendo em conta os imperativos de legalidade e de reserva de lei, e como já mencionado *supra*, só pode haver uma intromissão nos direitos fundamentais pelas instâncias do processo penal "na medida em que o legislador ordinário o tiver consignado".[142]

Ora, quando se refere direitos fundamentais, estes "são os direitos do homem, jurídico-institucionalmente garantidos e limitados espácio-temporalmente (…) seriam os direitos objetivamente vigentes numa ordem jurídica concreta"[143].

---

[140] RODRIGUES, Anabela Miranda, "*A Inteligência Artificial no Direito Penal*", ob. cit., p.16

[141] *Ibidem*, p.30, na mesma obra, Anabela Miranda Rodrigues refere que se trata "*de submeter a utilização de instrumentos algorítmicos e de IA ao filtro dos direitos fundamentais, para efeitos de enquadramento legal, a nível europeu, da sua entrada nos ordenamentos jurídicos nacionais processuais penais*", p.31

[142] ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", ob. cit., p. 147; "não há dúvida de que o princípio da investigação ou da verdade material, sem prejuízo da estrutura acusatória do processo penal português, tem valor constitucional", cfr. Ac. do TC n.º 137/02, Proc. n.º 363/01, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20020137.html.

[143] CANOTILHO, J.J. Gomes, "*Direito Constitucional*", 6ª edição revista, Livraria Almedina, Coimbra, 1993, p. 517. O conceito de direitos fundamentais é material e aberto, como se pode inferir do art. 16.º da CRP, cfr. CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 16.º*", *in*: Constituição da República Portuguesa Anotada, Vol. I, 3ª edição, Coimbra Editora, 2007, p.365. No mesmo sentido, MEDEIROS, Rui e CORTÊS, António, "Artigo 16.º", *in*: Constituição da República Portuguesa Anotada (Jorge Miranda/Rui Medeiros), Universidade Católica Editora, 2017, p.215. Existindo, portanto, direitos fundamentais fora do catálogo da Constituição, assim como direitos sem assento constitucional, cfr. CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Fundamentos da Constituição*", Coimbra Editora, 1991, pp. 114-117.

Posto isto, neste momento, serão abordados, por uma questão de objeto de estudo, apenas os direitos fundamentais mais implicados pelas tecnologias de reconhecimento facial.

Não se pode negar, as vantagens que estas proporcionam, auxiliando as autoridades competentes na procura pela verdade material, assim como, poderá ter um efeito de prevenção da criminalidade. Contudo, certo é que a utilização de tecnologias de reconhecimento facial restringe necessariamente direitos fundamentais, sendo inevitável que aquelas afetem estes.

2. Breve análise aos direitos fundamentais implicados pelo reconhecimento facial

Acontece que, se se pretende utilizar as tecnologias de reconhecimento facial, apesar das suas vantagens para a realização da justiça e para a descoberta da verdade material, estará em causa, uma restrição ao direito à reserva da intimidade da vida privada e familiar, assim como, já tendo sido referido por Costa Andrade "a revolução científico-tecnológica trouxe consigo a massificação de meios sem precedentes de devassa".[144] O direito em questão está previsto art. 26.º da CRP e nos arts. 190.º a 194.º do CP, e ainda, com consagração no art. 80.º CC.

Trata-se, no fundo, de um direito ao respeito pela vida privada[145], englobando tanto "o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar", assim como, "o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem".[146]

Estamos, portanto, perante um bem jurídico pessoal que assegura "ao indivíduo o domínio sobre a sua esfera privada e, por vias disso, um espaço de isolamento e auto-determinação resguardado contra as intromissões e injunções da sociedade e do Estado".[147]

---

[144] ANDRADE, Manuel da Costa, "*Artigo 192.º (Devassa da vida privada)*", *in*: Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, 1999, p. 726.

[145] MEDEIROS, Rui e CORTÊS, António, "*Artigo 16.º*", ob. cit. p. 452.

[146] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 467. Rui Medeiros e António Cortês definem este direito como "o direito de oposição à divulgação da vida privada", assim como "o direito ao respeito da vida privada, ou seja, o direito de oposição à investigação sobre a vida privada", cfr. MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 452.

[147] ANDRADE, Manuel da Costa, "*Artigo 192.º (Devassa da vida privada)*", ob. cit., p.727.

A demarcação deste domínio, ou seja, do que pertença a esta reserva, suscita grandes dificuldades, tendo sido elaboradas já diversas teorias. Apesar de inúmeras críticas, tem sido, inclusive pelo Tribunal Constitucional, usada a teoria das três esferas, "na sua versão gradualista, e com terminologia variada", segundo esta existe a esfera íntima, isto é, onde está o núcleo duro do direito, reconhecida a todas as pessoas e sendo inviolável[148], nas palavra de Costa Andrade trata-se da "barreira intransponível à (…) prova da verdade dos factos"[149]; a esfera privada, que admite ponderações de proporcionalidade; e a esfera social, sendo que nesta se está no quadro do direito à imagem e não do direito à intimidade da vida privada.[150]

Segundo Gomes Canotilho e Vital Moreira, que não se apoiam na teoria acabada de referir, consideram que o âmbito deste direito deve fazer referência apenas a três aspetos, sendo estes o respeito dos comportamentos, do anonimato e o respeito da vida em relação.[151]

É de notar, com particular importância, que este direito não se reporta apenas a situações ocorridas no domicílio, englobando também, factos ocorridos em locais públicos[152], ou seja, o âmbito deste direito é bastante vasto. [153]

Pelo exposto, sabe-se que não estamos perante um direito absoluto, inelimitável[154], sendo, muitas vezes, necessária a sua limitação para se alcançar a descoberta da verdade

---

[148] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., pp. 452-453.
[149] ANDRADE, Manuel da Costa, "*Artigo 192.º (Devassa da vida privada)*", ob. cit., pp. 729-730.
[150] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 452. Para uma melhor distinção, J.J. Gomes Canotilho, citando o parecer n.º 121/80 da PGR, refere que «*intimidade é o restrito espaço pessoal subtraído "à curiosidade pública por naturais razões de resguardo e melindre"»* e a vida privada será "*aquele conjunto de atividades, situações, atitudes ou comportamentos individuais que, ao tendo relação com a vida pública (privado entendido como separado de coisa pública), respeitam estritamente à vida individual e familiar da pessoa*", cfr. CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 468.
[151] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 468.
[152] RABINDRANATH, Capelo de Sousa, "*O Direito Geral de Personalidade*", pp.317 e ss., *apud* MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 453, segundo estes, o direito à reserva da intimidade da vida privada e familiar "*abrange não só o respeito da intimidade da vida privada, em particular a intimidade da vida pessoal, familiar, doméstica, sentimental e sexual e inclusivamente os respetivos acontecimentos e trajetórios, mas ainda o respeito de outras camadas intermédias e periféricas da vida privada, como as reservas do domicílio e de lugares adjacentes, da correspondência e de outros meios de comunicação privada, dos dados pessoais informatizáveis, dos lazeres*", bem como "*dos rendimentos patrimoniais e de demais elementos privados da atividade profissional e económica",* pp.453-454.
[153] "a privacidade não é um espaço material estabilizado e fixo, na medida em que existe uma relatividade histórico-cultural da privacidade, isto é, a oscilação das fronteiras entre o privado e o público ao ritmo das transformações civilizacionais", cfr. AC. STJ 28-09-2011, Proc. n.º 22/09.6YGLSB.S2, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25cd7aa80cc3adb0802579260032dd4a?OpenDocument.
[154] Como se pode comprovar, por exemplo, pelo art 34.º da CRP, cfr. MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 452.

material, contudo, esta situação levanta problemas específicos[155], sendo que se deve partir da ideia de que a limitação tem de ser alcançada "lealmente, pelo engenho e arte", e não por meios inconstitucionais[156], sendo, por exemplo, um limite à matéria de obtenção de provas[157], como se comprova pelo art. 32.º, n.º 8 da CRP e pelo art. 126.º, n.º 3 do CPP, podendo, como referido *supra*, levar à nulidade da prova obtida.

Qualquer restrição a este direito deverá respeitar o princípio da dignidade da pessoa humana e da proporcionalidade, tendo de ser ponderado o nível de intimidade dos dados, para que não se trate de uma intromissão abusiva, que levará a uma proibição de prova.[158] Tratar-se-á de uma intromissão abusiva quando efetuada "fora dos casos previstos na lei e sem intervenção judicial (art. 34º-2 e 4), quando desnecessária ou desproporcionada ou quando aniquiladora dos próprios direitos" (art. 18.º, n.º2 e 3 da CRP)[159], juízo este cada vez mais complexo de se realizar, principalmente com o surgimento de variados meios tecnológicos de obtenção de prova, dependendo este "da adequada ponderação da diversidade de situações em que o problema se coloca e da própria condição das pessoas".[160]

Ou seja, contendendo com a reserva absoluta de pessoalidade, sacrifica-se os interesses da prossecução da justiça penal.[161]

Assim como também, e neste sentido refere Schäfer, como já foi supramencionado, pode haver um recuo do primado da esfera íntima perante as necessidades da justiça criminal, isto à luz do princípio da proporcionalidade.[162] Ou seja, encontramo-nos perante um confronto, como referido por Kleinknecht, entre por "*um lado, o interesse da perseguição criminal encabeçado pela comunidade jurídica ofendida e tendo na devida conta o significado da matéria criminal; e, do outro lado, a ideia de justiça e o imperativo de um processo conforme às exigências de justiça*".[163]

---

[155] CANOTILHO, José Joaquim Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., pp. 468-469; MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., pp. 452-453.
[156] Excerto retirado de MEDEIROS, Rui e CORTÊS, António, "*Artigo 32.º*", ob. cit., pp.534-535.
[157] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 455.
[158] *Ibidem*, p. 453
[159] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 524.
[160] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 454.
[161] Ideia esta reforçada pelo Ac. Do TC, n.º 607/2003, de 8 de abril, Proc. n.º 594/03 que nos mostra que "os interesses gerais da investigação e da prossecução da justiça penal terão de ser sacrificados sempre que contendam com esta reserva absoluta de pessoalidade… nunca a inevitável compressão/ingerência na esfera da privacidade poderá sacrificar a dignidade da pessoa e/ou redundar no total aniquilamento desse direito fundamental", disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20030607.html.
[162] ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.34.
[163] KLEINKNECHT, "*NJW*" 1966, p.1543 *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., pp.34-35.

As questões cruciais que se colocam são: é admissível uma intromissão neste direito para prosseguir um interesse de investigação? Como também questionado por Sónia Fidalgo, "Com a aplicação das técnicas de inteligência artificial neste âmbito ganhamos em eficácia na luta contra o crime; alcançaremos, porém, uma *melhor* justiça penal?"[164]

A este respeito o Ac. do TRL de 10-05-2016 dispõe que "*vem a jurisprudência entendendo que quando as filmagens estão enquadradas em lugares públicos e visem a realização de interesses públicos, designadamente prevenção criminal, existe justa causa nesse procedimento, até por exigências de eficiência da justiça, o que afasta a ilicitude da sua captação, tanto mais que não são atingidos dados sensíveis da pessoa visionada, que é vista a circular em local público.*"[165] No entanto, no caso em questão fala-se em dados sensíveis, em dados pessoais, o que coloca, portanto, uma entrave ao uso das tecnologias de reconhecimento facial, uma vez que pode haver uma abusiva intromissão na reserva da vida privada, mesmo esta se justificando com o facto de que se visa a realização da justiça e a descoberta da verdade material.

Abrangido pelo âmbito de proteção deste direito temos a proibição de tratamento informático de dados referentes à vida privada (art. 35.º, n.º 3)[166], segundo este cada indivíduo dispõe livremente dos seus dados pessoais, determinando as condições de acesso e utilização destes por terceiros, podemos falar, verdadeiramente, de um direito à autodeterminação informacional.[167] A proteção contra o tratamento informático de dados analisa-se fundamentalmente em três direitos: "direito de acesso das pessoas aos registos informáticos para conhecimento dos seus dados pessoais deles constantes", a sua retificação e complementação; "direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão"; "direito ao não tratamento informático de certos tipos de dados".[168] Sendo que a informatização de direitos pessoais tem de obedecer a certos princípios como o da publicidade, a justificação social, isto é, a criação de bases de dados deve ter um objetivo geral e usos específicos

---

[164] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 132.

[165] Ac. do TRL de 10-05-2016, Proc. n.º 12/14.7SHLSB.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/358ab50ffb6b524a80257fe8002e11e0?OpenDocument.

[166] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., pp. 467-468; MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 452.

[167] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 452.

[168] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 35.º*", *in*: Constituição da República Portuguesa Anotada, Vol. I, 3ª edição, Coimbra Editora, 2007, p. 551.

socialmente aceites, a transparência, a especificação de finalidades e a limitação de recolha que deve ser feita por meios lícitos, princípio da fidelidade, isto é, os dados devem ser exatos, completos e atuais; a limitação da utilização, isto é, utilizados apenas para o que foram propostos, garantias de segurança, responsabilidade, isto é, deveres legais e deontológicos aos responsáveis pelos dados, princípio da política de abertura, princípio de limitação no tempo.[169]

Assumem aqui especial importância os dados biométricos, colocando, no entanto, questões de informação, confiança e proporcionalidade.[170] Ou seja, é necessário ter presente o risco da utilização de meios informáticos para os direitos fundamentais[171], tendo o Estado que "tomar medidas legislativas para a realização plena da autodeterminação da pessoa em face do uso da informática".[172]

Daqui há que concluir que, em primeiro lugar, para se recolherem dados é necessária uma finalidade constitucionalmente legítima, ser idónea e necessária para essa finalidade, não existindo outra medida menos penosa para obter o mesmo resultado, sendo ainda proporcional, evitando-se uma recolha injustificada destes que pode constituir uma intromissão ilegítima na vida privada das pessoas, evitando-se, ainda, que se obtenha facilmente informação sobre todos os movimentos da pessoa e costumes, "todos os espaços mais recônditos da sua vida privada e pessoal". Este direito pode ainda ser alvo de restrições, principalmente quando está em causa a investigação criminal, como se pode comprovar pela LPDP.[173]

Acontece que, tendo em conta o disposto, percebe-se a severidade da intromissão destas tecnologias neste direito fundamental, uma vez que, desta forma se permite o acesso a grandes quantidades de dados, tratando-se estes de dados biométricos, dados pessoais.

Desta feita é difícil contrariar a prova obtida através destes devido à "opacidade que envolve os sistemas de inteligência artificial (…) pondo-se, assim, em causa, o exercício do direito de defesa do arguido".[174]

---

[169] *Ibidem*, pp.552-553.
[170] FARIA, Maria Paula Ribeiro de "*Artigo 35.º*", *in* Constituição da República Portuguesa Anotada (Jorge Miranda/Rui Medeiros), Universidade Católica Editora, 2017, p. 570.
[171] *Ibidem*, p. 571.
[172] *Ibidem*, p.572.
[173] *Ibidem*, pp. 571-575.
[174] FIDALGO, Sónia, *"A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo",* ob. cit., p. 131-132. Relativamente ao direito de defesa esta será abordado mais à frente neste capítulo.

Na utilização de tecnologias de reconhecimento facial é necessário que haja em formato digital uma base de dados com fotografias e os respetivos dados biométricos das pessoas retratadas nas fotografias, fotografias estas disponíveis para se proceder à comparação. Desta forma, se percebe como estas tecnologias estão intrinsecamente ligadas a este direito fundamental. A questão é, poderá limitar-se este direito para uso de tecnologias de reconhecimento facial e, consequentemente, para a descoberta da verdade material?

Por outro lado, o direito à imagem também se revela crucial para a reflexão a que nos propomos, tratando-se este de um bem "*jurídico-penal autónomo, tutelados em si e de per si, independentemente da sua valência do ponto de vista da privacidade/intimidade*"[175], bem jurídico este que é eminentemente pessoal, reconhecendo-se à pessoa o domínio sobre a própria imagem.[176]

Este encontra-se previsto no art. 26.º da CRP, no art. 79.º do CC e no art. 199.º, n.º 2 CPP e trata-se do direito de não ser fotografado ou filmado, de não ter o seu retrato divulgado sem o seu consentimento[177], "*direito a não ver as expressões da sua personalidade distorcidas, o que inclui o direito a que, sem consentimento, a imagem não seja alterada em montagens fotográficas ou as palavras adulteradas ou indevidamente descontextualizadas em textos ou gravações. Numa palavra: as imagens e palavras devem ser divulgadas com rigor e autenticidade*".[178]

Quando se fala no direito à imagem, é necessário ter-se em atenção que em causa, não está apenas a captação da fotografia ou gravação, mas também a sua utilização.[179] Tendo cada pessoa o direito de autodefinir a utilização ou não da sua própria imagem, inclui-se neste direito um "direito à autodeterminação da imagem exterior".[180] Orlando de Carvalho fala no "*direito ao não conhecimento por outrem da sua própria imagem física: no que se inclui decerto o retrato, mas se incluem igualmente todas as outras captações possíveis do corpo do indivíduo, da sua projeção imagética*".[181]

---

[175] ANDRADE, Manuel da Costa, *"Artigo 199.º (Gravações e Fotografias Ilícitas)",* in Comentário Conimbricense do Código Penal: parte especial, dir. Jorge de Figueiredo Dias, Tomo I, 2ª Edição, Coimbra: Coimbra Editora, 2012, p.1196.
[176] *Ibidem,* p. 1199.
[177] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 467. No mesmo sentido MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 451.
[178] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p.451.
[179] ANDRADE, Manuel da Costa, *"Artigo 199.º (Gravações e Fotografias Ilícitas)",* ob. cit., p.1213.
[180] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p.451.
[181] *Teoria Geral, pág 72 apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.276.

A verdade é que este não se trata de um direto absoluto, podendo, também ele, ser limitado, no entanto, apenas em "função de contextos específicos"[182], sendo que este se trata de uma expressão típica "de autonomia pessoal constitucionalmente garantida por força do princípio da dignidade humana".[183]

Adverte-se para o facto de que a fotografia captada e/ou utilizada apenas assume relevo quando permita a identificação da pessoa fotografada, quando a pessoa fotografada possa ser identificável, reconhecível.[184] Assim sendo, é preciso atentar ao facto de a imagem captada num espaço público, dissolvendo-se neste, se distinguir daquela que apesar de tirada nesse espaço destaca a imagem pessoal, individualizando a pessoa em questão, deixando esta de ser anónima.[185]

Outro direito importante aqui, uma vez que um dos riscos das tecnologias de reconhecimento facial é o risco da discriminação, é o direito à proteção legal contra qualquer forma de discriminação, que se encontra previsto no art. 26.º da CRP, devendo ser lido em articulado com o art. 13.º da CRP. Este direito reconduz-se à prática de não discriminação (dimensão subjetiva) e à efetivação e promoção de exigência de igualdade de tratamento (dimensão objetiva), isto é, exigência de proteção.[186] Ou seja, existe um dever de estabelecer medidas legislativas adequadas e proporcionadas a combater situações intoleráveis de discriminação.[187]

Relativamente a este direito, não se alongará o seu estudo, sendo apenas pertinente referir, assim como supramencionado no Capítulo I da presente dissertação, que, uma vez que as tecnologias de reconhecimento facial podem levar a resultados errados, principalmente quando se fala em raças ou géneros diferentes, é necessário tomar em atenção esta tendência discriminatória[188], assim sendo existe aqui uma exigência de se tomar as medidas adequadas a prevenir esta tendência.

Convém ainda referir que a utilização das tecnologias em causa leva a uma restrição também ao direito de reunião e manifestação, trata-se de direito negativos, implicando estes

---

[182] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p.451.
[183] *Ibidem,* p.450.
[184] ANDRADE, Manuel da Costa, *"Artigo 199.º (Gravações e Fotografias Ilícitas)",* ob. cit., pp. 1213-1214.
[185] *Ibidem,* p.1215.
[186] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 469-470.
[187] MEDEIROS, Rui e CORTÊS, António, *"Artigo 26.º",* ob. cit., p.459.
[188] Como refere Anabela Miranda Rodrigues, "se os sistemas computacionais podem detetar a existência de discriminação, também é certo que sofrem do risco de introduzir *implicit bias*, por exemplo se o *input* não é completamente neutro", cfr. RODRIGUES, Anabela Miranda, "*A Inteligência Artificial no Direito Penal*", ob. cit., p.34.

a não interferência do Estado.[189] Fala-se em restrição a este uma vez que as pessoas, por receio de serem identificadas por participarem, por exemplo, em manifestações, deixam de o fazer, deixam de se mover e agir livremente.

Constitucionalmente previstas estão também garantias de processo criminal, no art. 32.º, referindo-se, especialmente, ao direito de defesa. Ora, dúvidas se colocam se o arguido conseguirá exercer o contraditório sendo que não tem acesso ao algoritmo utilizado, uma vez que, primeiro precisará perceber de que forma este foi desenvolvido e o processo até chegar àquele resultado para depois conseguir exercer o seu contraditório (*vide*, art. 327.º, n.º 2 do CPP).[190]

Ou seja, mostra-se a necessidade da transparência destes sistemas, o que muitas vezes não acontece, tendo em conta que são criadas por empresas privadas, sendo que só ela possui o *know how*.[191] Isto é, o arguido só pode contrariar a prova se tiver acesso a informação de carácter técnico, daí os sistemas terem de ser explicáveis e transparentes.[192] Só assim se "permitirá alcançar o equilíbrio entre os interesses da investigação e a proteção do direito de defesa do arguido"[193], como nos refere Anabela Miranda Rodrigues "a Carta sublinha a ideia de que a solução para o equilíbrio de interesses aqui em jogo passa pela «completa transparência técnica», acompanhada pela explicação do sistema computacional em linguagem acessível e clara".[194] Conclui-se assim que "a complexidade e a opacidade que caracterizam certos sistemas de inteligência artificial podem pôr em causa, ainda, o direito de defesa do arguido".[195]

3. Restrição dos direitos fundamentais

[189] MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", ob. cit., p. 686.
[190] PEREIRA, Rui Soares, "*A inteligência artificial e modelos de prova*", *in*: Inteligência Artificial & Direito, coord.: Manuel Lopes Rocha e Rui Soares Pereira, colaboração de Ana Coimbra Trigo, Edições Almedina, S.A., 2020, ISBN 978-972-40-8262-2, pp. 65-75 (em particular p.75).
[191] RODRIGUES, Anabela Miranda, "*A Inteligência Artificial no Direito Penal*", ob. cit., p.25.
[192] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 145, desta forma refere que "Devem ser criadas ferramentas que permitam ao arguido contraditar a prova, designadamente, proporcionando-se acesso aberto ao código fonte, criando-se mecanismos de certificação dos sistemas e explicando-se o sistema em linguagem clara, indicando-se, por exemplo, as ferramentas utilizadas".
[193] *Ibidem*, p. 146.
[194] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal", ob. cit., p.35
[195] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p.137.

Chegando aqui, há que repristinar o Capítulo I de forma a se perceber melhor a dimensão dos problemas existentes com a utilização de tecnologias de reconhecimento facial. Portanto, para a realização da justiça, para a descoberta da verdade material, através da utilização de tecnologias de reconhecimento facial, inevitavelmente tem de se restringir os demais direitos, isto é, o direito à reserva da intimidade da vida privada, o direito à autodeterminação informacional, o direito à imagem, o direito de reunião e manifestação, entre outros.

E facilmente se percebe como, passando a explicar, a verdade é que, com a utilização destas tecnologias, poderá haver uma intromissão na reserva de intimidade da vida privada, nos moldes atrás mencionados, sendo que esta intromissão pode ocorrer em espaços públicos; no direito à autodeterminação informacional, uma vez que estas tecnologias recolhem os dados biométricos, ou seja, dados pessoais, armazenam-nos e, posteriormente, comparam-nos; o direito à imagem, pois estes mecanismos captam a imagem da pessoa sem qualquer consentimento da mesma, procedendo ao armazenamento da sua imagem; e, relativamente aos direitos de manifestação e reunião, entende-se que, as pessoas, uma vez que facilmente identificadas, não participem em reuniões e manifestações com medo de serem identificadas e haver represálias, acabando por mudar os seus hábitos de forma a evitar que se proceda à sua identificação.

Ora, no que diz respeito ao processo penal não se pode olvidar de que se encontra limitado tanto pela dignidade humana, prevista no art. 1.º da CRP, como pelos princípios fundamentais.[196] Estando o Estado obrigado, para além de não poder violar estes direitos, também tem de instituir mecanismos que impeçam a violação destes.[197]

A verdade é que estamos perante direitos fundamentais que não são absolutos, podendo ser limitados[198], restringidos, excecionando os casos previstos na Constituição.

Acontece que esta restrição, como já referido, só pode ter lugar por via da lei, como previsto no art. 18.º, n.º2, 1ª parte da CRP, para salvaguardar outro direito fundamental ou interesse constitucionalmente protegido, previsto na 2ª parte do mesmo preceito, ademais, a medida restritiva tem de se sujeitar ao princípio da proibição do excesso/princípio da

[196] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", ob. cit., p. 524.
[197] *Ibidem*, p. 471.
[198] ANDRADE, José Carlos Vieira de, "*Os Direitos Fundamentais na Constituição Portuguesa de 1976*", 5ª edição, Almedina, 2012, p.263

proporcionalidade em sentido amplo, constituído por três dimensões: necessidade, adequação e proporcionalidade em sentido estrito, de forma a que se limite apenas ao necessário.[199] Estas leis restritivas têm, ainda, de revestir um carácter geral e abstrato, estando vinculadas ao princípio da salvaguarda do conteúdo essencial dos preceitos constitucionais garantidores de direitos, liberdades e garantias, como previsto no n.º3 do preceito constitucional referido.[200]

Desta feita, torna-se necessário definir o que é este núcleo essencial, segundo Vieira de Andrade "*corresponde às faculdades típicas que integram o direito, tal como é definido na hipótese normativa, e que correspondem à projeção da ideia de dignidade humana individual na respetiva esfera da realidade – abrangem aquelas dimensões dos valores pessoais que a Constituição visa em primeira linha proteger e que caracterizam e justificam a existência autónoma daquele direito fundamental*".[201]

Ora, o princípio da dignidade do homem constitui a base dos direitos fundamentais, desta forma, tem de ser vista como um limite absoluto e a ter em conta na restrição dos demais direitos fundamentais, "por vezes, a projeção da ideia de dignidade humana será de tal modo intensa que não pode admitir-se a violação em nenhum caso individual sem que o conteúdo essencial do preceito seja também atingido".[202]

A verdade é que a restrição destes direitos para fins de investigação criminal, apenas será legítima, caso se respeite os seguintes pressupostos: a reserva de lei formal, a proporcionalidade em sentido amplo e a reserva de juiz, impostos pelos arts. 18.º, n.ºs 2 e 3, 32.º, n.º 4, e 165.º, n.º 1, al. b), da CRP. Sandra Oliveira e Silva refere que se trata de *"«Um entendimento que obriga o legislador ordinário a uma atitude de perseverante vigilância sobre as novas possibilidades técnicas de investigação suscetíveis de contender com os direitos fundamentais, no sentido de sancionar a sua admissão, formal e materialmente legitimada, no processo penal»"*.[203]

---

[199] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Fundamentos da Constituição*", ob. cit., pp. 121-123.
[200] *Ibidem*.
[201] ANDRADE, José Carlos Vieira de, "*Os Direitos Fundamentais na Constituição Portuguesa de 1976*", ob. cit. p.165
[202] *Ibidem*, p.284-286
[203] ANDRADE, Costa, *"Bruscamente no Verão Passado",* a reforma do Código de Processo Penal. Observações críticas sobre uma lei que podia e devia ter sido diferente, Coimbra: Coimbra Editora, 2009, p. 140 *apud* SILVA, Sandra Oliveira e, "*Legalidade da prova e provas proibidas*", ob. cit., p.590.

Não sendo respeitados estes pressupostos estaremos perante uma proibição de prova, devido à sua intromissão na privacidade das pessoas.[204]

Relativamente ao princípio da proporcionalidade, distinguem-se três dimensões: da idoneidade, necessidade e da proporcionalidade em sentido estrito, como supramencionado. O princípio da idoneidade exige que a medida seja idónea, isto é adequada a atingir fins legítimos.[205] O princípio da necessidade refere que se deve eleger a medida menos prejudicial para aos direitos fundamentais dos cidadãos.[206] Por último, o princípio da proporcionalidade em sentido estrito implica que se verifique se o sacrifício dos direitos é proporcional à importância do objetivo que se pretende alcançar. Tendo de balançar os interesses em conflito. *"Tal ponderação arranca de um juízo de adequação e prognose que, muitas vezes se fundamenta em convicções subjetivas, e pré-conceitos, em lugar de se reconduzirem a uma equação pautada por valorações objetivas*".[207]

"A ponderação de bens constitucionais realizada pelo legislador dos direitos fundamentais só pode ser rejeitada quando constitua uma ponderação manifestamente errónea entre os fins perseguidos e as restrições previstas. (…) Tomando em atenção que a gravidade do crime a perseguir não será, só por si e enquanto tal, razão bastante para legitimar a danosidade social da violação das proibições de prova." [208]

O próximo passo será agora ver de que forma se podem limitar os direitos em causa quando se fala em reconhecimento facial.

Como já foi visto, devido ao surgimento de novas tecnologias no domínio da prova é incontornável a intromissão na esfera de privacidade. Contudo, não falamos apenas na esfera da privacidade de arguidos, mas também de terceiros.[209]

---

[204] ANDRADE, Manuel da Costa, "Bruscamente no Verão Passado", ob. cit, p.149, 150 e 157 *apud* FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 141.

[205] CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Fundamentos da Constituição*", ob. cit., pp. 133-135, definido mais pormenorizadamente no Ac. STJ 28-09-2011, este menciona ainda que "Significa o exposto que o juízo sobre a idoneidade não se esgota na comprovação da aptidão abstracta de uma medida determinada para conseguir determinado objectivo, nem na adequação objectiva da mesma, tendo em consideração as circunstâncias concretas, mas também requer o respeito pelo principio da idoneidade a forma concreta e ajustada como é aplicada a medida por forma a que não se persiga uma finalidade diferente da antecipada pela lei".

[206] *Ibidem*.

[207] Ac. STJ 28-09-2011.

[208] *Ibidem*.

[209] ANDRADE, Manuel da Costa, "*Bruscamente no Verão Passado*", a reforma do Código de Processo Penal. Observações críticas sobre um lei que podia e devia ter sido diferente, Coimbra: Coimbra Editora, 2009, p.149, 150 e 157 apud FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p.139.

No que toca à privacidade, não estando perante uma intromissão abusiva, pode legitimar-se o recurso a certos meios de prova com o mero consentimento, porém, como refere Püttner/Brühl "*o exercício da autonomia de um pode facilmente converter-se em coerção para o outro*", ou seja, o consentimento de uma pessoa pode atingir a esfera jurídica de outra, apesar de assegurar a "integridade do respetivo bem jurídico".[210] Isto acontece porque as manifestações de intromissão na esfera de privacidade não se limitam à esfera jurídica de uma só pessoa, como facilmente se percebe que estando uma câmara num local público, afeta a esfera jurídica de todas as pessoas que por lá passam.[211]

Relativamente ao direito à imagem, este não se sobrepõe a todas as ponderações de valores, quando se está perante um confronto com um valor ou direito, situado num patamar superior, dificilmente esta prevalece.[212]

Será que representa uma maior ingerência nos direitos fundamentais e no quotidiano dos cidadãos a instalação de uma câmara de vigilância e a utilização destas imagens para se proceder a reconhecimentos faciais? Há quem defenda que a intervenção policial "tem uma evidente carga de pressão física e agressividade latente (uniforme, armamento, posição de combate…)", representa uma maior ingerência do que a utilização de câmaras de videovigilância, sendo que, acrescendo a este facto, a presença policial massiva não seria tão eficaz quanto as câmaras ("A presença policial também pode ter eficácia dissuasória de comportamentos ilícitos, mas não permite localizar de forma imediata e com precisão os focos onde se produzem as alterações da segurança e não permite registar para efeitos de identificação as pessoas participantes nos factos"), defendendo que a utilização de câmaras seria uma medida menos drástica e restritiva.[213]

A verdade é que serão ilícitas todas as formas de gravação e utilização arbitrárias dos direitos à imagem que não esteja prevista na lei[214], a este propósito menciona-se o art. 167.º CPP que "*representa a consagração positivada da opção do legislador de não reconhecer à realização da justiça criminal – pese embora a sua inquestionável dignidade constitucional – a prevalência necessária para justificar, só por si e para além das áreas de justificação oferecidas pelas autorizações legais positivamente sancionadas, os atentados*

[210] PÜTTNER/BRÜHL, *JA*, p.297, *apud* ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.53.
[211] ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", ob. cit., p.*52.*
[212] Ac. do STJ de 28-09-2011.
[213] Excertos retirados do Ac. STJ de 28-09-2011.
[214] ANDRADE, Manuel da Costa, *"Artigo 199.º (Gravações e Fotografias Ilícitas)",* ob. cit., p.1226.

…à imagem"[215], ou seja, a finalidade de descoberta da verdade material não legitima a produção da gravação à margem do consentimento ou de autorização legal.[216]

É certo que, se olharmos para o art. 250.º, n.º 6 do CPP, este prevê a possibilidade de utilização de fotografias para se proceder à identificação de um suspeito, contudo, fá-lo subsidiariamente, sendo uma questão de *ultima ratio*. Contudo, a verdade é que só como última medida é que se pode recorrer a este reconhecimento, poder-se-á, tendo em atenção isto, admitir um reconhecimento baseado em dados biométricos retirados de imagens captadas por câmaras de videovigilância e tendo em conta tecnologias que procedem a esse reconhecimento automaticamente, com todos os problemas a elas associados? Isto é, no caso das tecnologias de reconhecimento facial há uma maior ingerência nos direitos fundamentais, será que se pode admitir o uso destas, tendo em conta que uma medida com menor ingerência apenas é admitida subsidiariamente?

Como salientado no Ac. do STJ de 28-09-2011, Mário Monte refere que "*não estará excluída agora possibilidade de se utilizar um meio de vigilância audiovisual, num certo espaço vigiado, para fins de investigação criminal, onde fique registada a voz e a imagem, desde que tal registo seja previamente autorizado ou ordenado por juiz*", relativamente a um crime do catálogo e devido à necessidade de utilização desse meio de obtenção de prova para a investigação.[217]

4. Considerações Finais

Após as considerações já tecidas, e conhecendo as vantagens da utilização de tecnologias de reconhecimento facial, haverá que se estudar a possibilidade de serem usadas em processo penal, sem nunca perder de vista a proteção dos direitos fundamentais, em especial os enumerados neste Capítulo.

Em causa, como sabemos, está o respeito pela dignidade da pessoa humana, sendo que existindo intervenções abusivas por parte dos órgãos de perseguição penal, são

[215] *Ibidem*.
[216] *Ibidem*.
[217] Ac. do STJ de 28-09-2011.

suscetíveis de abalar a "confiança da comunidade na conformidade do processo penal aos princípios do Estado de Direito".[218]

Assim como foi referido no título anterior, tem de ser necessário usar estas tecnologias para se poder com a utilização delas restringir direitos, "caso contrário, corremos o risco de mudar as normas culturais, levando à aceitação da falta de privacidade como o princípio geral."[219]

Será o reconhecimento facial necessário? Tratar-se-á do meio menos prejudicial para os direitos dos cidadãos? Não seria mais fácil, com resultados mais fidedignos, ao invés de utilizar mecanismos de reconhecimento facial, estar perante as câmaras um agente que, observando a ocorrência de um ilícito típico se dirigiria para o local a fim de identificar os envolvidos? Isto de forma a que não fosse necessário o armazenamento de dados pessoais e a posterior comparação destes, associada aos riscos de precisão destas tecnologias?

Acontece que já no Ac. do STJ de 27-09-2017 se fez referência ao reconhecimento facial e à antropometria, tendo sido, no entanto, colocadas imensas dúvidas da precisão dos resultados tendo em conta a variação física da pessoa em questão.

Tendo em conta o princípio da proporcionalidade em sentido estrito, será razoável o sacrifício dos direitos fundamentais a fim de se proceder à identificação das pessoas por meio de recurso a tecnologias de reconhecimento facial?

A verdade é que, como nos diz Anabela Miranda Rodrigues, existe "*um poder computacional sem precedentes, em que computadores têm uma capacidade que permite processar quantidades praticamente infinitas de dados em tempo irrisório e a custos de armazenamento cada vez mais baratos, e a disponibilidade de quantidades ingentes de dados, constantemente gerados por aparelhos digitais, a título gratuito, foram as duas premissas que permitiram oferecer ao sistema de justiça penal instrumentos que lhe são de enorme utilidade, mas sem que, em grande parte, se tivesse acautelado, ao mesmo tempo, a diminuição da distância, sempre inevitável, mas que se alargava, entre o progresso*

---

[218] SCHÄFER, *in LÖWE/ROSENBERG, Einleitung,* Cap.14, Rn.14 *apud ANDRADE, Manuel da Costa, "Sobre as proibições de prova em processo penal", ob. cit.*, p. 224.

[219] EDPB – European Data Protection Board, "*Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo*", Versão 2.0, Adotado em 29 de janeiro de 2020, p.6, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf, consultado a 16 de novembro de 2021.

tecnológico e regulação."[220] A mesma autora refere que "Não se deve desperdiçar uma tecnologia potencialmente útil, nem subestimar os seus riscos"[221]

Não parece que seja proporcional, havendo uma clara intromissão nos direitos fundamentais, intromissão esta que não se coaduna com a finalidade da descoberta da verdade material. Sendo que, em causa temos mais do que um direito fundamental que terá de ser limitado.

Primeiramente temos o caso de limitação do direito à imagem, uma vez que são captadas fotografias do rosto dos cidadãos, com a finalidade de estes serem identificados. Das fotografias captadas são depois retirados dados biométricos, interferindo, desta feita, com a proibição de tratamento informático de dados referentes à vida privada. Com a constante captação e identificação dos cidadãos temos uma intromissão na reserva da intimidade da vida privada, uma vez que, facilmente se procederá à localização de um cidadão. Associado a isto estão os demais problemas elencados e analisados no Capítulo I.

Como referido por Costa Andrade, o "*propósito de carrear provas para o processo penal e prosseguir a verdade material também não justifica, fora dos casos expressamente previstos na lei, a produção ou utilização das fotografias (filmes, registos videográficos) arbitrárias*".[222]

Chegando ao fim da exposição, considera-se pertinente referir que há quem acredite que pode ser utilizado como meio de prova, desde que este não seja o único meio[223], havendo, no entanto, quem divirja deste pensamento, como é o caso de Joy Buolamwini que acredita que estes softwares não deveriam ser treinados para decidir o futuro de uma pessoa.[224]

A Agência Europeia pelos direitos fundamentais, reforçando a ideia de que, apesar de que sempre existirá uma margem de erro com impacto nos direitos fundamentais, a precisão desta tecnologia tem melhorado, acabando por concluir pela necessidade de uma

---

[220] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal", ob. cit., p.13.
[221] *Ibidem*, p.51.
[222] ANDRADE, Manuel da Costa, *"Artigo 199.º (Gravações e Fotografias Ilícitas)",* ob. cit., p.1228.
[223] BARROS, Isabel Maria Pereira Paes de e SILVA, Isabela Inês Bernardino de Souza e, "*Utilização do Reconhecimento Facial Eletrónico por empresas para identificação de suspeitos: segurança ou violação do Estado democrático de Direito?*", Revista Transgressões, Ciências Criminais em Debate, v.8, n.1, julho 2020, p. 71, disponível em https://1library.org/document/y932g6ly-utilizacao-reconhecimento-eletronico-identificacao-suspeitos-seguranca-violacao-democratico.html, consultado a 18 de março de 2022. Da mesma forma, cfr. MCGREGOR, L., MURRAY, D. AND NG, VIVIAN, "*International Human Rights Law as a Framework For Algorithmic Accountability*", ICLQ vol 68, April 2019 p.337, https://doi.org/10.1017/S0020589319000046, consultado a 30 de novembro de 2021.
[224] BUOLAMWINI, Joy e GEBRU, Timnit, "*Gender Shades: Intersectional Accuracy Disparities*", *ob. cit.*.

regulamentação específica sobre esta matéria, sendo determinado quando é que o uso destas se mostra adequado, necessário e proporcional, advertindo ainda para a necessidade de supervisão dos dados processados por uma autoridade independente, tendo em conta a intromissão nos direitos fundamentais.[225]

Conclui-se com uma reflexão feita por Sónia Fidalgo, *«Os direitos fundamentais não valem "sob reserva do progresso técnico"*[226]*, contudo, só através de um diálogo entre juristas e cientistas se pode tentar alcançar um solução para este problema, isto é, "encontrar um (renovado) equilíbrio entre a descoberta da verdade material e a realização da justiça, por um lado, e a proteção dos direitos fundamentais do arguido, por outro.»*[227]

[225] FRA – European Union Agency For Fundamental Rights, *"Facial recognition technology: fundamental rights considerations in the context of law enforcement"*, pp. 33-34.
[226] SCHANTZ, Peter «Verfassungsrechtliche Probleme von "Online-Durchsunchungen"», Kirtische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft, vol. 90, n.º3, 2007, p.310-330, apud FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 156.
[227] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p. 156.

CONCLUSÃO

Com o nosso estudo, procuramos olhar para as tecnologias de reconhecimento facial, em primeira linha, para perceber melhor o que são e o seu modo de funcionamento. Conseguiu-se aqui apurar que estas tecnologias são bastante vantajosas, no entanto, contrapondo com estas, existem também problemas que acompanham o surgimento e desenvolvimento destas tecnologias, problemas esses que têm de ser acautelados sob pena de violação de direitos fundamentais.

Apurar se, na atualidade, estas tecnologias são meios de obtenção de prova admissíveis, é de extrema importância, na medida em que pode ser uma vantagem ao nível da descoberta da verdade material, servindo como uma ajuda para a descoberta desta.

Foram vistos os corolários da admissibilidade da prova, tendo-se chegado à conclusão que, neste momento, não são admissíveis meios de obtenção de prova, isto está relacionado principalmente com o terceiro corolário referido que nos diz que estando em causa direitos fundamentais, não se basta com a não previsão de uma proibição de prova para ser admissível, tendo, inclusive que existir uma lei expressa a autorizar a utilização destas tecnologias como meios de obtenção de prova.

Foi referido o facto de inexistência de regulamentação da matéria em causa, como referido por Miguel João Costa e António Manuel Abrantes "*o momento presente é um momento de incertezas e indefinições. No plano legislativo e paralegislativo estão ainda a ser dados os primeiros passos; a experiência jurisprudencial é ainda exígua*."[228]

Ademais, depois foram elencados os direitos fundamentais mais afetados pelas tecnologias em questão, tecendo breves considerações sobre cada um, tarefa esta relevante, contudo, a verdade é que "a legislação será sempre insuficiente".[229]

Percorremos o regime de restrição dos direitos fundamentais, nos principais pontos de interesse destes para o presente estudo, sendo de extrema importância uma vez que para o uso de tecnologias de reconhecimento facial no processo penal português é essencial o respeito pelos limites impostos de tal regime.

---

[228] COSTA, Miguel João e ABRANTES, António Manuel, "*Os Desafios da Inteligência Artificial da Perspectiva Transnacional: A Jurisdição e a Cooperação Judiciária*", in "A Inteligência Artificial no Direito Penal", coor: Anabela Miranda Rodrigues, Almedina, 2022, p. 207 (163-217).
[229] RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal", ob. cit. p.50.

Devemos ainda ter em conta, tomando por referências diversos estudos elaborados e mencionados no presente trabalho, que os resultados vão-se alterando tendo em conta o rápido desenvolvimento da tecnologia. E cada vez mais as pessoas se acostumam à exposição às novas tecnologias.[230]

De facto, com as captações das imagens dos cidadãos com a finalidade da sua posterior identificação, com a extração dos dados biométricos e o seu armazenamento, tratando-se estes de dados íntimos, com a constante 'perseguição' feita aos cidadãos, sendo facilmente localizados dificilmente se antevê a possibilidade da admissibilidade destes mecanismos como meios de obtenção de prova. Associado ao que se acabou de referir estão os restantes problemas associados como é o caso da falta de precisão destas tecnologias, os resultados discriminatórios e a facilidade de contornar os resultados, utilizando mecanismos que podem de certo modo 'enganar' as tecnologias.

Concluímos assim, que nesta vasta área em desenvolvimento que a previsão de normas jurídicas ficou aquém do desenvolvimento destas tecnologias.[231] Efetivamente a realidade é sempre mais rica e dinâmica que as previsões legais.

[230] FRA – European Union Agency For Fundamental Rights*, "Facial recognition technology: fundamental rights considerations…",* ob. cit., pp. 18 – 22.
[231] FIDALGO, Sónia, "*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*", ob. cit., p.138.

BIBLIOGRAFIA

ABREU, Viviana Rubina Gonçalves, *"Reconhecimento Facial – Comparação do Uso de Descritores Geométricos Heurísticos e Aprendizagem Profunda"*, 2021, Dissertação no âmbito do Mestrado Integrado em Engenharia Electrotécnica e de Computadores, Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

ADA LOVELACE INSTITUTE, *"Beyond face value: public attitudes to facial recognition technology"* September 2019, disponível em https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/, consultado a 27 de outubro de 2021.

AKHTAR, Marya – "*Police use of facial recognition technology and the right to privacy and data protection in Europe"*. Naveiñ Reet: Nordic Journal of Law and Social Research, n.º 9, 2019, pp. 325-344, disponível em https://tidsskrift.dk/nnjlsr/article/view/122165/169414, consultado a 16 de setembro de 2021.

ALBERGARIA, Pedro Soares de, "*Artigo 125.º - Legalidade da Prova*", *in:* Comentário Judiciário do Código de Processo Penal., 2ª Edição, Coimbra: Edições Almedina.

ALBERGARIA, Pedro Soares de, "*Artigo 126.º - Métodos Proibidos de Prova", in:* Comentário Judiciário do Código de Processo Penal, 2ª Edição, Coimbra: Edições Almedina.

ANDRADE, Manuel da Costa, "*Artigo 192.º (Devassa da vida privada)*", *in*: Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, 1999.

ANDRADE, Manuel da Costa, "*Proibições da prova em processo penal (conceitos e princípios fundamentais)*", *in* Revista Jurídica da Universidade Portucalense, N.º 13 (2008), ISSN 0874-2839, pp. 143-157.

ANDRADE, José Carlos Vieira de, "*Os Direitos Fundamentais na Constituição Portuguesa de 1976*", 5ª edição, Almedina, 2012, pp.163-383.

ANDRADE, Manuel da Costa, "*Artigo 199.º (Gravações e Fotografias Ilícitas)*", *in* Comentário Conimbricense do Código Penal: parte especial, dir. Jorge de Figueiredo Dias, Tomo I, 2ª Edição, Coimbra: Coimbra Editora, 2012.

ANDRADE, Manuel da Costa, "*Sobre as proibições de prova em processo penal*", Gestlegal, 2ª edição, março 2022.

ANTUNES, Maria João, "*Direito Processual Penal*", 2ª Edição, Almedina, 2019.

ARAÚJO, Marcos Elias Cláudio de & PASQUALI, Luiz, "Histórico dos Processos de Identificação", disponível em https://doczz.com.br/doc/7242/cap%C3%ADtulo-i---hist%C3%B3rico-dos-processos-de-identifica%C3%A7%C3%A3o, consultado a 11 junho 2022.

Article 29 Data Protection Working Party (2012), "*Opinion 02/2012 on facial recognition in online and mobile services*", 00727/12/EN, WP 192, Brussels, 22 March 2012, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf, consultado a 13 de novembro de 2021.

Article 29 – Data Protection Working Party, "*Opinion 4/2007 on the concept of personal data*", junho, 01248/07/EN WP136, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, consultado a 13 de novembro de 2021.

Article 29 Data Protection Working Party, *"Opinion 3/2012 on developments on biometric technologies",* 27 de abril de 2012, 00720/12/EN, WP193, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, consultado a 13 de novembro de 2021.

BARROS, Isabel Maria Pereira Paes de e SILVA, Isabela Inês Bernardino de Souza e, "*Utilização do Reconhecimento Facial Eletrónico por empresas para identificação de suspeitos: segurança ou violação do Estado democrático de Direito?*", Revista Transgressões, Ciências Criminais em Debate, v.8, n.1, julho 2020, disponível em https://1library.org/document/y932g6ly-utilizacao-reconhecimento-eletronico-identificacao-suspeitos-seguranca-violacao-democratico.html, consultado a 18 de março de 2022.

Big Brother Watch, *"Stop Facial Recognition",* disponível em https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/, consultado a 27 de outubro de 2021.

BUCKLEY, Ben, HUNTER, Matt, *"Say cheese! Privacy and facial recognition",* Computer Law & Security Review 27 (2011), Linklaters LLP., publicado por ELSEVIER, disponível em https://www.sciencedirect.com/science/article/pii/S0267364911001567, consultado a 17 de dezembro de 2021.

BUOLAMWINI, Joy, "*how I'm fighting bias in algorithms",* produção de TedxBeaconStreet, 2016, vídeo, disponível em: https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms, consultado a 8 de fevereiro de 2022.

BUOLAMWINI, Joy e GEBRU, Timnit, *"Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*", *Proceedings of Machine Learning Research* 81: 1-15, Conference on Fairness, Accountability, and Transparency, disponível em http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf, consultado a 6 de setembro de 2022.

CANOTILHO, José Joaquim Gomes e MOREIRA, Vital, "*Fundamentos da Constituição*", Coimbra Editora, 1991.

CANOTILHO, J.J. Gomes, "*Direito Constitucional*", 6ª edição revista, Livraria Almedina, Coimbra, 1993.

CANOTILHO, José Joaquim Gomes e MOREIRA, Vital, "*Artigo 16.º*", *in*: Constituição da República Portuguesa Anotada, Vol. I, 3ª edição, Coimbra Editora, 2007.

CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 26.º*", *in*: Constituição da República Portuguesa Anotada, Vol. I, 3ª edição, Coimbra Editora, 2007.

CANOTILHO, J.J. Gomes e MOREIRA, Vital, "*Artigo 35.º*", *in*: Constituição da República Portuguesa Anotada, Vol. I, 3ª edição, Coimbra Editora, 2007.

CNIL, *"Expérimentation de la reconnaissance facial edans deux lycées: la CNIL precise sa position",* 29 de outubro de 2019, disponível em https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position, consultado a 18 de novembro de 2021.

CONCEIÇÃO, Valdir Silva, NUNES; Edna Maria e ROCHA, Ângela Machado, *"O reconhecimento facial como uma das vertentes da Inteligência Artificial (IA): um estudo de prospeção tecnológica"*, Cadernos de Prospecção – Salvador, v. 13, n. 3, junho, 2020, disponível em http://dx.doi.org/10.9771/cp.v13i3.32818, consultado a 16 de novembro de 2021.

CONGER, K., FAUSSET, R., KOVALESKI, S.F., *"San Francisco Bans Facial Recognition Technology",* The New York Times Magazine, 14 de maio de 2019, disponível em https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html, consultado a 27 de setembro de 2021.

COSTA, Miguel João e ABRANTES, António Manuel, "*Os Desafios da Inteligência Artificial da Perspectiva Transnacional: A Jurisdição e a Cooperação Judiciária*", *in* "A Inteligência Artificial no Direito Penal", coor: Anabela Miranda Rodrigues, Almedina, 2022, pp. 163-217.

DIAS, Jorge Figueiredo, "Direito Processual Penal I", Primeiro Volume, Coimbra Editora, 1974.

DIAS, Jorge Figueiredo, "Revisitação de algumas ideias-mestras da teoria das proibições de prova em processo penal (também à luz da jurisprudência constitucional portuguesa)", *in* Revista de Legislação e de Jurisprudência, Coimbra, ISSN 0870-8487. A 146, N.º 4000 (2016), pp. 3-16.

DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B. – "*A Technological and Ethical Analysis of Facial Recognition in the Modern Era."* 7 de dezembro de 2018, Engineering 183EW – Engineering and Society, – disponível em https://www.academia.edu/38066258/A_, consultado a 4 de outubro de 2021.

Eu-LISA, *"Smart Borders Pilot Project Technical Report Annexes Volume 2*", European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 2015, pp. 307-335, ISBN 978-92-95203-95-2 doi:10.2857/898335. consultado a 8 de fevereiro de 2022.

EDPB – European Data Protection Board, "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo", Versão 2.0, Adotado em 29 de janeiro de 2020, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf, consultado a 16 de novembro de 2021.

European Data Protection Board, *"Facial recongnition in school render Sweden's first GDPR fine"*, 22 de agosto de 2019, disponível em https://edpb.europa.eu/news/national-

news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv, consultado a 15 de novembro de 2021.

FARIA, Maria Paula Ribeiro de "*Artigo 35.º*", in Constituição da República Portuguesa Anotada (Jorge Miranda/Rui Medeiros), Universidade Católica Editora, 2017.

FRA – European Union Agency For Fundamental Rights*, "#BigData: Discrimination in data-supported decision making",* 2018, ISBN 978-92-9474-069-4, doi:10.2811/343905, consultado a 16 de novembro de 2021.

FRA- European Union Agency For Fundamental Rights, "Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights", 2019, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf, consultado a 16 de setembro de 2021.

FRA – European Union Agency For Fundamental Rights, *"Facial recognition technology: fundamental rights considerations in the context of law enforcement"*, novembro 2019, disponível em https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law, consultado a 13 de novembro de 2021.

FRA – European Union Agency For Fundamental Rights, *"The revised Visa Information System and its fundamental rights implications. Opinion of the European Union Agency for Fundamental Rights",* Viena, 30 de agosto de 2018, disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-visa-information-system-02-2018-corr_en.pdf, consultado a 16 de novembro de 2021.

FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", *in: A Inteligência Artificial no Direito Penal*, coord: Anabela Miranda Rodrigues, Almedina, 2022, pp.129-161.

GALBALLY, J.;FERRARA, P.; HARAKSIM, R.; PSYLLOS, A. e BESLAY, L., "*Study on Face Identification Technology for its Implementation in the Schengen Information System*",

EUR 29808 EN, Publication Office of the European Union, Luxemburg, 2019, ISBN 978-92-76-08843-1, doi:10.2760/661464, JRC116530, disponível em https://op.europa.eu/en/publication-detail/-/publication/dd473249-adbf-11e9-9d01-01aa75ed71a1/language-en, consultado a 5 de janeiro de 2022.

GARTNER, *What is Big Data?* – Gartner IT Glossary – Big Data, 2018, disponível em http://www.gartner.com/it-glossary/big-data, consultado a 16 de setembro de 2021.

HILL, Kashmir, *"Your Face Is Not Your Own. When a secretive start-up scraped the internet to build a facial-recognition tool, it tested a legal and ethical limit – and blew the future of privacy in America wide open.",* The New York Times Magazine, 2021, disponível em https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html, consultado a 9 de janeiro de 2022.

Human Rights Council, *"Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression",* 28 de maio de 2019, disponível em https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement, consultado a 9 de novembro de 2021.

LENTINO, Amanda. *"This Chinese facial recogniton start-up can identify a person in seconds*". CNBC Disruptor 50, 2019, disponível em https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html, consultado a 1 de outubro de 2021.

LI, Stan Z. e JAIN, Anil K., Handbook of Face Recognition, 2005 Springer Science+Business Media, Inc., disponível em https://link.springer.com/content/pdf/10.1007/b138828.pdf, consultado a 20 de setembro de 2021.

LIBBY, C. & EHRENFELD, J. – *Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare*. Journal of Medical Systems, 2021 – informação disponível em

https://link.springer.com/article/10.1007/s10916-021-01723-w, consultado a 20 de fevereiro de 2022.

MARASCIULO, Marília, "*Reconhecimento facial: prós e contras da tecnologia que veio para ficar*", GALILEU, junho de 2020, disponível em https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html, consultado a 18 de setembro de 2021.

MARQUES, Germano, "Curso de Processo Penal", Volume II, 4ª Edição, 2008.

MCCARTHY, John, "*WHAT IS ARTIFICIAL INTELLIGENCE?"*, Computer Science Department Stanford University, Stanford, CA 94305, disponível em http://jmc.stanford.edu/articles/whatisai/whatisai.pdf, consultado a 16 de setembro de 2021.

MCGREGOR, L., MURRAY, D. AND NG, VIVIAN, "*International Human Rights Law as a Framework For Algorithmic Accountability*", ICLQ vol 68, April 2019, https://doi.org/10.1017/S0020589319000046, consultado a 30 de novembro de 2021.

MCSORLEY, Tim, *"The Case for a Ban on Facial Recognition Surveillance in Canada"*, International Civil Liberties Monitoring Group, Canada, Surveillance & Society, 19(2), disponível em https://doi.org/10.24908/ss.v19i2.14777, consultado a 9 de janeiro de 2022.

MEDEIROS, Rui e CORTÊS, António, "*Artigo 16.º*", *in*: Constituição da República Portuguesa Anotada (Jorge Miranda/Rui Medeiros), Universidade Católica Editora, 2017.

MEDEIROS, Rui e CORTÊS, António, "*Artigo 26.º*", *in*: Constituição da República Portuguesa Anotada (Jorge Miranda/Rui Medeiros), Universidade Católica Editora, 2017.

MOZUR, Paul. "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", The New York Times, 2019, disponível em https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html, consultado a 14 de novembro de 2021.

NEGRI, Sérgio; OLIVEIRA, Samuel & COSTA, Ramon, "*Proteção de Dados e Inteligência Artificial: Persptivas Éticas e Regulatórias. O Uso de Tecnologias de Reconhecimento Facial baseadas em Inteligência Artificial e o Direito à Proteção de Dados*", RDP, Brasília, Volume 17, n.º 93, maio/junho 2020 pp. 82-103, disponível em https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740/Negri%3B%20Oliveira%3B%20Costa%2C%202020, consultado a 24 de outubro de 2021.

NISSENBAUM, Helen e INTRONA, Lucas D., "*Facial Recognition Technology. A survey of Policy and Implementation Issues*", The Center for Catastrophe Preparedness and Response, disponível em https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues, consultado a 19 de dezembro de 2021.

Nlets – the International Justice and Public Safety Network, *"Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field",* 30 de junho de 2011, disponível em https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf, consultado a 23 de outubro de 2021.

NORRIS, Clive, "*From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control*", *in* "Surveillance as Social Sorting. Privacy, risk, and digital discrimination", Routledge, David Lyon, 2003, ISBN 0-203-99488-4, pp. 263-266, pp. 245-281 disponível em https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf, consultado a 15 de setembro de 2021.

O'FLAHERTY, Michael – "*Facial Recognition Technology and Fundamental Rights*. Opinions", European Data Protection Law Review (EDPL), Vol. 6, Issue 2 (2020), disponível em HeinOnline https://heinonline.org/HOL/Page?public=true&handle=hein.journals/edpl6&div=29&start_page=170&collection=journals&set_as_cursor=13&men_tab=srchresults, consultado a 12 de outubro de 2021.

ONG, Thuy *"Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints".* The Verge, 2017, disponível em https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium, consultado a 1 de outubro de 2021.

ORVALHO, Verónica, "Reconhecimento Facial", Ver. Ciência Elem., Casa das Ciências, 2019 – disponível em https://rce.casadasciencias.org/rceapp/art/2019/073/, consultado a 16 de setembro de 2021.

ORWELL, George – *1984* (Ana Luísa Faria, Trad.). Coleção Mil Folhas, PUBLICO, 2002, ISBN 84-8130-562-6.

Parlamento Europeu, "O que é a inteligência artificial e como funciona?", disponível em https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona, consultado a 16 de setembro de 2021.

PEREIRA, Rui Soares, "A inteligência artificial e modelos de prova", *in*: Inteligência Artificial & Direito, coord.: Manuel Lopes Rocha e Rui Soares Pereira, colaboração de Ana Coimbra Trigo, Edições Almedina, S.A., 2020, ISBN 978-972-40-8262-2, pp. 65-75.

PHILLIPS, Tom. *"China testing facial-recognition surveillance system in Xinjiang – report",* The Guardian, 2018, disponível em https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report, consultado a 1 de outubro de 2021.

POGO – Project on Government Oversight, *"Facial Recognition Facing the Future of Surveillance"*, 4 de março de 2019, disponível em https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance, consultado a 18 de outubro de 2021.

RODRIGUES, Anabela Miranda, "A Inteligência Artificial no Direito Penal", Almedina, 2022, pp. 11-59.

RODRIGUES, Sara Raquel dos Santos, *"Desenvolvimento de um Sistema de Reconhecimento Facial"*, 2020, Dissertação do Mestrado em Engenharia Eletrónica e de Computadores, Departamento de Engenharia Eletrotécnica, Instituto Superior de Engenharia do Porto.

RUBINSTEIN, Ira S., Provacy Localism, Washington Law Review, Volume 93, Issue 4, 2018, pp. 1974-1980, disponível em https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4083&context=wlr, consultado a 17 de setembro de 2021.

SANTOS, Hugo Luz dos, "Inteligência Artificial e Processo Penal", Braga: Nova Causa, Edições Jurídicas, 2022, ISBN 9789899026308.

SCHERMANN, M. HEMSEN, H. BUCHMÜLLER, C. BITTER, T. KRCMAR, H. MARKL, V. & HOEREN T., "*Big Data, Na Interdisciplinary Opportunity for Information Systems Research*", Business & Information Systems Engineering 6, 2014, disponível em https://link.springer.com/article/10.1007/s12599-014-0345-1, consultado a 16 de setembro de 2021.

SILVA, Sandra Oliveira e, "Legalidade da prova e provas proibidas", in Revista Portuguesa de Ciência Criminal, Ano 21, n.º4, 2011, Coimbra Editora, pp. 545-591.

SIROVICH, L. KIRBY, M., *"Low-dimensional procedure for the characterization of human faces",* Journal of the Optical Society of America. A, Optics and image science, Vol.4, 1987 – disponível em: https://www.researchgate.net/publication/19588504_Low-Dimensional_Procedure_for_the_Characterization_of_Human_Faces, consultado a 7 de março de 2022.

SIMONITE, Tom, *"Facebook Can Now Find Your Face, Even When It's Not Tagged",* Wired, 19 de dezembro de 2017, disponível em https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/.

SMITH, Aaron, *"More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recogniion Responsibly",* Pew Research Center, 2019, disponível em https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/, consultado a 1 de outubro de 2021.

TURK, Matthew e PENTLAND, Alex, "Eigenfaces for Recognition", Massachusetts Institute of Technology, Journal of Cognittive Neuroscience, Volume 3, number 1 – disponível em https://www.face-rec.org/algorithms/PCA/jcn.pdf, consultado a 7 de março de 2022.

WECHSLER, Harry – "Reliable Face Recognition Methods, System Design, Implementation and Evaluatio", George Mason University, USA, Springer – Disponível em https://link.springer.com/content/pdf/10.1007/978-0-387-38464-1.pdf, consultado a 3 de dezembro de 2021.

WHITTAKER, M.; CRAWFORD, K.; DOBBE, R.; FRIED, G.; KAZIUNAS, E.; MATHUR, V.; WEST, S.; RICHARDSON, R.; SCHULTZ, J. e SCHWARTZ, O., "AI Now Report 2018", AI Now Institute, New York University dezembro 2018, disponível em https://ainowinstitute.org/AI_Now_2018_Report.pdf, consultado a 31 de outubro de 2021

WIEHL, Tom*, "Human and Computerized Facial Recognition: comparison and constitutional analysis",* Northwestern Interdisciplinary Law Review, Vol. VI. No. 1, 2013, disponível em https://heinonline.org/HOL/LandingPage?handle=hein.journals/nwilr6&div=9&id=&page=, consultado a 17 de outubro de 2021.

"Regulate facial-recongition technology", Springer Nature Limited, Vol. 572, 2019, disponível em https://media.nature.com/original/magazine-assets/d41586-019-02514-7/d41586-019-02514-7.pdf, consultado a 25 de novembro de 2021.

"China: Big Data Fuels Crackdown in Minority Region. Predictive Policing Program Flags Individuals for Investigations, Detentions", Human Rights Watch, 2018, disponível em https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region, consultado a 1 de outubro de 2021

"Eradicating Ideological Viruses. China's Campaign of Repression. Against Xinjiang's Muslims", Humam Rights Watch, 2018, ISBN: 978-1-6231-36567, disponível em https://www.hrw.org/sites/default/files/report_pdf/china0918_web.pdf, consultado a 1 de outubro de 2021.

"Cognitec awarded contract by German federal criminal police office", SOURCESecurity.com, making the world a better place, disponível em https://www.sourcesecurity.com/news/co-2232-ga.837.html, consultado a 1 de outubro de 2021.

"Prefeitura lança programa Rio+Seguro", Prefeitura da Cidade do Rio de Janeiro, disponível em http://www.rio.rj.gov.br/web/guest/exibeconteudo?id=7505084, consultado a 1 de outubro de 2021.

JURISPRUDÊNCIA

Acórdão do Tribunal Constitucional n.º 137/02 – proc. n.º 363/01, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20020137.html.

Acórdão do Tribunal Constitucional n.º 607/2003, proc. n.º 594/03 disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20030607.html.

Acórdão do Tribunal da Relação de Lisboa de 03/05/2006, proc. n.º 872/2006-4, disponível em http://www.dgsi.pt/jtrl.nsf/0/2ee49abdddb133948025717f0042790b?OpenDocument.

Acórdão do Supremo Tribunal de Justiça de 28-09-2011, proc. n.º 22/09.6YGLSB.S2, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25cd7aa80cc3adb0802579260032dd4a?OpenDocument.

Acórdão do Tribunal da Relação de Lisboa de 10-05-2016, proc. n.º 12/14.7SHLSB.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/358ab50ffb6b524a80257fe8002e11e0?OpenDocument.

Acórdão do Supremo Tribunal de Justiça de 27-09-2017, disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/79760e66f0bf4ba4802581bb003b2bd8?OpenDocument.