Lusíada
Repositório das Universidades Lusíada

Universidades Lusíada

Ramos, Sofia Marreiros, 2000-

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

http://hdl.handle.net/11067/8678

Metadados

Data de Publicação 2025

Resumo Os avanços da tecnologia e o desenvolvimento da inteligência artificial proporcionam o aparecimento de novos métodos de investigação, em particular, no âmbito do reconhecimento facial. Por um lado, isso pode ser um progresso para o ordenamento jurídico português, ao fazer uso como um meio de prova e permitindo uma maior rapidez na investigação através de uma identificação mais rápida. Adicionalmente, pode constituir-se como um meio essencial para a realização dos fins do processo penal, como a d...

Advances in technology and the development of artificial intelligence have led to the emergence of new investigation methods, particularly in the field of facial recognition. On the one hand, this can be a step forward for the Portuguese legal system, as it can be used as a means of proof and allows for faster investigation through quicker identification. In addition, it can be an essential means of realising the ends of criminal proceedings, such as discovering the material truth and achieving ...

Palavras Chave Direitos fundamentais, Reconhecimento facial (Informática), Processo penal - Inovações tecnológicas, Identificação biométrica

Tipo masterThesis

Revisão de Pares Não

Coleções [ULL-FD] Dissertações

Esta página foi gerada automaticamente em 2026-10-29T23:02:36Z com informação proveniente do Repositório

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Realizado por:
Sofia Marreiros Ramos

Orientado por:
Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Constituição do Júri:

Presidente:	Professor Doutor António Júlio da Fonseca Santos Cunha
Orientadora:	Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito
Arguente:	Professor Doutor José Alberto Rodríguez Lorenzo González

Dissertação aprovada em: 10 de março de 2026

Lisboa

2025

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Sofia Marreiros Ramos

Lisboa

Julho 2025

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Sofia Marreiros Ramos

Lisboa

Julho 2025

Sofia Marreiros Ramos

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Dissertação apresentada à Faculdade de Direito da Universidade Lusíada para a obtenção do grau de Mestre em Direito.

Área científica: Ciências Jurídico-Criminais

Orientadora: Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Lisboa

Julho 2025

FICHA TÉCNICA

Autora Sofia Marreiros Ramos

Orientadora Professora Doutora Ana Bárbara Pina de Morais de Sousa e Brito

Título A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Local Lisboa

Ano 2025

CASA DO CONHECIMENTO DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

RAMOS, Sofia Marreiros, 2000-

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal / Sofia Marreiros Ramos ; orientado por Ana Bárbara Pina de Morais de Sousa e Brito. - Lisboa : [s.n.], 2025. - Dissertação de Mestrado em Direito, Faculdade de Direito da Universidade Lusíada.

I - BRITO, Ana Bárbara Pina de Morais de Sousa e, 1970-

LCSH
1. Reconhecimento facial (Informática)
2. Processo penal - Inovações tecnológicas
3. Identificação biométrica
4. Direitos fundamentais
5. Universidade Lusíada. Faculdade de Direito - Teses
6. Teses - Portugal - Lisboa

1. Human face recognition (Computer science)
2. Criminal procedure - Technological innovations
3. Biometric identification
4. Civil rights
5. Universidade Lusíada. Faculdade de Direito - Dissertations
6. Dissertations, academic - Portugal - Lisbon

LCC
1. K5475.R36 2025

AVISO LEGAL

O conteúdo desta dissertação reflete as perspetivas, o trabalho e as interpretações da autora no momento da sua entrega. Esta dissertação pode conter incorreções, tanto conceptuais como metodológicas, que podem ter sido identificadas em momento posterior ao da sua entrega. Por conseguinte, qualquer utilização dos seus conteúdos deve ser exercida com cautela. Ao entregar esta dissertação, a autora declara que a mesma é resultante do seu próprio trabalho, contém contributos originais e são reconhecidas todas as fontes utilizadas, encontrando-se tais fontes devidamente citadas no corpo do texto e identificadas na secção de referências. A autora declara, ainda, que não divulga na presente dissertação quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor ou de propriedade industrial.

AGRADECIMENTOS

Terminado este percurso que culmina o fim de uma jornada marcada por grandes desafios, aprendizagens e crescimento que não teria sido possível sem o apoio de diversas pessoas.

Queria agradecer à Professora Doutora Ana Bárbara Sousa e Brito pelo apoio e ensinamentos que foram prestados desde a licenciatura até ao mestrado e por ter aceitado ser orientadora do meu projeto de dissertação.

Queria expressar a minha sincera gratidão ao Professor Dr. João Raposo pela ajuda, pelos conselhos, pela compreensão e orientações essenciais para a concretização desta investigação e pela sua disponibilidade em aceitar ser coorientador desta dissertação.

Aos meus familiares, em especial aos meus pais e ao meu irmão, um sincero obrigada pelo apoio incondicional; pelo suporte e por acreditarem em mim mesmo quando eu duvidava, por me incentivarem a seguir em frente e por celebrarem comigo cada pequena conquista deste percurso.

Um especial agradecimento ao meu namorado pelo apoio, pela compreensão, pelo carinho, por cada palavra de motivação e por cada atitude que demonstrou o quanto esteve ao meu lado.

Agradeço também aos meus colegas e amigos, que partilharam comigo este percurso, pela interajuda, pelos incentivos nos momentos mais exigentes, pelo apoio tornando este percurso mais leve e enriquecedor.

Por fim, agradeço também à instituição Universidade Lusíada Lisboa pelo rigor e excelência que contribuíram para a realização desta dissertação.

APRESENTAÇÃO

A contribuição do reconhecimento facial por algoritmos de inteligência artificial para o processo penal

Sofia Marreiros Ramos

Os avanços da tecnologia e o desenvolvimento da inteligência artificial proporcionam o aparecimento de novos métodos de investigação, em particular, no âmbito do reconhecimento facial. Por um lado, isso pode ser um progresso para o ordenamento jurídico português, ao fazer uso como um meio de prova e permitindo uma maior rapidez na investigação através de uma identificação mais rápida. Adicionalmente, pode constituir-se como um meio essencial para a realização dos fins do processo penal, como a descoberta da verdade material e a realização da justiça. Por outro lado, temos problemas associados à afetação que o reconhecimento facial proporciona nos direitos fundamentais, como a intimidade da vida privada; o direito à imagem; o direito à autodeterminação; a liberdade de reunião e de manifestação e princípios basilares no processo português como o princípio do contraditório. Por último, pode ainda acarretar problemas de discriminação e de erros na identificação.

A forma como o reconhecimento opera, a sua pouca regulamentação e os riscos que lhe estão associados, como a restrição constante dos direitos fundamentais sem que haja uma regulamentação legal, obsta à sua implementação como meio de prova. No entanto, e apesar de não poder ser utilizado como meio de prova, podemos prever a possibilidade de fazer uso destes sistemas como um auxílio aos meios de prova já existentes, de forma a poder beneficiar das vantagens dos mesmos, garantindo sempre os direitos fundamentais e os princípios do Estado de Direito Democrático.

Palavras-chave: Inteligência Artificial; Reconhecimento Facial; Restrição de Direitos Fundamentais; Admissibilidade como meio de prova

PRESENTATION

The contribution of facial recognition by artificial intelligence algorithms to criminal proceedings

Sofia Marreiros Ramos

Advances in technology and the development of artificial intelligence have led to the emergence of new investigation methods, particularly in the field of facial recognition. On the one hand, this can be a step forward for the Portuguese legal system, as it can be used as a means of proof and allows for faster investigation through quicker identification. In addition, it can be an essential means of realising the ends of criminal proceedings, such as discovering the material truth and achieving justice. On the other hand, there are problems associated with the impact that facial recognition has on fundamental rights, such as privacy; the right to an image; the right to self-determination; freedom of assembly and demonstration and basic principles in Portuguese procedure such as the adversarial principle. Finally, it can also lead to problems of discrimination and misidentification.

The way in which recognition operates, its lack of regulation and the risks associated with it, such as the constant restriction of fundamental rights without legal regulation, hinder its implementation as a means of proof. However, although it can't be used as a means of proof, we can envisage the possibility of using these systems as an aid to existing means of proof, in order to benefit from their advantages, while always guaranteeing fundamental rights and the principles of the democratic rule of law.

Key words: Artificial Intelligence; Facial Recognition; Restriction of Fundamental Rights; Admissibility as evidence

LISTA DE ABREVIATURAS

AL. - Alínea

ART. - Artigo

CFR. - Confere

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

CC – Código Civil

Idem – o mesmo

P. – Página

RGPD – Regulamento Geral sobre a Proteção de dados

ÍNDICE

AGRADECIMENTOS **6**

LISTA DE ABREVIATURAS **9**

1. INTRODUÇÃO **12**

2. PROVA POR RECONHECIMENTO **15**

2.1 FRAGILIDADES DA PROVA POR RECONHECIMENTO 18

2.2. CAUSAS QUE COMPROMETEM A FRAGILIDADE DA PROVA POR RECONHECIMENTO ... 21

3. SISTEMAS DE IDENTIFICAÇÃO BIOMÉTRICA **27**

3.1 MODALIDADES DE BIOMETRIA 29

3.1.1 Marcha *29*

3.1.2 A geometria da mão *30*

3.1.3 A Voz *31*

3.1.4 A Impressão digital *32*

3.1.5 A Medição da Íris *33*

3.1.6 A Medição da Retina *33*

3.1.7 O ADN *34*

3.2. O RECONHECIMENTO FACIAL 35

4. ALGUNS ASPETOS SOBRE A INTELIGÊNCIA ARTIFICIAL **42**

5. VANTAGENS NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL **45**

6. LIMITAÇÕES NO USO DO RECONHECIMENTO FACIAL **47**

7. RELAÇÃO ENTRE O RECONHECIMENTO FACIAL E OS DIREITOS FUNDAMENTAIS **50**

7.1. RESPEITO PELA INTIMIDADE DA VIDA PRIVADA E PROTEÇÃO DE DADOS PESSOAIS ... 50

7.2 O DIREITO À PROTEÇÃO DA DIGNIDADE HUMANA 58

7.3 DIREITO À IMAGEM 58

7.4 DIREITO DE AUTODETERMINAÇÃO DO TITULAR 61

7.5 PRECONCEITOS E DISCRIMINAÇÃO 62

7.6 DIREITO A UM PROCESSO JUSTO E EQUITATIVO 63

7.7 DIREITO À LIBERDADE DE EXPRESSÃO, REUNIÃO E MANIFESTAÇÃO 66

8. RESTRIÇÃO DOS DIREITOS FUNDAMENTAIS 71

9. O USO DO RECONHECIMENTO FACIAL NA INVESTIGAÇÃO 82

10. A MATERIALIZAÇÃO DO RISCO DE ERRO EM SITUAÇÕES DE RECONHECIMENTO FACIAL 86

11. REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL PELA UNIÃO EUROPEIA 88

11.1. ABORDAGEM BASEADA NO RISCO 90

11.2. PROIBIÇÕES E RESTRIÇÕES 92

12. ADMISSIBILIDADE DO RECONHECIMENTO FACIAL NO PROCESSO PENAL 93

13. ORIENTAÇÕES PARA O USO DO RECONHECIMENTO FACIAL 104

13.1. AUTORIDADES RESPONSÁVEIS PELA APLICAÇÃO DA LEI E UTILIZAÇÃO PERMITIDA 105

13.2 QUALIDADE E REPRESENTATIVIDADE DOS DADOS E ALGORITMOS UTILIZADOS 106

13.3 FIABILIDADE DE INSTRUMENTOS UTILIZADOS 107

13.4 INTERVENÇÃO HUMANA 108

13.5 PRINCÍPIO DA NECESSIDADE 110

13.6 REQUISITOS DE TESTE 111

13.7 RESTRIÇÕES NA UTILIZAÇÃO DOS SISTEMAS DE RECONHECIMENTO FACIAL 112

13.8 CONTROLO E AUDITORIA DOS SISTEMAS DE RECONHECIMENTO FACIAL 113

13.9 PROTEÇÃO DOS DIREITOS DAS PESSOAS 113

13.10 PRINCÍPIO DA TRANSPARÊNCIA E EQUIDADE 115

13.11 CONSENTIMENTO 118

14. CONCLUSÕES 120

BIBLIOGRAFIA 125

JURISPRUDÊNCIA: 127

WEBGRAFIA: 130

1. INTRODUÇÃO

Nos últimos anos temos sido confrontados com diversos problemas associados à prova por reconhecimento prevista no número 1 do artigo 147º do CPP. Esta prova tem como finalidade apurar o responsável pelo crime. Não obstante, diversos estudos têm vindo a demonstrar a fragilidade deste meio de prova, que pode ser afetada por vários fatores, desde logo, a dependência da memória da pessoa que assistiu aos factos,a luminosidade, a distância do local e o tempo decorrido desde o acontecimento dos factos.

Perante os avanços tecnológicos, começam a surgir outros mecanismos probatórios baseados na inteligência artificial como o reconhecimento facial, que é baseado em processos algorítmicos que permitem esclarecer a identidade de uma pessoa através de uma imagem ou de um vídeo. Desta forma, é possível encontrar a sua identidade através da comparação automatizada da imagem com outras imagens contidas em bases de dados[1], permitindo, com maior rapidez, a identificação de uma pessoa. Para além disso, estes mecanismos apresentam também outros benefícios, como melhorias na segurança pública; resultados mais precisos e eficientes; prevenção e combate da criminalidade.

A presente dissertação incide sobre o estudo aprofundado do reconhecimento facial e a sua possibilidade de aplicação no processo penal português. São várias as vantagens associadas ao uso destes sistemas nas diversas áreas do quotidiano, desde o uso no âmbito criminal; aos usos nas esferas social e empresarial. Não obstante todas as vantagens que estão associadas a estes sistemas, a verdade é que estas tecnologias foram desenvolvidas sem um quadro normativo, o que significa que a par das diversas vantagens associadas, é mister entender os riscos e o impacto que as mesmas podem ter ao nível da privacidade, dos direitos fundamentais, vieses algorítmicas e discriminação. Questões relacionadas com a vigilância em massa, o uso desproporcional e indevido de dados biométricos, a falta de transparência e de justificação de decisões automatizadas têm sido amplamente discutidos pelos legisladores nacionais e internacionalmente. Apesar de o reconhecimento facial não ser algo recente, a problematização do mesmo incide sobre a falta de regulamentação e os

[1] Cfr. MOBILIO, Giuseppe (2021) - *TECNOLOGIE DI RICONOSCIMENTO FACCIALE Rischi per i diritti fondamentali e sfide regolative*,pp. 11-12. [consultado a 11.02.2025]. Disponível na internet :https://flore.unifi.it/retrieve/e398c381-3a8a-179a-e053-3705fe0a4cff/Mobilio%2c%20Tecnologie%20di%20riconoscimento%20facciale%2c%202021.pdf.

consequentes perigos associados a ele sem que haja normas que regulamentem a sua utilização.

Com o presente estudo, pretende-se, num primeiro momento, explicar no que consiste a prova por reconhecimento, evidenciando, posteriormente, as fragilidades deste meio de prova e apresentando as diversas causas que comprometem a sua fiabilidade. Para isto, recorre-se a conhecimentos da psicologia e a estudos/experiências que permitem entender como funciona a recuperação da memória e como a mudança de contexto, o passar do tempo e a forma como as questões são formuladas podem prejudicar este processo de identificação.

Num segundo momento, são explicados os sistemas de identificação biométrica e as suas modalidades comportamentais, as quais são a base do reconhecimento desde o modo de andar, a medição da íris, a medição da retina, a estrutura geométrica, a impressão digital, o ADN e o reconhecimento facial. Posteriormente, são evidenciados alguns aspetos importantes sobre a inteligência artificial, explicando de forma pormenorizada a maneira como estes sistemas operam. Seguidamente, é descrito um capítulo sobre o uso do reconhecimento facial na investigação por órgãos policiais, abordando-se a forma como estes sistemas são utilizadas nas investigações criminais e apresentando-se os diversos casos onde se pode fazer uso do reconhecimento facial, desde o controlo fronteiriço, controlo da criminalidade, identificação de pessoas, perseguição de criminosos, encontrar pessoas que se encontrem perdidas e controlo/prevenção de criminalidade.

Nesta investigação, são igualmente abordadas as vantagens na utilização destes sistemas desde inovações no âmbito as vigilâncias, do combate ao crime e da melhor eficiência. Ainda dentro deste âmbito, são identificados os desafios/limitações associados a estes sistemas, como a precisão dos diferentes algoritmos, os desafios éticos e as condenações que ocorreram por força da má identificação, dos erros produzidos pelos algoritmos. Questões relacionadas com a afetação dos direitos fundamentais em concreto, o grande impacto que têm nestes direitos devido à recolha de uma grande quantidade de dados e a sua posterior análise; a possibilidade de rastreamento de movimentos; o armazenamentos de dados sem o consentimento das pessoas visadas; o direito à imagem; o direito de autodeterminação que no uso destes sistemas não permite o titular decidir sobre a forma como as suas informações são

tratadas e armazenadas; os preconceitos e discriminação (e aqui são apresentados estudos onde se permite verificar que as taxas de precisão tendem a ser mais baixas em certos grupos demográficos); e o direito à liberdade de expressão, reunião e manifestação (que, acaba por ter um impacto negativo oprimindo de alguma forma o exercício destes direitos).

Os sucessivos avanços destas tecnologias e o crescente interesse na procura de novas alternativas levaram a que fossem dados os primeiros passos para a sua regulação. Neste sentido, procede-se a uma análise do Regulamento de Inteligência Artificial, que estabelece as regras harmonizadas em matéria de inteligência artificial, sendo o primeiro quadro jurídico nesta matéria a nível mundial de forma a entender quais os diferentes riscos, proibições e a forma como estes sistemas são regulamentados e utilizados. É do interesse desta investigação apresentar algumas orientações que estão regulamentadas em alguns Estados sobre as orientações que devem ser adotadas na utilização destes sistemas.

Apesar de o reconhecimento facial já estar regulamentado em alguns países e ser usado na aplicação da lei, a questão é até que ponto é que essa utilização não produz repercussões significativas sobre grupos de pessoas, incluindo minorias. A verdade é que essas repercussões têm efeitos significativos na nossa forma de viver, de agir, inclusive na estabilidade política, social e democrática[2].

Estas são algumas questões que guiam esta investigação. O objetivo subjacente não é dar respostas definitivas, mas sim refletir de forma crítica o que está por detrás destes sistemas que os leva a ser por um lado tão vantajosos, rápidos e eficientes e, por outro, tão invasivos, criando barreiras à sua aplicação. As questões de investigação deste estudo são as seguintes: será possível a regulamentação destes sistemas no processo penal português? De que forma é que conseguimos compatibilizar estes sistemas com os direitos fundamentais? Quais as possíveis direções futuras para o desenvolvimento destes sistemas de forma responsável e equitativa.

[2] Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto Versione 2.0*, pp. 8-9. [consultado a 12.02.2025]. Disponível na internet: https://www.edpb.europa.eu/system/files/202405/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf.

2. PROVA POR RECONHECIMENTO

A prova por reconhecimento é um dos meios de prova mais relevantes na investigação criminal. O CPP português tipificou a prova por reconhecimento nos artigos 147º, 148º e 149º, diferenciando-se os dois primeiros artigos pelo objeto em causa. No primeiro está em causa o reconhecimento de pessoas, no segundo, o reconhecimento de objetos e, no artigo 149º, estão subjacentes uma pluralidade de reconhecimentos[3] [4]. Esta dissertação procura estudar o primeiro tipo de reconhecimento, i.e., o reconhecimento de pessoas.

A finalidade deste meio de prova é a constatação de uma determinada realidade através da identificação pormenorizada feita por uma pessoa, ou seja, identificar o autor do ilícito criminal, que consiste num conjunto de competências de memorização visuais conducentes ao reconhecimento de uma pessoa por outra, em função de já a ter visto numa outra situação juridicamente relevante[5]. Segundo vários estudos, este reconhecimento pode ser influenciado por algumas circunstâncias, como a motivação do reconhecedor (no sentido de existir ou não algum interesse, ainda que não propositado, mas que possa de alguma forma influenciar a sua perceção), as próprias condições físicas do reconhecedor (como a idade, a memória e a perceção visual), circunstâncias relacionadas com a duração do contacto visual entre o reconhecedor e a pessoa a reconhecer ou o conhecimento anterior e as condições do local onde o facto ocorreu.[6]

Dada a fragilidade deste meio de prova, o legislador procedeu à imposição da observância de regras e procedimentos, acautelando o risco de precipitação e de má identificação do sujeito, sob pena de este meio de prova não puder ser valorado[7] nos

[3] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial.* Edições Almedina, p.21

[4] A pluralidade de reconhecimentos ocorre quando uma pessoa é chamada a reconhecer pessoas ou vários objetos ou quando várias pessoas são chamadas a reconhecer uma ou mais pessoas ou um ou mais objetos. Neste tipo de reconhecimentos, a sua realização é feita separadamente para cada pessoa que vai proceder ao reconhecimento bem como cada pessoa a reconhecer ou cada objeto a reconhecer. Para que não haja a possibilidade de influência ou descredibilização do ato processual o legislador estabeleceu a proibição de comunicação entre as pessoas que vão realizar o reconhecimento, o mesmo para cada pessoa a reconhecer ou cada objeto a reconhecer – Cfr. ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, Editora: Fronteira do Caos, pp.46-47

[5] LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado,* 4ª edição, Edições Almedina, pp 292-293

[6] Idem, p.293

[7] Neste sentido, LISBOA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Lisboa, processo 433/15.8PBSNT.L1-9, de 28-09-2017, Relator Filipa Costa Lourenço que dispõe: "I- A prova por reconhecimento é, como se sabe, um meio de prova especialmente problemático e falível quando não sejam

termos do art. 147º nº 7 do CPP, traduzindo-se, assim, numa proibição de valoração de prova, não tendo valor como meio de prova seja em que fase do processo for.

A prova por reconhecimento de pessoas é efetuada em duas partes. A primeira é denominada como reconhecimento por descrição ou intelectual e a segunda é designada como reconhecimento presencial ou físico virtual[8].

Em relação à primeira parte, o reconhecimento previsto no número 1 do art. 147º do CPP, traduz-se numa descrição feita pela pessoa que deve fazer a identificação à entidade que estiver a presidir a diligência em concreto, seja um órgão de polícia criminal, o Ministério Público, o Juiz de instrução ou o juiz presidente, com a indicação de todos os pormenores de que se recorda e o máximo de detalhes que foram percecionados na situação ocorrida, centrando-se na identidade que foi experienciado no passado por parte do reconhecedor. Após essa descrição, a mesma é inquirida para aferir se já tinha visto a pessoa descrita e em que circunstâncias. É importante realçar que esta pessoa que vai efetuar o reconhecimento pode assumir qualquer qualidade, isto é, pode ser uma testemunha, um ofendido ou um assistente, o mesmo no que diz respeito à pessoa a identificar, não tem de se tratar do arguido, podendo assumir outra qualidade[9]. Neste primeiro reconhecimento, também designado como um ato preliminar, não existe contacto visual entre o reconhecedor e a pessoa a identificar[10].

Posteriormente, são colocadas questões que procuram indagar se existem ou não fatores que possam colocar em causa a fiabilidade da identificação em causa, como, por exemplo, quais as condições de observação da pessoa a identificar foi realizada; condições de luminosidade; distância e período de duração da observação e perguntas referentes à condição do próprio observador como limitações físicas e especificidades[11]. Esta identificação deve-se à incerteza ou indefinição quanto à identidade do autor do crime[12].

---

tomadas as devidas precauções. Por isso mesmo, as respetivas formalidades são estabelecidas na lei sob pena de invalidade (nº 7 do art. 147º, CPP). Assim, a existência de um reconhecimento positivo é um dos meios de prova que, quer entre nós, quer em muitos países estrangeiros, mais influencia os tribunais no sentido de afirmar a culpabilidade da pessoa assim identificada, sobretudo quando a pessoa que efetuou o reconhecimento afirma a sua convicção sem margem para dúvidas, pois o reconhecimento é, como se sabe, um meio de prova especialmente problemático e falível quando não sejam tomadas as devidas precauções".

[8] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.40

[9] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.40

[10] LOBO, Fernando Gama, *Código de Processo Penal*, p.294

[11] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.41

[12] SILVA, Francisca Oliveira, *Prova por Reconhecimento e Inteligência* Artificial, p.23

Se, não obstante, essa descrição não for suficiente, o ato processual não pode dar-se por concluído, pelo facto da descrição feita ter sido vaga ou levantar dúvidas sobre a identidade do suspeito. Passamos então para o reconhecimento presencial. Este segundo momento traz ao confronto a pessoa que procede ao reconhecimento com a pessoa a reconhecer, seguindo as condições legais previstas no número 2 do art. 147º do CPP. Este ato traduz-se na constituição de um painel ou linha de reconhecimento onde são trazidas pelo menos duas pessoas à presença da testemunha que apresentem grandes semelhanças seja idade, sexo, estatura, cor do cabelo; cor dos olhos (incluindo o vestuário) com a pessoa a identificar[13]. É colocada então a pessoa a reconhecer na linha de reconhecimento sendo que deve apresentar-se com as condições o mais parecidas possíveis às condições que teria naquele momento em que foi vista pela pessoa a identificar, em particular vestuário, cabelo ou outros pormenores que sejam considerados necessários para o reconhecimento. É importante mencionar que caso existam alterações irreversíveis, será impossível que a pessoa se apresenta como antes, falamos em casos como queimaduras que abranjam parte da cara, no entanto se estivermos perante alterações reversíveis como o uso de barba, bigode, cabelo mais comprido ou de forma muito diferente é possível ser removido nos termos do art. 154º do CPP por ordem do juiz. Também existe a possibilidade de o arguido ser colocado com adereços seja encapuçado ou mascarado, o mais parecido possível de como se encontrava na altura em que foi visto sem que isto constitua uma violação ao direito de não autoinculpação[14] ou princípio *nemo tenetur se ipsum accusare*[15].

Posteriormente, é perguntado à pessoa a identificar se reconhece alguma daquelas pessoas e, em caso afirmativo, que indique qual. Devem ser documentadas todas as perguntas e respostas que procederam na diligência em causa de forma a permitir uma maior credibilidade deste meio de prova. É igualmente importante referir que no decurso do processo podem ser ordenados a realização de alguns comportamentos por parte da entidade que dirige a diligência às pessoas a identificar e

[13] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.41
[14] Idem, pp.42-43
[15] LISBOA, TRIBUNAL DA RELAÇÃO- Acórdão do Tribunal da Relação de Lisboa, processo 483/15.4IDLSB.L1-3 de 14-03-2018 dispõe“ O princípio *nemo tenetur se ipsum accusare* significa fundamentalmente que ninguém pode ser obrigado a testemunhar contra si próprio, a produzir prova contra si mesmo ou a fornecer coactivamente qualquer tipo de declaração ou informação que o possa incriminar. O princípio não se restringe ao mero direito ao silêncio, - artigo 61º n.º 1, alínea d) CPP, mas abrange de uma forma ampla o direito de a pessoa não ser obrigada a apresentar elementos que provem a sua culpabilidade. Trata-se em todo o caso de um direito que não é absoluto e que se deve entender como sujeito à ponderação com outros interesses e com deveres de colaboração, nomeadamente no âmbito do Direito Fiscal”,[consultado a 30.11.2024]. Disponível na internet: https://www.dgsi.pt/jtrl.nsf/-/4F697801A7E4B393802582CC0050ACCF.

à pessoa a reconhecer como colocação em diferentes posições ou a locução em voz alta[16] de trechos ou comportamentos que possam ajudar na identificação[17].

Nos termos do número 3 do art. 147º do CPP, são estabelecidas garantias para a pessoa que vai proceder à identificação. Esta situação prende-se com a possibilidade de a pessoa identificadora ser intimidada ou perturbada no processo de identificação. Nesses casos, e se não tiver lugar em audiência, deve ser efetuado sem que a pessoa seja vista pelo identificado, não existindo assim qualquer contacto seja ocular ou físico entre a linha de reconhecimento e a pessoa a fazer o reconhecimento[18]. No entanto todos os procedimentos e regras são iguais aos que já foram mencionados anteriormente a diferença é apenas a utilização de um espaço diferente onde torna impossível visualizar a pessoa que vai realizar o reconhecimento[19].

Este meio de prova introduz a reconstrução da memória do identificador em relação a um facto passado e, revelando-se o resultado probatório positivo pode traduzir-se num forte juízo de suspeição da culpabilidade do sujeito.

2.1 FRAGILIDADES DA PROVA POR RECONHECIMENTO

Não obstante a importância deste meio de prova no processo penal português, cuja relevância se pode comprovar pelo aumento de estudos empíricos e científicos nos últimos anos, têm-se vindo a verificar uma falta de fiabilidade da prova por reconhecimento. Os avanços científicos têm vindo a demonstrar que a memória não guarda uma cópia fiel dos factos, podendo, dessa forma, existir vários fatores que podem comprometer a memória dos factos ocorridos. Nem sempre existe uma compatibilidade entre, por um lado, as memórias relativamente à descrição das características e a memória visual – reconhecimento do rosto da pessoa o que significa

[16] Atenção porque o art. 61º, número 1 alínea d) do CPP dispõe que: "O arguido goza, em especial, em qualquer fase do processo e salvas as exceções da lei, dos direitos de":
(...) "d) Não responder a perguntas feitas, por qualquer entidade, sobre os factos que lhe forem imputados e sobre o conteúdo das declarações que acerca deles prestar", o que significa que o arguido pode recusar-se a efetuar nomeadamente a alocução em voz alta. Cfr. ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.43.
[17] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.43.
[18] COIMBRA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Coimbra de 10-11-2010, processo 209/09.1PBFIG.C1, disponível em https://www.dgsi.pt/jtrc.nsf/-/8FA09BD5C06877AA802577EE0041E7F1
[19] ALVES, Bruno (2012) – *A prova por Reconhecimento em Processo Penal*, p.44

que, nem sempre as pessoas que se encontram a fazer o reconhecimento e que explicam pormenorizadamente e com muitos detalhes o reconhecimento não são necessariamente melhores. Ao invés, pessoas que na descrição são pouco detalhadas, podem ser capazes de efetuar uma melhor identificação[20]. Para além disso, o processo de reconhecimento baseia-se numa descrição geral, embora o mais rigorosa possível, de estrutura, peso, tamanho, idade, roupa e penteados, mas a verdade é que nem a polícia nem os tribunais têm a certeza se a descrição está correta ou não, o que, mais uma vez, constitui um fator que pode fragilizar este meio de prova[21].

Com os avanços científicos na área da psicologia da memória, verificou-se que este meio de prova apresenta uma falta de confiabilidade. Esta realidade começou a ser mais evidente com o aparecimento de exames de ADN, que demonstraram que 70% das condenações que ocorriam nos Estados Unidos estavam associados a erros na identificação por testemunhas oculares[22] contribuindo para condenações injustas[23].

Como sabemos, a memória pode ser distorcida ou conter lacunas por vários fatores, como o tempo decorrido desde o momento da prática do facto, que pode levar a que a memória perca alguns pormenores acerca do que foi presenciado; a distância a que a pessoa se encontrava do local onde o crime foi cometido; o trauma que a pessoa sofreu ao presenciar o crime, condições morfológicas e ambientais do próprio local (permitindo ou não uma boa visibilidade, a claridade)[24]; tal como as alterações na aparência, também podem fragilizar este meio de prova. Com o passar do tempo é normal que surjam algumas alterações nas pessoas, seja algo simples como um corte de cabelo, deixar crescer a barba, *piercings* ou tatuagens, seja algo mais definitivo como a própria idade ou procedimentos cirúrgicos ou estéticos.

---

[20]MENDES, Paulo Sousa; PEREIRA, Rui Soares (2020) - *Novos desafios Da Prova Penal,* Edições Almedina, p.118

[21] Idem, p.118

[22] Um dos casos apresentados pelo *Innocence Project* foi de Ronald Cotton que foi preso em 1995 e foi condenado à pena de prisão perpétua em razão de dois julgamentos. Cotton foi acusado num primeiro julgamento por violação e num segundo julgamento por roubo. Em 1987 acabou por ser condenado por ambas as violações e duas acusações de roubo. Na investigação que ocorreu após a condenação o departamento de polícia de Burlington entregou provas que inclusive continham o sêmen do agressor para o teste de DNA. As amostras da vítima não tinham compatibilidade com o Cotton. A defesa enviou os resultados para o banco de dados de DNA do Sate Bureau of Investigation que mostrou compatibilidade com um condenado que teria feito uma confissão a um colega de prisão. Em julho de 1995 após ter cumprido 10 anos e meio de prisão o Governador da Carolina do Norte perdoou Cotton - Innocence Project: *Identificação incorreta de testemunha ocular*, [consultado a 20.09.2024]. Disponível em https://innocenceproject.org/eyewitness-misidentification/

[23] LOURENÇO, Maria João (ano 45) - *Prova por reconhecimento (falta de) confiabilidade, recomendações, boas práticas e propostas de alteração do actual regime* in Revista Do Ministério Público 177, pp. 115-116

[24] Innocence Project: *Identificação incorreta de testemunha ocular*, [consultado a 20.09.2024]. Disponível em https://innocenceproject.org/eyewitness-misidentification/

Para além da variável referida no parágrafo anterior, ainda temos a chamada variável do sistema. Este tema diz respeito aos aspetos controlados pelo sistema jurídico e, neste campo, temos os procedimentos com a aplicação da lei penal no processo da identificação pela testemunha, a apresentação de fotografias, entre outros.

Em Portugal, são poucos os estudos desenvolvidos acerca da prova por reconhecimento e da sua fiabilidade. Isto pode dever-se ao desconhecimento acerca dos fatores que podem influenciar a fiabilidade deste meio de prova e de se aceitar a prova por reconhecimento como um meio idóneo para imputar a responsabilidade criminal ao arguido[25]. Não obstante, a verdade é que também existiram casos onde ocorreram erros na identificação. Um caso com repercussão foi o de Éder Fontes (com 18 anos na altura da ocorrência dos factos) acusado de um roubo de um telemóvel onde a principal prova que levou à sua condenação foi a identificação por uma das vítimas. Numa primeira fase, houve o reconhecimento através de fotografias, num segundo momento foi obtida uma confirmação através do reconhecimento presencial, procedimento em que foram colocadas duas pessoas ao lado do suspeito, uma delas com mais de 40 anos e outro vestido com uniforme de segurança[26]. No julgamento através de imagens foi feito um novo reconhecimento, no entanto, persistiram dúvidas acerca de se Éder tinha ou não sido reconhecido no reconhecimento. Éder foi condenado a uma pena de prisão efetiva de quatro anos e meio, tendo cumprido a pena até ao último dia[27].

De facto, consegue entender-se que a prova por reconhecimento é uma peça fundamental para o processo penal português, mas isso não invalida, contudo, o que temos vindo a afirmar e a verificar quanto à pouca fiabilidade que este meio de prova pode ter, acabando muitas vezes por ser determinante para a responsabilidade criminal, seja por erro da pessoa que faz o reconhecimento, por comentários desadequados

[25] LOURENÇO, Maria João (ano 45) - *Prova por reconhecimento (falta de) confiabilidade, recomendações, boas práticas e propostas de alteração do actual regime* in Revista Do Ministério Público, p.116

[26] No caso em concreto não foi respeitado o procedimento que a lei impõe no reconhecimento por pessoas. Subjacente a este reconhecimento está tipificado como exigência (previsto no número 2 do artigo 147º do CPP), que as pessoas que compõe o painel de reconhecimento devem ser o mais semelhante possível à descrição que foi feita pelo sujeito ativo, assegurando que não são colocados no painel sujeitos com grandes assimetrias seja em razão do género, cor de cabelo e vestuário. No exemplo em causa, temos um rapaz que na altura dos factos tinha 18 anos, um homem de 40 anos e um terceiro sujeito vestido com um informe de segurança, portanto subjacente à incorreta identificação também está a violação das normas do procedimento do reconhecimento presencial.

[27] MENDES, Paulo Sousa; PEREIRA, Rui Soares (2020) - *Novos Desafios Da Prova Penal,* p.114

proferidos pelos próprios investigadores ou pelas autoridades que procedem ao reconhecimento ou aspetos do procedimento que possam de alguma forma gerar dúvidas e que acabam por conduzir a erros na identificação.

2.2. CAUSAS QUE COMPROMETEM A FRAGILIDADE DA PROVA POR RECONHECIMENTO

Como sabemos, a prova por reconhecimento de pessoas depende muito do processo cognitivo e mnemónico da pessoa que vai proceder ao reconhecimento e resulta das recordações da pessoa reconhecedora para a sua produção o que torna este meio de prova passível de não ser fidedigno. A ideia de que a memória retém toda a informação e funciona como uma câmara tem sido colocada em causa por investigações desenvolvidas sobretudo na área da psicologia, porque mais do que reproduzir os acontecimentos passados, existe um processo reconstrutivo[28]. Por mais que a memória humana seja flexível e capaz de armazenar informações durantes anos, ela é suscetível a erros, daí que a recordação dos factos seja uma reconstrução de informação imperfeita do que foi anteriormente guardado. Estudos têm demonstrado que a memória pode sofrer interferências que podem suscetibilizar o registo da informação, o armazenamento ou a recuperação, podendo traduzir-se nas chamadas falsas memórias e resultar em erros judiciários. Salienta o autor Luís Filipe Pires de Sousa que "A memória é incompleta porque o individuo não pode simplesmente prestar atenção a tudo que tenha importância do ponto de vista de uma investigação"[29].

A memória humana pode ser dividia em 3 processos: a codificação, a retenção e a recuperação, sendo que o reconhecimento de pessoas está essencialmente presente na última fase. Na primeira fase, acontece uma espécie de seleção das informações que foram percecionadas e que têm uma maior probabilidade de serem necessárias no momento presenciado descartando assim detalhes que não eram relevantes na situação. Segundo Luís Filipe Pires de Sousa "os processos seletivos fazem com que a nossa memória seja forçosamente incompleta, que ocorra uma economia cognitiva no sentido de que poupamos muitos recursos no processamento de

[28] SOUSA, Luís Filipe Pires de (2020) - *Prova Testemunhal – Noções da Psicologia do Testemunho*, 2ª edição, Edições Almedina, p.7
[29] SOUSA, Luís Filipe Pires de (2020) - *Prova Testemunhal – Noções da Psicologia do Testemunho* p.7

interpretação e codificação da realidade"[30]. Na segunda fase, temos a retenção da informação que foi codificada, nesta fase, podendo ainda verificar-se a aquisição de novas informações gerando-se um efeito de integração se se esta informação se revelar semelhante à já adquirida. Na última fase, temos um processo de resgate das memórias que foram anteriormente armazenadas e a sua posterior comunicação[31].

Podemos falar da memória como uma conjugação de informações que foram percecionadas por uma experiência passada, não podendo caraterizá-la como um registo completo da realidade, mas sim como um conjunto de interpretações. Na fase da recuperação da memória acabamos por ser influenciados por vários fatores, não apenas por motivos subjacentes à própria pessoa que procede ao reconhecimento como a idade (circunstâncias pessoais); as convicções e as crenças; o estado psíquico (como as próprias condições da perceção e, neste ponto, já interfere o tempo que decorreu desde o momento do facto); a distância do local; o tempo de observação e as condições de luminosidade[32].

Em relação ao reconhecimento dos rostos, segundo investigações desenvolvidas, o ser humano é capaz de reconhecer milhares de rostos relativamente aos quais já tinha tido contacto anteriormente, seja pessoalmente ou através de meios de comunicação social. No entanto, os rostos diferem de uma pessoa para outra, as próprias caraterísticas físicas são suficientes para a fiabilidade do reconhecimento.

Pese embora o exposto anteriormente, existem estudos experimentais desenvolvidos por autores como Buckout, em 1974, que vieram demonstrar que esta capacidade no reconhecimento de faces não é tão fiável como numa primeira perceção parecia ser. O estudo experimental realizado por Buckout (1974) simulou uma tentativa de roubo a um estudante perante 141 alunos numa sala de aula. O que se pretendia com este estudo era a identificação do assaltante e, nesse pressuposto, foram, então, apresentadas uma sequência de seis fotografias contendo uma do assaltante sete semanas depois. As conclusões do estudo demonstraram que 40% das pessoas fizeram

[30] Idem, p.15
[31] SOUSA, Luís Filipe Pires de (2020) - *Prova Testemunhal – Noções da Psicologia do Testemunho,* pp. 16-17
[32] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência* Artificial, pp.25-26

uma identificação correta e que 25% dos presentes não tiveram a capacidade de identificar o assaltante, determinando uma pessoa inocente[33].

Como podemos constatar pela experiência apresentada e por estudos da psicologia já mencionados, existe uma falta de fiabilidade dos processos de perceção e de memória. Os estudos descrevem ainda que a capacidade de reconhecer de forma correta um rosto em comparação com outros depende do intervalo de tempo entre o momento da ocorrência do facto e o ato de reconhecimento. Por exemplo, aspetos percecionados considerados menos relevantes, cerca de 80 a 90% das vezes acabam por cair no esquecimento no período de 24 horas. Mesmo as informações consideradas relevantes vão-se desvanecendo com o decorrer da passagem do tempo, o que implica que o conteúdo armazenado na memória humana vai diminuindo de forma considerável, promovendo o desgaste das memórias que foram visualizadas e experienciadas[34].

Existem, contudo, outros fatores que se revelam igualmente importantes, desde logo, a semelhança entre os rostos. Uma das exigências tipificadas na lei é que as pessoas sejam as mais parecidas em termos de características, seja através de reconhecimento por sequência de fotografias ou numa parada de pessoas ou ainda a presença ou ausência do autor do ilícito criminal na sequência[35].

Para além dos fatores anteriormente mencionados, também podem ocorrer situações em que as próprias testemunhas oculares abordem o assunto que percecionaram implicando essa partilha a possibilidade de adicionamento de factos à recordação original com novas informações[36].

Ainda como fator que pode influenciar temos a recuperação da memória, fase em que é solicitado à pessoa que se encontra a fazer o reconhecimento para transmitir a informação pertinente. Este processo pode ser condicionado por fatores psicológicos que podem afetar o equilíbrio entre os estímulos físicos, sensações e perceções. Esta fase de recuperação da memória pode ser desenvolvida através de duas modalidades. Numa primeira modalidade designada como descrição solicita-se à pessoa a identificar que descreva de forma livre todos os pormenores de que se lembra; na segunda

[33] PINTO, Amâncio da Costa (1986) - *Uma análise experimental sobre a credibilidade das identificações efectuadas por testemunhas ocultares* in Revista de Investigação Criminal, vol. 21, pp. 67-72.
[34] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência* Artificial, p.27
[35] Amâncio da Costa Pinto (1986) - *Uma análise experimental sobre a credibilidade das identificações efectuadas por testemunhas ocultares* in Revista de Investigação Criminal, vol. 21, pp. 67-72.
[36] Francisca Oliveira Silva (2024) - *Prova por Reconhecimento e Inteligência* Artificial, p.28

modalidade designada como reconhecimento, já é uma fase em que o sujeito compara as informações que são apresentadas (estímulos externos) com o conteúdo armazenado na sua memória com o objetivo de depreender se viu uma determinada pessoa ou percecionou uma situação. Como já foi mencionado anteriormente uma modalidade não anula a outra em conformidade com o preceito legal do número 1 do art. 147º e do número 2, em que num primeiro momento temos a descrição do identificado com todos os aspetos revelantes e numa segunda fase o reconhecimento da pessoa entre várias que lhe são apresentadas[37].

Esta última fase de recuperação da memória também pode apresentar fragilidades em função da forma como as perguntas são colocadas e da própria conduta de quem direciona esse processo influenciando a informação armazenada na memória. Segundo as palavras do autor Luís Filipe Pires de Sousa:

> "O modo como se formulam as perguntas e o comportamento do entrevistador, como veremos influem no conteúdo da recuperação. No momento da recuperação, voltam a produzir-se fenómenos interpretativos para suprir os hiatos da memória de modo que, confrontados com determinados elementos que não recordamos, acionamos os nossos esquemas para nos facultarem o "valor mais provável" que tenderemos a incluir na nossa evocação como se fossem elementos conservados da representação inicial"[38].

Ainda subjacente ao aspeto da forma como a testemunha ocular pode ser influenciada com base nas questões lhe são apresentadas, evidenciamos o estudo desenvolvido por Elisabeth F.Lodtus and John C.Palmer[39] na Universidade de Washington, que se baseia em acidentes de viação. O ponto central de investigação deste trabalho académico foi o estudo de como a alteração de uma simples palavra na pergunta, quando formulada às pessoas que assistiram aos factos, poderia alterar a sua resposta. Neste âmbito, são relatadas duas experiências nas quais os sujeitos de diferentes grupos de pessoas assistiram a um filme sobre acidentes de viação. Após terem assistido ao filme, foram questionados sobre os eventos ocorridos que tinham acabado de presenciar. A mesma questão "A que velocidade é que o automóvel circulava?" foi colocada aos vários grupos embora com a diferença de uma palavra.

[37] Idem, p.30
[38] SOUSA, Luís Filipe Pires de (2020) - *Prova Testemunhal – Noções da Psicologia do Testemunho*, p.17
[39] LOFTUS, Elizabeth F.; PALMER, John C. (1974) - *Reconstruction of Automobile Destruction : An Example of the Interaction Between Language and Memory'* in JOURNAL OF VERBAL LEARNING AND VERBAL BEHAVIOR 13, pp. 585-589, [consultado a 30.09.2024]. Disponível na Internet: https://www.demenzemedicinagenerale.net/images/mens-sana/AutomobileDestruction.pdf

Num grupo, foi utilizada a palavra “embate”; num outro grupo, foi utilizada a palavra “colisão”, no último, perguntou-se a que velocidade circulava no momento do “abalroamento”. A velocidade que foi apontada por cada um dos grupos foi variando, chegando inclusive a ser registada uma diferença de 10km/h[40].

Os resultados deste estudo demonstram que a forma como se formula uma determinada pergunta (nomeadamente a alteração de uma simples palavra) marca e afeta a resposta da testemunha a essa mesma questão. Uma semana depois, os sujeitos voltaram a responder a várias questões, mas a pergunta crítica era se “tinham visto algum vidro quebrado”. A verdade é que não tinha existido nenhum vidro partido no acidente, mas como a palavra “quebrado” está relacionada com acidentes de viação ocorridos a alta velocidade, era de esperar que a esmagadora maioria dos inquiridos, quando confrontados com a pergunta, pudessem responder sim com mais frequência à questão. O resultado importante era que existia uma maior probabilidade de dizer que tinham visto o vidro partido quando o verbo utilizado era “esmagar” do que quando o verbo utilizado era “bater”, o que demonstra que a alteração de uma palavra pode, de forma implícita, conter uma maior ou menor violência distorcendo, assim, a memória que temos dos factos ocorridos[41].

Para além das limitações apresentadas anteriormente, importa referir a pressão que o sujeito sente em reconhecer alguém. De facto, ao recair sobre si uma expetativa, também designada como *yes effect* – este efeito pode comprometer a credibilidade do depoimento da testemunha, podendo resultar numa resposta que não corresponde exatamente à sua perceção ou à memória que tem dos factos presenciados. As falsas recordações que ocorrem quando uma pessoa acredita ter visto outra pessoa, um evento ou um detalhe que, na verdade, não aconteceu ou aconteceu de forma diferente. A *unconscious transferece* é uma circunstância relativamente à qual uma testemunha pode identificar incorretamente um suspeito (que é inocente) pelo facto de já o ter visto antes, mas não como autor do crime. Quando ocorre o momento da identificação, a testemunha, na essência, procura olhar para cada rosto de forma a percecionar se lhe é ou não familiar[42].

[40] Idem, pp. 585-589
[41] Idem, pp. 585-589
[42] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial,* p.32

Ross et al. (1994) descreveu um caso real em que um marinheiro foi apontado numa identificação não porque tivesse cometido o crime, mas porque a vítima, um bilheteiro de comboio, já o tinha visto antes quando lhe tinha vendido um bilhete. São casos muito particulares e que não são frequentes, mas que podem resultar em condenações injustas. Uma explicação para o motivo pelo qual uma testemunha identificaria uma pessoa (inocente) que já tinha percecionado noutro local que não o do crime "é que a memória dessa pessoa foi transferida mentalmente para a memória do crime", o que acontece de forma inconsciente, daí o termo transferência inconsciente[43].

Ainda dentro deste contexto, temos a chamada *cross racial effect*, que é a dificuldade da pessoa que faz a identificação de reconhecer alguém que tem uma aparência diferente da sua. Neste ponto, surge a ideia do estereótipo. No fundo, a memória guarda a imagem do tipo de ladrão, do tipo de violador o que pode levar a um reconhecimento falso na medida em que se reconhece alguém que sendo inocente é semelhante à imagem preconcebida[44].

Apesar da prova por reconhecimento ser um meio de prova muito utilizado no nosso ordenamento jurídico para identificar os responsáveis pela prática dos crimes, é, como podemos verificar, vulnerável a diversos fatores que podem comprometer o processo. Não obstante o esforço do legislador em impor diversas exigências e formalismos neste procedimento, a verdade é que não é suficiente para remover todos os problemas que este meio de prova levanta. Todos estes problemas, desde a pouca fiabilidade da memória humana que pode ser comprometida por diversos fatores, influências externas, pressão psicológica e os erros das testemunhas oculares na identificação conjugados podem conduzir à condenação de pessoas inocentes.

Com a evolução tecnológica, foram surgindo novas técnicas de investigação que em comparação aos métodos tradicionais apresentam vários benefícios. Estamos a referir-nos aos chamados sistemas de identificação biométrica, com particular incidência no nosso tema que é o reconhecimento facial.

---

[43] PIKE, Graham, (2019) - *Visual, identification – Unconscious transference,* Forensic psychology, [consultado a 30.09.2024],. Disponível na Internet: https://www.open.edu/openlearn/mod/oucontent/view.php?id=68097&section=1.4

[44] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial*, p.32

3. SISTEMAS DE IDENTIFICAÇÃO BIOMÉTRICA

A biometria pode ser definida com um estudo que se dedica à medição de características biológicas ou físicas através de um sistema automático permitindo identificar uma pessoa[45].

Segundo o Biometric institute: "Biometria significa, literalmente, "medição corporal" de qualquer tipo, mas, cada vez mais, o termo é usado no sentido mais restrito de "medições corporais e cálculos relacionados a características humanas que podem ser usados para identificar e/ou agrupar pessoas com base em um único ou múltiplos atributos biométricos"[46].

Segundo este instituto, podemos distinguir duas modalidades no uso da biometria, as características fisiológicas e comportamentais.

A primeira modalidade incide sobre aspetos físicos e estruturais, em particular o uso da impressão digital, a geometria da mão, a retina, a íris e características faciais. É de particular relevância mencionar que quando falamos nas características fisiológicas, a maioria são permanentes e firmes relativamente a alterações, não obstante estas características podem não prevalecer no caso de serem destruídas seja de forma intencional ou propositada[47]. Em relação à segunda modalidade da biometria, a identidade é feita através dos próprios movimentos, gestos, agilidade motora através do desenvolvimento de uma ou mais funções. A forma como andamos, os timbres da voz são analisados e armazenados. Os fatores como os próprios movimentos das pessoas, a forma como andamos, como posicionais os pés, as nossas mãos são analisadas por estes sistemas biométricos que usam essas informações e esses dados que foram recolhidos para confirmarem ou não se corresponde a um perfil de usuário ou não (sendo um impostor)[48].

[45] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial*, p.39
[46] Biometrics Institute, [consultado a 3.10.2024]. Disponível na internet: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.
[47] Segundo o Biometrics Institute: "exemplos no caso de impressões digitais, podem incluir a erosão parcial das cristas de fricção nas mãos daqueles envolvidos em longo prazo no manuseio ou assentamento de tijolos, a perda ou amputação de mãos/dedos e, em casos extremos, cirurgia invasiva ou automutilação para remover ou alterar a estrutura da crista", [consultado a 3.10.2024]. Disponível na internet: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.
[48] Biometrics Institute, [consultado a 3.10.2024]. Disponível na internet: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.

De acordo com Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, o conceito de identificação biométrica pode ser definido como:

> "O reconhecimento automatizado de características humanas físicas, fisiológicas e comportamentais, tais como o rosto, o movimento dos olhos, a forma do corpo, a voz, a pronúncia, a marcha, a postura, a frequência cardíaca, a pressão arterial, o odor, as características da digitação, com o objetivo de verificar a identidade de uma pessoa comparando os dados biométricos dessa pessoa com dados biométricos de pessoas armazenados numa base de dados de referência, independentemente de a pessoa ter ou não dado consentimento prévio"[49].

A biometria tem como fundamento a reunião de alguns aspetos: universalidade (no sentido de deve existir em todas as pessoas e cada uma deve possuir o traço biométrico) a singularidade (no sentido das características que cada um de nós detém são particulares permitindo especificar); a permanência (as características mantêm-se mesmo com o decorrer do tempo) e a possibilidade [50] da caraterística biométrica poder ser medida quantitativamente[51]. Os sistemas biométricos são desenvolvidos e focados na comparação de características fisiológicas retiradas na extração, processamento e comparação de micro características de imagens adquiridas.

Relativamente ao funcionamento do sistema de reconhecimento biométrico, inicia-se com a fase do registo, isto é, consiste na deteção e aquisição da caraterística biométrica (estamos a falar da impressão digital, a face, a íris entre outras), permitindo

[49] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024, [consultado a 3.10.2024]. Disponível na internet: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32024R1689.

[50] Não obstante segundo a autora Ernestina Sacchetto (2019) no estudo *Spunti per una riflessione sul rapporto fra biometria e processo penale: ideas para reflexionar sobre la relación entre biometría y proceso penal* in Revista Trimestral De Derecho Penal,l ainda podemos encontrar outras modalidades para além das referidas anteriormente como a adquiribilidade (qualidade que permite a deteção de forma mais rápida e simples); a confiabilidade (com a particularidade de que deve permitir a repetição de operações de forma a verificar o resultado), a privacidade (adoção de medidas adequadas respeitando a confidencialidade), a possibilidade de organizar os resultados e disponibilizá-los em consultas posteriores e o grau de satisfação (indica a satisfação de cada individuo em aceitar a metodologia biométrica aplicada. Cfr. Nota de rodapé nº5 pág.467, [consultado a 4.10.2024]. Disponível na Internet: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf.

[51] JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil (2004) - *An Introduction to Biometric Recognition* in IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, p. 9, [consultado a 4.10.2024]. Disponível na Internet: https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf.

a aquisição de qualidades únicas que de seguida serão convertidas num modelo denominado como “modelo biométrico” que constitui uma representação matemática digital da amostra biológica. Numa segunda fase e terminada a fase da inscrição passamos para o procedimento de comparação dos modelos para determinar o grau de semelhança e correlação. Ao nível de similaridade geralmente é atribuída uma classificação, que em quase todos os sistemas é avaliada em relação a um número predefinido que serve como um limite mínimo, o que significa que se ultrapassar o limite, ou seja, se estiver dentro do intervalo estatístico de valores pré-definido ocorrerá a chamada correspondência e será considerada válida e o individuo será reconhecido. Caso contrário não existirá correspondência e consequentemente o reconhecimento falhará [52].

3.1 MODALIDADES DE BIOMETRIA

Podemos definir modalidades biométricas como um sistema automático concebido para reconhecer uma caraterística biométrica especifica, ou seja, diferentes formas de identificar ou autenticar indivíduos tendo em conta características biológicas (como a impressão digital, a mão, a retina, a voz, a íris) e comportamentais (como a voz, a forma de andar de cada pessoa[53]). De facto, como é possível depreender, os sistemas baseados nas características fisiológicas serão mais fiáveis do que sistemas baseados em características comportamentais.

3.1.1 MARCHA

A marcha é uma biometria comportamental que pode ser capturada através de uma câmara, permitindo a verificação biométrica através características físicas do sujeito como a dinâmica do próprio corpo, a celeridade do movimento, ângulos como o joelho, o tornozelo bem como a parte das coxas e dos pés. A captura destes movimentos

[52] SACCHETTO, Ernestina (2019) - *Spunti per una riflessione sul rapporto fra biometria e processo penale: ideas para reflexionar sobre la relación entre biometría y proceso penal*, pp.468- 469 in Revista Trimestral De Derecho Penal [consultado a 4.10.2024]. Disponível na Internet: https://dpc-rivista trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf.

[53] *Biometric Recognition: Challengs and opportunities* in National Library of Medicine: National Center for Biotechnology Information, [consultado a 07.10.2024]. Disponível na Internet: https://www.ncbi.nlm.nih.gov/books/NBK219892/

é realizada por câmaras e sensores colocados à distância não necessitando da cooperação do sujeito[54]. A marcha, apesar de não ser considerada uma característica universal, é tida como um elemento identificador. Alguns exemplos incluídos na marcha são o caminhar, o correr, e o subir escadas. É importante realçar que a marcha pode não permanecer imutável podendo sofrer alterações devido à passagem do tempo, possíveis lesões graves envolvendo articulações ou o cérebro e situações de embriaguez[55]. Não obstante, esta modalidade da biometria apresenta dificuldades, a autora Francisca Oliveira Silva relativamente a este aspeto expõe: "estes sistemas biométricos enfrentam uma grande dificuldade, que se prende com a impossibilidade de criar uma base de dados que permita a operação de confronto. A inexistência de uma base de dados impede comparações automáticas baseadas na forma como as pessoas andam, inviabilizando qualquer identificação"[56].

A modalidade biométrica da marcha pode ser influenciada por vários fatores, desde logo a escolha do calçado, a superfície de caminhada e as roupas. Apesar de ser uma das modalidades muito utilizadas, estes sistemas de reconhecimento de marcha ainda se encontram em desenvolvimento[57].

3.1.2 A GEOMETRIA DA MÃO

A geometria da mão é um sistema que se relaciona com a estrutura geométrica da mão que incluí características da geometria dos dedos, a superfície da própria mão, como a forma, a largura, o comprimento dos dedos e das juntas, a densidade dos dedos e da palma da mão. Embora este sistema biométrico tenha surgido na década de setenta do século XX e, hoje ainda seja um sistema bastante utilizado a verdade é que a singularidade da geometria da mão tem sido bastante debatida. O problema

[54] Biometrics Institute: *Types of biometrics – Gait*, [consultado a 4.10.2024]. Disponível na Internet: https://www.biometricsinstitute.org/types-of-biometrics-gait/
[54]JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil (2004) - *An Introduction to Biometric Recognition* in Ieee Transactions on Circuits and Systems for Video Technology, , VOL. 14, No. 1, p. 9, [consultado a 4.10.2024]. Disponível na Internet: https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf..
[55] Idem, p.9
[56] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial,* p.41
[57] *Biometric Recognition: Challenges and Opportunities* in National Librsry of Medicine: National Center for Biotechology Information, [consultado a 07.10.2024] Disponível na Internet: https://www.ncbi.nlm.nih.gov/books/NBK219892/ .

sustentado baseia-se na ideia de que, a geometria da mão não contém elementos únicos que permitam identificar um indivíduo como a impressão digital. Não obstante e ainda subjacente aos problemas da geometria da mão ainda temos como objeto de discussão a invariância, ou seja, na medida em que podem existir alterações com o decorrer do tempo seja por situações relacionadas com a idade das pessoas ou por doenças, por essa razão este sistema é utilizado sobretudo para autenticação (em modo de "verificação).

A medição das caraterísticas físico-geométricas da mão é realizada através de uma câmara ou dispositivo baseado em scanner que permite capturar medidas geométricas como comprimentos, distâncias e ângulos[58]. As imagens são retiradas no momento em que a palma da mão se encontra para baixo numa placa de suporte, as características medidas são extraídas durante esse processo (o comprimento, largura e área de superfície da mão do indivíduo). As imagens e os dados que foram capturados são arquivadas num banco de dados para depois serem usadas para autenticar a identidade do inscrito de forma que nas próximas vezes quando as mãos do sujeito forem fotografadas novamente possam ser comparadas com as imagens de referência arquivadas confirmando ou rejeitando a identidade[59].

3.1.3 A Voz

O reconhecimento através da voz é processo que combina características biométricas físicas e comportamentais. As características físicas baseiam- se na forma e no tamanho das vias vocais, da boca, dos tratos vocais, das cavidades nasais e dos lábios que são utilizados na síntese do tom. As características físicas, como a pronúncia, são invariáveis com o passar do tempo, seja por condições médicas, pela idade, o estado emocional, entre outras. O reconhecimento através da voz, apesar de ser muito utilizado (não apenas na área forense como outras áreas como o setor financeiro e comercial), por ser fácil de coletar, apresenta algumas desvantagens, desde logo porque os recursos da fala são sensíveis a vários fatores como o ruído de fundo[60].

---

[58] SACCHETTO, Ernestina (2019) - *Spunti per una riflessione sul rapporto fra biometria e processo penale: ideas para reflexionar sobre la relación entre biometría y proceso penal*, p. 470 in Revista Trimestral De Derecho Penal. [consultado a 7.10.2024]. Disponível na internet: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf .

[59]Biometrics Institute – *Hand Geometry*, [consultado a 7.10.2024]. Disponível na Internet: https://www.biometricsinstitute.org/types-of-biometrics-hand-geometry/.

[60] JAIN, Anil K.; FLTNN, Patrick; ROSS, Arun A. (2008) - *Handbook of Biometrics*, [consultado a 8.10.2024]. Disponível na internet: https://content.e-bookshelf.de/media/reading/L-1927-957d45a798.pdf

O reconhecimento da voz é feito através da medição das ondas sonoras. Após a medição a voz é recolhida e verificada através de um *software* que vai produzir um conjunto de dados que decorrem da modulação da fala, da pronúncia, da frequência entre outros. Estes elementos vão permitir a criação de um modelo também designado como "impressão de voz" ou "modelo de voz", que depois a partir da comparação de duas ou mais amostras vão permitir avaliar se pertencem ou não à mesma pessoa[61].

3.1.4 A IMPRESSÃO DIGITAL

A identificação baseada no reconhecimento das impressões digitais que pode ser definida como o padrão de sulcos e vales na superfície da ponta do dedo (cuja formação é feita nos primeiros sete meses de desenvolvimento fetal)[62] é considerada uma das técnicas mais utilizadas, são únicas e podem ser utilizadas para identificar indivíduos. Estes sistemas analisam as saliências localizadas nas pontas dos dedos sendo extraídas através da utilização de sensores[63], criando um modelo biométrico. Posteriormente esses modelos são armazenados num conjunto de dados permitindo executar comparações individuais ou pesquisas através do banco de dados. Estes sistemas têm sido utilizados no âmbito do processo penal[64].

[61] *Types of Biometrics – Voice,* in Biometrics Institute, [consultado a 8.10.2024]. Disponível na internet https://www.biometricsinstitute.org/types-of-biometrics-voice/.

[63] De acordo com o *Biometric Institute*, é importante realçar que as impressões digitais podem ser registadas através de papel e tinta. No entanto, hoje em dia, a maioria dos sistemas biométricos é feito através de um *scanner,* ou seja, o dedo é colocado sobre uma placa ou através de um método sem contacto que captura o detalhe necessário. A utilização destes mecanismos digitais permite reduzir problemas que estavam associados à má identificação da imagem da impressão digital (como o sebo e o calor epidérmico que resultado dos dedos), [consultado a 09.10.2024]. Disponível na Internet https://www.biometricsinstitute.org/types-of-biometrics-fingerprint/.

[64] LISBOA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Lisboa, processo 458/11.2PBBRR.L1-3 de 07-10-2020 sobre o reconhecimento da impressão digital que embora seja importante no processo penal é necessária que seja conjugado com outros indícios: **"**Uma impressão digital ou palmar é um indício que, conjugado com outros indícios, pode fundamentar uma decisão condenatória, por via da prova indireta. Tal só será possível se existirem outros meios de prova ou indícios que, correlacionados com as conclusões do juízo científico de análise comparativa dos vestígios lofoscópicos, permitem, através de um raciocínio lógico, coerente e fundamentado em critérios de razoabilidade, probabilidade e regras de experiência comum, retirar o facto desconhecido – o de que foi a pessoa a quem pertencem as impressões digitais ou palmares a autora dos factos integradores do crime – a partir do facto conhecido – o de que essa pessoa esteve naquele local ou em contacto físico direto com determinados objetos – tal como é permitido pelos arts. 349º e 351º do Código Civil e 125º do Código de Processo Penal, para além de qualquer dúvida razoável". [consultado a 9.10.2024]. Disponível na Internet: http://www.gde.mj.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9b9f410576a6aabb80258a4b0054c467?OpenDocument .

Relativamente às vantagens eles revelam-se valorosos em termos de precisão, rapidez e disponibilidade imediata dos dados, por outro lado surgiram algumas dificuldades embora parcialmente superadas através dos avanços da ciência e da tecnologia relacionados com a capacidade de cálculo e de questões referentes aos falsos positivos[65].

3.1.5 A MEDIÇÃO DA ÍRIS

Os sistemas biométricos de reconhecimento são rápidos, muito precisos e bastante conceituados, apesar de serem uma modalidade recente que ainda não ganhou muita adoção nos mercados. Estes sistemas, baseados na estrutura da íris, permitem analisar a parte do olho que cerca a pupila, possibilitando a identificação de uma pessoa através da medição da íris. Para o processo de medição da íris, é utilizado um sensor de baixa intensidade e uma luz infravermelha que permite reconhecer as particularidades e padrões únicos da pessoa[66].

Relativamente aos padrões capturados, as primeiras câmaras eram posicionadas perto dos olhos, de forma a conseguir registar de forma mais detalhada as caraterísticas. Com os avanços da tecnologia, surgiram novos mecanismos em que a câmara é colocada a uma distância considerável capturando a íris mesmo em movimento (como, por exemplo, no portão de embargue do aeroporto. É importante realçar que o sistema de reconhecimento através da íris é passível de ser interrompido por vários fatores, como o movimento da pessoa durante o registo e protocolos de registo que não sejam adequados; doenças oculares; a iluminação do ambiente; reflexos de óculos, entre outras[67].

3.1.6 A MEDIÇÃO DA RETINA

[65] SACCHETTO, Ernestina (2019) - *Spunti per una riflessione sul rapporto fra biometria e processo penale: ideas para reflexionar sobre la relación entre biometría y proceso penal*, pp.469-470 in Revista Trimestral De Derecho Penal [consultado a 9.10.2024]. Disponível na Internet: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf.

[66] MAGALHÃES, Paulo Sérgio; SANTOS, Henrique Dinis (2003) - *Biometria e Autenticação,* Atas da 4ª Conferência da Associação Portuguesa de Sistemas de Informação" (edição em CD-ROM: ISBN 97 2-9354-42-1), Porto p.8, [consultado a 12.09.2024]. Disponível na Internet: https://core.ac.uk/reader/55603020.

[67] Biometrics Institute: *Types of Biometrics*, [consultado a 12.10.2024]. Disponível na Internet: https://www.biometricsinstitute.org/types-of-biometrics-eyes-iris/ .

O reconhecimento através da medição da retina é realizado através da análise dos vasos sanguíneos que se encontram na parte posterior do olho através de uma luz infravermelha, permitindo retirar os detalhes necessários. É importante realçar que apesar da medição da retina ser muito precisa, é invasiva e pode ser afetada por doenças e condições oculares como cataratas, diabetes e glaucoma. Devido ao custo do equipamento, ele é utilizado, principalmente, em aplicações de verificação de identidade em instalações de alta segurança[68].

3.1.7 O ADN

O ADN é uma substância que se encontra nas células do corpo de cada ser humano. Todo o ADN em cada célula compreende um conjunto de informações e instruções biológicas. Nele encontramos uma enorme quantidade de informações que é essencial para o desenvolvimento do ser humano, permitindo a construção de estruturas biológicas para a manutenção dos processos vitais.

As células contêm particularidades de ADN, o que permite rastrear a identidade de uma pessoa através dos materiais biológicos deixados no corpo. O reconhecimento através da análise do ADN é muito utilizado em investigações policiais e apesar de existirem fatores que possam dar falsas correspondências, como, por exemplo, a amostra biológica conter uma quantidade mínima de ADN e a contaminação ou danificação do perfil detetado no local do crime (nos últimos tempos, tem-se verificado uma melhoria na recolha, análise e tratamento das amostradas de ADN[69] permitindo uma maior fiabilidade). No âmbito das investigações criminais, compara -se o ADN que foi encontrado no local onde foi cometido o crime com outro que por referência é retirado do suspeito do crime. Se após a comparação, os dois perfis não coincidirem, então, isso

[68] Biometrics Institute*: Types of Biometrics – Eye: Retina*. [consultado a 14.10.2024]. Disponível na Internet: https://www.biometricsinstitute.org/types-of-biometrics-eye-retina/.

[69] A jurisprudência portuguesa faz uso da análise do ADN nas investigações criminais, TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional, número 240/23, processo número 175/2022 de 11/05/2023 dispõe: "O fim da recolha de ADN é, efetivamente, facilitar a investigação de crimes com autor desconhecido que tenham sido cometidos no passado ou que venham a ser cometidos ainda num futuro relativamente próximo (necessariamente dentro do prazo de manutenção da amostra na base de dados), podendo identificar-se neste ponto também alguns objetivos de prevenção penal, face à identificação das taxas de recidiva relacionadas com a prática de determinados crimes. Visa, portanto, a redução do número de investigações criminais não resolvidas, permitindo não só identificar os culpados, como afastar os inocentes da mira dos atos de investigação criminal, bem como proteger os direitos e liberdades fundamentais das vítimas. Acautela-se simultaneamente alguma persuasão dissuasiva da prática de futuros crimes por parte de agentes que sabem ter o seu perfil de ADN constante de uma base de dados acessível para efeitos de investigação criminal". [consultado a 05.02.2025]. Disponível na internet: https://www.tribunalconstitucional.pt/tc/acordaos/20230240.html.

significa que não pertencem à mesma pessoa. No entanto, se existir uma compatibilização, é necessário averiguar se o ADN do local do crime corresponde ao suspeito ou a outra pessoa com o mesmo perfil genético[70].

3.2. O RECONHECIMENTO FACIAL

O reconhecimento facial traduz-se num método automático ou semiautomático que regista e compara as caraterísticas faciais selecionadas de uma determinada imagem. Este sistema biométrico baseia-se na utilização da inteligência artificial e no uso de tecnologias, sendo, hoje em dia, utilizado em diversos setores desde as ciências forenses ao uso em organizações privadas e na administração pública.

Um aumento considerável na precisão que tem sido alcançado nestes últimos anos com a recente evolução da tecnologia do reconhecimento facial é sustentado pela inteligência artificial, que adquiriu a sua própria identidade num campo da tecnologia da informação em torno da extração de informações de imagens, de acordo com as suas metodologias, paradigmas e problemas levando muitas pessoas, empresas e inclusive autoridades a testarem e a utilizarem o uso desta tecnologia no mundo. A crescente disponibilidade e progresso de meios, recursos e ferramentas impulsionou um grande interesse na capacidade de processamento de imagens em vários âmbitos diferentes dando fomento ao que hoje conhecemos como reconhecimento facial[71].

Um conjunto de fatores como a disponibilidade e a facilidade de acesso a tecnologias de custo reduzido; a evolução e exploração computacional; a sofisticação de algoritmos de processamento e a flexibilidade e acesso a bases de dados (em específico, dados pessoais) impulsionaram os sistemas de reconhecimento facial[72].

---

[70]SACCHETTO, Ernestina (2019) - *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in Revista Trimestral De Derecho Penal Contemporaneo, p.472 [consultado a 14.09.2024]. Disponível na Internet: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf.

[71] Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull´uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, pp. 5-9. [consultado a 13.10.2024]. Disponível na internet: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

[72] MOBILIO, Giuseppe (2021) - *Tecnologie Di Riconoscimento Facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica s.r.l. P. 38. [consultado a 12.10.2024]. Disponível na internet: https://flore.unifi.it/retrieve/e398c381-3a8a-179a-e053-3705fe0a4cff/Mobilio%2c%20Tecnologie%20di%20riconoscimento%20facciale%2c%202021.pdf.

Cada vez mais, existe um maior interesse na utilização destes sistemas, em grande parte, devido à sua eficiência e por serem facilmente coletáveis na medida em que são capazes de capturar uma imagem à distância sem que o sujeito se aperceba. No entanto, subjacente a esta utilização, estão também inerentes algumas desvantagens, porque as caraterísticas do rosto estão sujeitas a alterações, como, por exemplo, a passagem do tempo, lesões ou cirurgias estéticas e a sua precisão em muito depende das condições e formas de utilização das tecnologias, isto é, é necessário que a imagem tenha uma boa qualidade, no que diz respeito à representação do rosto da pessoa a ser identificada e em relação às imagens relativamente às quais a comparação é realizada. O próprio sistema pode ser influenciado por fatores como a distância do sensor, a visibilidade do rosto, o grau de cooperação da pessoa e a qualidade das imagens[73].

Ainda que seja possível analisar milhares de dados pessoais e informações num tempo reduzido e num simples toque de um botão, a eles estão associados aspetos de discriminação algorítmica e incorreta identificação, afetando diversos direitos fundamentais, o que pode trazer grandes prejuízos, aspeto que será abordado posteriormente[74].

O reconhecimento facial enquadra-se na tecnologia biométrica que abrange todos os processos automatizados para reconhecer uma pessoa, criando os chamados dados biométricos que permitem confirmar a identificação de uma pessoa.

O funcionamento do reconhecimento facial ocorre através da comparação das caraterísticas faciais que foram retiradas de uma determinada imagem (imagem ou vídeo)[75] designada como “amostra biométrica”, extraindo uma representação digital

[73] SACCHETTO, Ernestina (2019) - *Spunti per una riflessione sul rapporto fra biometria e processo penale* in Rivista Trimestrale: Derecho Penal Contemporaneo, pp.470-471 [consultado a 14.09.2024]. Disponível na Internet: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf.

[74] Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull´uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, pp. 5-7, [consultado a 13.10.2024]. Disponível na internet: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

[75] É importante mencionar que a mera detenção e captação de imagens de rostos através das câmaras de videovigilância não representa necessariamente um sistema de reconhecimento fácil, não obstante de puder despertar questões relacionada com a ética e a eficácia. Não podem ser considerados sistemas biométricos técnicas digitais que tornem percetíveis comportamentos anómalos, episódios de violência ou reconheçam emoções desde que não se destinem a identificar de forma única uma pessoa. Estes exemplos não são totalmente distantes do reconhecimento facial e encontram-se sujeitos às regras da proteção de dados pessoais. – Cfr. Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull´uso della*

designada como “modelo”, que contém as caraterísticas únicas extraídas da amostra e que é armazenada num banco de dados.

Para o procedimento de reconhecimento facial, o aparelho vai proceder a uma comparação do modelo com outros que já estão criados ou diretamente com amostras biométricas de rostos que se encontrem em imagens, fotografias ou vídeos.
O sistema de reconhecimento facial é, assim, um sistema que se encontra disposto em dois momentos. Numa primeira fase, temos a aquisição da imagem do rosto e a transformação num modelo e, posteriormente, temos o reconhecimento do rosto através da comparação do modelo correspondente com outros[76].

No fundo, podemos identificar uma sequência de fases para o reconhecimento facial. Num primeiro momento, temos a chamada aquisição da imagem, ou seja, a representação e a conversão do rosto de uma pessoa num formato digital. A aquisição de imagem pode ser obtida de forma voluntária em espaços controlados ou através de fotografias em passaportes ou fotografias de identificação, designados como “sistemas biométricos interativos” ou de forma involuntária e em espaços que não são controlados, designados como “sistemas biométricos passivos”, como é o caso de câmaras de videovigilância que filmam ao vivo (seja num ambiente fechado ou aberto tendo consequências na qualidade da imagem). Após o momento da aquisição da imagem, temos a identificação do rosto, procedimento que pode ser muito complexo em particular quando são feitos através de sistemas biométricos passivos. Posteriormente à identificação do rosto, passamos à fase da normalização, que é um processo que devido à posição ou iluminação recorre a técnicas que permitem atenuar variações na região da face, podendo consistir na conversão para tamanho padrão, rotação ou alinhamento nas cores. Ainda nesta fase, podem ser identificados “marcos” – elementos do rosto como o nariz, boca e olhos. Seguidamente ao processo de normalização, temos a extração de recursos, sistema que permite isolar e extrair as características biométricas do rosto da pessoa. Estas características podem ser retiradas como uma representação matemática de toda a imagem do rosto ou através de caraterísticas individuais,

tecnologia di riconoscimento facciale nel settore delle attività di contrasto, pp. 9-11. [consultado a 13.10.2024]. Disponível na internet: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

[76] Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull´uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*, pp.9-10. [consultado a 13.10.2024]. Disponível na internet: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

abrangendo apenas algumas características específicas do rosto ou a combinação dos dois métodos referidos criando o "modelo de referência biométrico"[77].

Após a criação do modelo de referência biométrico segue-se o registo que é a armazenamento do modelo biométrico ou de uma imagem numa base de dados com o objetivo de uma comparação posterior.

Num momento posterior temos a fase da comparação, método que permite medir as semelhanças ou as características biométricas de um modelo de referência com outros modelos que já se encontram armazenados nas bases de dados.

Após o momento da comparação, temos a verificação. Este processo baseia-se na verificação se a imagem adquirida corresponde a uma pessoa que já se encontra conhecida e identificada[78]. Na autenticação, o sistema simplesmente verifica se a imagem capturada é da mesma pessoa que foi retratada noutra imagem. No caso em concreto, não se conhece a pessoa em questão (isto acontece em situações em que os dados de *login* são inseridos para aceder ou desbloquear um dispositivo ou serviço)[79].

A maioria destes tipos de correspondência beneficia do uso de técnicas de aprendizagem de máquina, sendo que a qualidade e a capacidade de aprendizagem das mesmas dependem de fatores como o tamanho e a representatividade dos exemplares que são inseridos durante o processo de aprendizagem através do chamado "banco de dados de treinamento". Neste processo de aprendizagem é processado um número de elevado de amostras por um computador, onde umas amostras compreendem a imagem alvo e outras contêm outra coisa e, neste caso podemos ter vários exemplos como o facto de estes sistemas puderem ser utilizados para reconhecer gado apresentando milhares de imagens de diferentes tipos de animais[80].

---

[77] Idem, p.47

[78] Este processo de verificação começou a ser utilizado em espaços como o aeroporto onde é comparado a imagem dos passageiros com a fotografia contida no passaporte.

[79] Mobilio, M. (2021) - *Tecnologie di riconoscimento facciale*. Universidade de Florença. [consultado a 21.10.2024]. Disponível na internet: https://flore.unifi.it/retrieve/e398c381-3a8a-179a-e053-3705fe0a4cff/Mobilio%2c%20Tecnologie%20di%20riconoscimento%20facciale%2c%202021.pdf

[80] JR., Perritt Henry H. (2021) - *Defending Face-Recognition Technology (And Defending Against It),* Vol. 25 : Iss. 1 , Article 2, pp. 46-47 in Journal of Technology law & police, [consultado a 21.10.2024]. Disponível na internet: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1003&context=jtlp.

Este processo de aprendizagem de máquina tem várias etapas, aprende o que é o rosto; aprende como reorientar uma imagem fácil para posteriormente puder ser comparada de forma mais fácil com outras; desenvolve a capacidade de perceber quais as características que definem o rosto e aperfeiçoa algoritmos para aplicar a um conjunto de imagens faciais[81].

Como base do reconhecimento facial, temos subjacente dois bancos de dados, o banco de dados de treinamento e o banco de dados de usuários inscritos. O banco de treinamento de dados compreende um conjunto de rostos que seriam selecionados para representar as características demográficas da população. Este banco de dados tem subjacente a aprendizagem de recursos que vão permitir distinguir as diferentes faces. No banco de dados de treinamento é essencial incluir-se o mais amplo e variedade número de rosto incluindo expressões faciais, como sorrisos ou olhares semicerrados. Não obstante, este banco de dados também deve incluir diversos sexos, idades e nacionalidades, de forma a puder reconhecer toda a população (por exemplo, um banco de dados que não contém muitos rostos de idosos não fará um bom trabalho de reconhecimento com pessoas de rostos mais velhos). A melhor forma de conseguir um banco de dados de treinamento é incluir as características mais diversas (raciais e demográficas) da população permitindo, assim, produzir algoritmos mais robustos e com maior qualidade[82].

Ao invés, o banco de dados de utilizadores inscritos tinha como base os rostos das pessoas desde fotos de licenças e fotos de passaporte, tendo como propósito determinar se a imagem obtida através dos sistemas corresponde a uma que se encontre no banco de dados de inscritos - permitindo que o sistema produza dados de identificação da pessoa com o rosto correspondente. O banco de dados cadastrada tem uma finalidade diferente do banco de dados de treinamento, sendo direcionado de forma diferente, contendo imagens de alta qualidade de pessoas conhecidas - sendo as bases mais comuns fotografias de presidiários, fotografias contidas em passaportes e cartas de condução. A precisão aceitável para o reconhecimento facial implica que haja um número elevado de imagens de rosto digitalizadas. Falamos em milhares ou milhões.

[81] JR., Henry H. Perritt (2021) - *Defending Face-Recognition Technology (And Defending Against It),I*n Journal of Technology Law & Policy: Vol. 25 : Iss. 1 , Article 2, p.46, [consultado a 22.10.2024 Disponível na internet: https://scholarship.law.ufl.edu/jtlp/vol25/iss1/2

[82] Idem, pp. 48-51. [consultado a 22.10.2024]. Disponível na internet: : https://scholarship.law.ufl.edu/jtlp/vol25/iss1/2

Só assim, com uma amostra grande de diferentes amostras de rosto nos bancos de dados é que permite que o algoritmo possa aprender quais os recursos que distinguem os diferentes rostos (é um processo que basta ser realizado uma vez, após isso o programa aprende os marcos distintivos)[83].

O reconhecimento facial pode ter duas funções distintas. Uma primeira finalidade de autenticação de uma pessoa, com o propósito de indagar se é quem afirma ser. No caso em apreço, é comparado um modelo biométrico ou uma amostra que se encontra pré-registado (por exemplo, um passaporte) com o rosto da pessoa. Uma segunda função que este sistema pode conter é a identificação de uma pessoa com o propósito de a encontrar numa área específica ou entre um grupo de uma imagem ou banco de dados. No caso em concreto, procede-se à comparação de um modelo com uma base de dados ou amostras (referência). Tanto na autenticação como na identificação de pessoas, ambos os casos são baseados numa correspondência entre modelos, o comparado e o(s) de referência[84].

É, de facto, importante salientar que os sistemas de reconhecimento facial fazem as avaliações através de algoritmos que executam cálculos que se traduzem em probabilidades sobre a correspondência entre uma imagem de uma pessoa e uma base de dados. Iniciado o processo, o sistema irá determinar um número de resultados, sendo a quantidade livremente escolhida e ordenada tendo em conta a probabilidade da pessoa em avaliação puder ou não ser incluída. Estes sistemas de reconhecimento facial podem não ser exatos, estando associado a uma percentagem de erro, porque existem fatores como o movimento da pessoa quando é fotografada, a inclinação e a pose do rosto, a qualidade e resolução da imagem; a idade; cor e condição da pele do sujeito; a sua expressão inclusive a forma de pentear o cabelo ou a maquilhagem[85].

---

[83] JR., Perritt Henry H. (2021) - Defending Face-Recognition Technology (And Defending Against It), Vol. 25 : Iss. 1 , Article 2, pp. 46-51 in Journal of Technology law & police. [consultado a 21.10.2024]. Disponível na internet: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1003&context=jtlp.

[84] Linee guida 05/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di, contrasto Versione 2.0 Adottate il 26 aprile 2023 in edpb (European Data Protection Board), pp. 8-10, [consultado a 22.10.2024]. Disponível na internet https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

[85] MOBILIO, Giuseppe (2021)- *Tecnologie Di Riconoscimento Facciale: Rischi per i diritti fondamentali e sfide regolative*, pp. 35-36, [consultado a 17.10.2024]. Disponível na internet: https://flore.unifi.it/retrieve/e398c381-3a8a-179a-e053-3705fe0a4cff/Mobilio%2c%20Tecnologie%20di%20riconoscimento%20facciale%2c%202021.pdf.

É importante salientar que os sistemas de reconhecimento facial podem ter dois resultados possíveis, também designados como resultados binários. Nessa medida, é importante distinguirmos os falsos positivos e os falsos negativos. Um falso positivo diz respeito a uma conjuntura onde uma imagem é falsamente correspondida a outra imagem presente na lista de observação. No contexto de aplicação da lei, traduz-se numa incorreta identificação pelo sistema como estando numa lista de vigilância o que representa consequências relevantes nos direitos fundamentais dessas pessoas, permitindo que, por exemplo, uma determinada pessoa tenha acesso a um determinado ambiente – em caso de verificação ou, por outro lado, seja desencadeado por parte da polícia a identificação de uma pessoa errada – em caso de identificação. A taxa de identificação de falsos positivos dispõe a proporção de analogias que foram erradamente encontradas (por exemplo, o número de pessoas identificadas, mas que na realidade não constavam na lista de vigilância) de entre todas as pessoas que não constam nessa lista. Pelo contrário, os designados "falsos negativos" são aqueles em que não existiu uma correspondência, ou seja, que não constaram na lista de observação, mas que, na realidade, são correspondentes (por exemplo, não permitindo que o proprietário tenha acesso a algo – no caso de verificação ou permitindo que uma pessoa perigosa não seja identificada e passe nos controlos de fronteira)[86].

A taxa de identificação de falsos negativos pode traduzir-se na proporção de pessoas que erroneamente não foram identificadas entre aquelas que deviam ser identificadas.

Em relação às taxas de erro, é importante realçar que o algoritmo é apenas uma probabilidade, nunca é um resultado definitivo. Em termos de percentagem, por exemplo, com uma probabilidade de 80%, uma pessoa numa imagem facial é a pessoa que aparece numa outra lista de observação, o que significa que é indispensável definir fronteiras ou listas de classificação necessárias para tomar decisões sobre as correspondências. Em segundo lugar, devido a um limiar de probabilidade, é necessário um compromisso entre os falsos positivos e os falsos negativos. Isto significa que os falsos positivos diminuirão e os falsos negativos aumentarão se o limiar determinado for

[86]FRA – European Union Agency For Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p. 9. [consultado a 17.10.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

mais elevado e vice-versa. O que ocorre nestas situações é que essas taxas são comunicadas com a outra taxa com um nível fixo, ou seja, pegando num exemplo, a taxa de erro é comunicada à taxa fixa de identificação de falsos positivos de 1%. As taxas devem ainda ser ponderadas tendo como referência a quantidade de casos reais, isto é, se houver um controlo em massa, uma taxa de identificação de falsos positivos que seja potencialmente pequena pode, mesmo assim, significar que um número significativo de pessoas é identificado de forma incorreta. Por exemplo, numa taxa de identificação de falsos positivos de 0,01 entre 100.000, pessoas, isso significa um erro na identificação de 1000 pessoas[87].

É importante mencionar que subjacente a esta questão dos falsos positivos e falsos negativos está a qualidade dos dados obtidos, a exatidão, a interpretação e a forma como os mesmos são tratados. É necessária uma atualização constante das imagens faciais constantes nas listas armazenadas de forma a permitir um tratamento rigoroso. É necessário que sejam feitas avaliações de exatidão envolvendo diferentes grupos sociais na medida em que taxas de exatidão gerais podem ser enganadoras.[88]

4. ALGUNS ASPETOS SOBRE A INTELIGÊNCIA ARTIFICIAL

Ao falarmos do processo de reconhecimento facial, é necessário relacioná-lo com o avanço da tecnologia de inteligência artificial. Os avanços computacionais, o grande volume de dados e o desenvolvimento de programas informáticos permitiram um desenvolvimento no âmbito da inteligência artificial.

A inteligência artificial é algo que está presente no nosso quotidiano e que nos traz muitos aspetos positivos, em áreas como a saúde (permitindo uma maior rapidez no diagnóstico de doenças), uma maior segurança; uma melhor adaptação às alterações climáticas entre outras.

Segundo a Comissão Europeia, a inteligência artificial pode ser definida como:

> ” o sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implicação e que, para

[87] Idem, pp. 8-10

[88] FRA – European Union Agency For Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 9-10, [consultado a 9.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

> objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais"[89].

Estes sistemas podem ter atuação no mundo virtual seja por meio de assistentes de voz, projetos de análise de imagens, sistemas de reconhecimento facial, entre outros. Nesse caso, encontram- se integrados no *software*. Ao invés, podem estar compreendidos em mecanismos físicos como robôs avançados ou veículos aéreos não tripulados.

Estas tecnologias são utilizadas para que sistemas que normalmente necessitem de intervenção humana sejam agora capazes de executar as tarefas processando muita informação de forma rápida e exata. Relativamente ao funcionamento, em concreto, dos sistemas de inteligência artificial, primeiro, temos a análise de grandes quantidades de dados. Após essa fase, temos a deteção de padrões através de algoritmos; posteriormente, a execução de tarefas e, por fim, a aprendizagem e o melhoramento do desempenho[90]. A máquina adquire capacidades de poder desenvolver competências que são semelhantes às do ser humano como a racionalidade, a aprendizagem, o planeamento e a criatividade.

Em termos mais pormenorizados, dá- se um programa ao computador (com regras de processamento e funções) e dados de *imput*[91]; através desses dados o computador através do programa processar os dados e gerar um output[92]. O que se pretende é criar processos cuja forma de funcionar é definida por nós ou recriar algo de que já tenhamos conhecimento. São dados, então, ao computador dados de *input e output* e um algoritmo que analisa estes dados e permite criar um "modelo" – que corresponde ao processo de regras e funções que convertem o *input* no *output*. Estes processos permitem modelar, através do computador, fenómenos bastante complexos, como, por exemplo, melhorar processos industriais; modelar organismos vivos e inteligentes; prever efeitos de medicamentos, entre outros. Através da inteligência

[89] Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024
[90] Conselho da União Europeia: *A IA em síntese: utilização e impacto*, [consultado a 23.10.2024]. Disponível em https://www.consilium.europa.eu/pt/policies/ai-explained/.
[91] É um processo que consiste em introduzir dados num computador com a finalidade de os armazenar ou processar.
[92] É o processo que se refere aos dados resultantes de um processo, ou seja, a informação que é emitida por um sistema informático.

artificial, é possível que os sistemas entendam o ambiente que os rodeia; lidem com as situações e solucionem problemas de acordo com um objetivo pré-definido[93]. O processo passa por o computador receber os dados (sejam eles já preparados ou recolhidos através dos sensores como a câmara de videovigilância) processa e responde. Estes sistemas estão de tal forma desenvolvidos que são habilitados a adaptar o seu comportamento, até certo ponto, através da verificação de efeitos de ações anteriores e de um trabalho autónomo[94].

Os sistemas de inteligência artificial podem de forma muito simplificada e resumida representar-se através de três capacidades: perceção e sensores; raciocínio/processamento de informações e tomada de decisões e atuação[95]. Em relação à primeira capacidade, é essencial que os sistemas de inteligência artificial contenham sensores adequados que sejam capazes de percecionar os dados num determinado âmbito e que são essenciais para os objetivos que foram determinados a perseguir e que são atribuídos pelo ser humano. Por exemplo, se um sistema de inteligência artificial for construído para limpar um determinado ambiente quando se encontra sujo, podem incluir sensores que comportam câmaras para fotografar o chão. Os sensores do sistema poderão ser câmaras; microfones; um teclado ou outros mecanismos que permitam a entrada de dados tal como os chamados sensores de quantidades físicas, como sensores de pressão; de temperatura de distância ou sensores táticos. Relativamente aos dados e informações que são obtidos, podem ser diferenciados em dados estruturados que são estruturados em modelos pré-definidos (como uma base de dados) e dados não estruturados, que não têm uma organização estruturada (como um parágrafo de um texto). Após a fase da perceção, temos o raciocínio onde os dados que foram percecionados são agora analisados, a fim de ser tomada uma ação tendo subjacente o objetivo definido, ou seja, estes dados são agora transformados em informação para que o sistema de raciocínio e processamento os consiga compreender. Pegando no exemplo da limpeza, o sistema obtém a imagem de

[93] VINAGRE, João; MONIZ, Nuno (2020) – *Inteligência Artificial: Riscos e promessas* in Revista de Ciência Elementar., V8 (04):052, pp. 2-4. [consultado a 24.10.2024]. Disponível na internet: https://rce.casadasciencias.org/rceapp/pdf/2020/052/.

[94] Parlamento Europeu: *o que é a inteligência artificial*, [consultado a 23.10.2024]. Disponível na Internet: https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona#o-que--a-inteligncia-artificial-3.

[95] Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial, Comissão Europeia (2018) – *Uma Definição de IA: Principais Capacidades e Disciplinas Científicas*, pp. 1-3. [consultado a 24.10.2024]. Disponível na internet: https://lms.nau.edu.pt/assets/courseware/v1/3e0b4d98484f187196e18fb8e2d7e6bf/asset-v1:DGE+IAESC+2020_T4+type@asset+block/ADEFINITIONOFAI-PTpdf.pdf.

um pavimento que não se encontra limpo ao módulo do raciocínio e este vai ter de tomar uma decisão em limpar ou não. Não obstante, o módulo de raciocínio/processamento tem de tentar fazer uma análise sobre a fotografia e consoante essa interpretação decidir agir na limpeza do pavimento ou não, o que implica uma transformação e interpretação dos dados em informação. Numa segunda fase, temos o raciocínio sobre a informação, produzindo um modelo numérico com o objetivo de decidir qual é a melhor ação para o caso concreto. É importante mencionar que quando se utiliza o termo "decisão", isso não significa uma total autonomia dos sistemas de inteligência artificial. A decisão pode significar a escolha de uma orientação que é transmitido ao ser humano que tem nas suas mãos a ação final. Por fim, temos a atuação que é a execução do sistema através dos meios que tem ao seu dispor. Os atuadores podem ser braços articulados ou podem consistir em *software* (não tem de ser necessariamente físicos)[96].

De facto, podemos retirar que efetivamente a inteligência artificial contribui para um conjunto de benefícios sejam eles económicos, ambientais ou sociais, mas é preciso ter atenção que subjacente a estes sistemas temos que a sua utilização pode criar riscos aos interesses públicos e, em particular, aos direitos e liberdades fundamentais. Esses prejuízos podem ser materiais ou imateriais compreendendo danos físicos, psicológicos sociais e económicos.

5. VANTAGENS NA UTILIZAÇÃO DO RECONHECIMENTO FACIAL

Os sistemas de reconhecimento facial têm vindo a ser desenvolvidos devido ao grande avanço tecnológico permitindo o rastreio, a vigilância de pessoas e a agregação de um elevado número de dados sobre as pessoas, os seus movimentos, redes e relações. O reconhecimento facial pode ser utilizado como uma vantagem para detetar, investigar e dissuadir crimes e danos graves; para combater as ameaças à segurança de forma a promover interesses coletivos em matéria de segurança pública.

Em termos gerais, existem algumas categorias de utilização do reconhecimento facial que são mais relevantes para o contexto de polícia e segurança. Como primeira categoria temos a verificação da identidade de uma pessoa, procede-se a uma comparação de um modelo biométrico derivado da imagem facial da pessoa com um modelo pré-armazenado no sistema. Um exemplo comum é o controlo automático de

[96] Idem, pp. 1-3

passaportes na passagem da fronteira, onde a câmara capta uma imagem do rosto de uma pessoa e digitaliza o seu passaporte. De seguida, o sistema procede a uma comparação das duas imagens assegurando que a pessoa apresenta o seu documento de identidade correspondente à imagem facial armazenada na documentação[97].

De seguida, temos a identificação de uma pessoa – esta identificação envolve uma comparação de um modelo biométrico singular de uma pessoa com uma base de dados de imagens faciais a fim de encontrar a identidade correspondente à pessoa. Esta identificação pode tratar-se de uma comparação "um para muitos" ou uma comparação "muitos para muitos" em situações onde o cenário de vigilância em que são encontradas várias imagens faciais na imagem. Os sistemas de reconhecimento facial podem operar em tempo real "live" ou em retrospetiva "post". Exemplos comuns deste tipo de utilização no domínio da polícia e da segurança em tempo real[98] incluem um sistema de câmaras que analisa as pessoas que passam e comparam os seus traços faciais com a imagem de outras pessoas contidas numa lista de interesse já armazenada[99].

Ainda no âmbito da identificação, podemos ainda enunciar a identificação em caso de pena de prisão – onde é realizado a colheita de dados biométricos, nomeadamente a impressão digital e uma foto que permite a identificação, posteriormente essa fotografia é armazenada num banco de dados que pode ser usada futuramente para consultas. Esta imagem também pode ser partilhada com outros órgãos policiais com objetivos similares.

Temos ainda a identificação de pessoas em situação de investigação: no caso em concreto se existir a possibilidade de acesso a uma fotografia ou a um vídeo do rosto da pessoa durante o processo de investigação procede-se à análise da mesma através do sistema de reconhecimento facial de forma a obter pistas ou informações. Se, não

[97] Esta categoria de utilização de sistemas de reconhecimento facial tem um menor impacto na vida das pessoas na medida em que o único pressuposto é confirmar se o individuo é a pessoa que afirma ser seja para efeitos de acesso a um sistema; instalação ou para desbloquear um dispositivo para utilização.
[98] A identificação em tempo real tem sido muito discutida uma vez que é uma tecnologia intrusiva na medida implica uma recolha de dados sensíveis à distância e sem o conhecimento da pessoa. As críticas feito a este rastreio em tempo real é a possibilidade de afetar direitos humanos nomeadamente o direito à privacidade.
[99] LYNCH, Nessa (2024) - *Facial Recognition Technology in Policing and Security - Case Studies in Regulation* in Laws, pp 3-4, [consultado a 5.11.2024]. Disponível na internet https://www.mdpi.com/2075-471X/13/3/35.

obstante, não for possível uma correspondência, a fotografia poderá ser arquivada para o futuro[100].

Para além dos usos mencionados, os sistemas de reconhecimento facial também podem ajudar na categorização e reconhecimento de emoções que tem subjacente a extração de informações demográficas da imagem facial de uma pessoa. Dentro desta categoria podem ser incluídos fatores como a étnica, o sexo ou a idade[101]. Relativamente ao reconhecimento por emoções também denominado como reconhecimento de emoções faciais tem subjacente a possibilidade de deteção de emoções através de uma leitura e análise dos rostos das pessoas. Estas técnicas são utilizadas em contextos de policiamento e segurança, nomeadamente na análise e deteção de emoções em multidões de forma a prever riscos ou a potencial criminalidade[102].

6. LIMITAÇÕES NO USO DO RECONHECIMENTO FACIAL

Em relação à possibilidade dos controlos externos que podem ser utilizados em relação às pessoas os sistemas de reconhecimento facial têm assumido um papel primordial em relação a outros métodos de reconhecimento biométrico na medida em que não são invasivos em razão de requererem pouca ou nenhuma cooperação do sujeito, sendo que quando a tecnologia de reconhecimento facial funciona em espaços públicos o consentimento da pessoa é muito difícil de obter e, pelo facto do sistema não estar sujeito a alterações de comportamento sejam elas voluntárias ou não por parte da pessoa sujeita ao reconhecimento.

Embora o reconhecimento facial esteja associado a benefícios reais na sua aplicação desde a verificação da identidade de uma pessoa para fins de segurança pública e de eficiência; a uma maior proteção que oferece em tempo útil como por exemplo a maior eficácia e rapidez para detetar fraudes ou roubos de identidade ou

[100] MEZZOMO, Maria Luiza (2024) - *O Uso Do Reconhecimento Facial Na Investigação Criminal E Na Segurança Pública,* Edições Almedina, pp.24-25
[101] Estes casos de utilização podem de alguma forma gerar preocupações em relação à idade de género ou à sexualidade.
[102] LYNCH, Nessa (2024) - *Facial Recognition Technology in Policing and Security - Case Studies in Regulation* in Laws,p.4, [consultado a 6.11.2024]. Disponível na internet: https://www.mdpi.com/2075-471X/13/3/35

mesmo encontrando pessoas que se encontram desaparecidas, o seu desenvolvimento não obstante tem vindo a suscitar preocupação que decorre das próprias caraterísticas dos sistemas de reconhecimento facial; questões relacionadas com a utilização e exatidão desta tecnologia e o impacto que poderá ter nos direitos fundamentais resultando numa posição de fraqueza das pessoas cujas imagens faciais são captadas e depois comparadas com uma "lista de vigilância".

Para além das razões já enunciadas um dos problemas que se tem colocado relativamente à utilização destes sistemas acentua na identificação biométrica "em tempo real" de pessoas singulares para efeitos de aplicação de lei. Esta questão é bastante sensível na medida em que é muito intrusiva para os direitos e liberdades das pessoas prejudicando o direito à intimidade da vida privada de cada um que é sujeito a esses sistemas devido à sensação de vigilância constante. De acordo com o Regulamento da União Europeia 2024/1689, de 13 de Junho de 2024, a identificação à distância tem tido imprecisões técnicas pelos sistemas de inteligência artificial determinando resultados incorretos podendo gerar efeitos discriminatórios nomeadamente em aspetos relacionados com a idade, etnia, sexo, raça ou deficiência. Além de que, a necessidade de maiores controlos ou correções associadas à utilização desses sistemas que operam em "tempo real" originam riscos para os direitos e liberdades das pessoas em causa pelas autoridades responsáveis pela aplicação da lei. Seguindo este pensamento o Regulamento da (UE) proibiu a utilização desses sistemas para aplicação da lei, com a exceção de situações definidas de modo restrito e em casos onde se demonstre que é estritamente necessário seja por motivos de interesse público relevantes e cuja importância predomine sobre os riscos[103].

É importante salientar que determinar o nível e a exatidão do software de reconhecimento facial ainda é um desafio na medida em que existem diferentes e variadas formas de avaliar e determinar a autenticidade do mesmo, dependendo do objetivo, da tarefa atribuída e do seu próprio contexto de utilização. Ao usar o reconhecimento facial em locais frequentados por milhões de pessoas como em estações de comboios/autocarros; aeroportos, uma proporção ainda que pequena de possibilidade de erro por exemplo 0,01% ainda é traduzida em centenas de pessoas que foram erroneamente assinaladas por estes sistemas. Foi inclusive salientado por

[103] Cfr. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial

estudos empíricos que demonstraram que o desempenho técnico da maioria dos sistemas de reconhecimento facial ainda continua com limitações inclusive na deteção de imagens faciais. As taxas de erro podem ser significativas em particular quando as fotografias que são comparadas entre si contêm iluminação, sombras, fundos, poses ou expressões diferentes; quando são imagens de baixa resolução ou os sistemas de reconhecimento facial são menos exatos e quando existam grandes discrepâncias de idade (por exemplo comparar a imagem de uma pessoa na idade jovem e depois compará-la 10 anos depois). Associados a estas questões da possibilidade de erro, temos que existem diferentes formas de calcular e de interpretar as taxas de erro para além de que quando falamos de exatidão de erros ainda temos os problemas associados à precisão[104] e à facilidade com que um sistema pode ser enganado através de por exemplo imagens faciais falsas.

As tecnologias de reconhecimento facial continuam a apresentar muitas dificuldades em situações onde é feita a comparação com gémeos ou pessoas que tenham uma geometria de rosto muito próxima, acabando por os confundir. Estes erros são facilmente cometidos por estes sistemas, é suficiente por exemplo que exista quantidades e qualidades desiguais de dados; quantidades diferentes de rostos de diferentes grupos sociais ou se for um sistema treinado com milhões rostos masculinos e milhares de rostos femininos ou pessoas de outras etnias aí os sistemas claramente não vão ter o mesma capacidade de exatidão nestes últimos dois grupos levando consequentemente a uma maior possibilidade de erro também determinado como viesamento algorítmico[105].

A utilização do reconhecimento facial implica uma recolha de informações particularmente sensíveis sobre um grande número de pessoas o que implica riscos de segurança em torno da recolha e conservação de dados de reconhecimento facial tal como o risco de violação e utilização indevida dessas informações.

---

[104] Em 2020 várias empresas de tecnologia como a IBM, Amazon e a Microsoft revelaram que iriam fazer uma pausa ou terminar as vendas do reconhecimento facial às agências de aplicação da lei e de segurança devido às preocupações de precisão e de privacidade. Nos Estados Unidos também houve alguns governos locais que proibiram qualquer departamento da cidade inclusive na aplicação da lei de utilização do reconhecimento facial como Somerville, Massachusetts, e São Francisco, Califórnia – cfr. SMITH, Marcus; MANN, Monique (2024) - *The Cambridge Handbook of Facial Recognition in the Modern State: Facial Recognition Technology and Potential for Bias and Discrimination* by Cambridge University Press, p.89. [consultado a 14.11.2024]. Disponível na internet: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B1C4A7F38AE00781EC8A559EFE48B3DF/9781009321198c7_87-95.pdf/facial-recognition-technology-and-potential-for-bias-and-discrimination.pdf.

[105] D'AGUIAR, Filipa Pais; GONZÁLEZ, José A.R.L. (2024) - *Direito Animalista, A Natureza e Além (Inteligência Artificial e Reconhecimento Facial)*, Dialética Editora, pp. 157-158

Como os autores José González e Filipa Aguiar dispõem de forma a assegurar a possibilidade de discriminação era recorrer à Lei 27/2021 – Carta Portuguesa de Direitos Humanos na Era Digital que dispõe no artigo 9 número 2: "2 - As decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei"[106].

É agora importante realçar que com os avanços que o reconhecimento facial têm demonstrado conjugando também o fomento da inteligência artificial têm vindo a suscitar fortes preocupações em torno dos direitos fundamentais.

7. RELAÇÃO ENTRE O RECONHECIMENTO FACIAL E OS DIREITOS FUNDAMENTAIS

7.1. RESPEITO PELA INTIMIDADE DA VIDA PRIVADA E PROTEÇÃO DE DADOS PESSOAIS

Os direitos à intimidade da vida privada e à proteção de dados pessoais são um dos direitos fundamentais que são colocados em causa na utilização dos sistemas de reconhecimento facial. Os sistemas de reconhecimento facial têm um grande impacto nestes direitos porque permitem a recolha e posterior análise de uma grande quantidade de dados biométricos. Esses bancos de dados podem ter utilidade para rastrear movimentos, para associações e comportamentos de pessoas, levantando preocupações relacionadas com o direito ao anonimato em locais públicos e o receio destas tecnologias serem utilizadas para fins além da segurança pública ou controlo social. Para além disso, são sistemas que operam à distância, o que significa que as pessoas podem ser identificadas ou rastreadas sem o seu consentimento pelo simples facto de se moverem em espaços públicos onde estão presentes estes sistemas.

[106] Idem, p. 158

Estes direitos têm vindo a ser descritos como um direito "clássico" à proteção da vida privada e um direito mais "recente/moderno" à proteção de dados. Embora sejam direitos que possam estar relacionados visto que ambos visam a autonomia e a dignidade humana, permitindo uma liberdade no desenvolvimento da personalidade; das formações e convicções e opiniões que são desenvolvidos na sua esfera pessoal, constituindo uma condição para o exercício de outros direitos fundamentais como a liberdade de pensamento, consciência e religião; liberdade de expressão; liberdade de informação e liberdade de reunião e de associação, no entanto são direitos distintos e autónomos[107].

O direito à intimidade da vida privada tem consagração constitucional no art. 26º; previsão no art. 80º do CC e no art. 8º da Convenção Europeia dos Direitos Humanos (CEDH). O direito à intimidade está diretamente ligado ao princípio da dignidade da pessoa humana que é tido como um princípio intrínseco de qualquer ser humano tendo subjacente valores como o respeito, a liberdade e a igualdade, traduzindo-se na qualidade de ser humano, permitindo que cada um beneficie de um espaço de privacidade seja no contexto doméstico; familiar e afetivo. Este conceito de "vida privada" compreende a integridade física e psicológica de cada pessoa, podendo abranger diversos aspetos da sua identidade física e social. O direito à intimidade privada é consagrado constitucionalmente logo após o direito à vida e à integridade da pessoa, disposto como "outos direitos pessoais" fazendo parte de um círculo que tem como fundamento a proteção de direitos nucleares da pessoa ou também designados como direitos de personalidades sujeitos a um regime garantístico previsto nos arts. 17º e seguintes e 24º e seguintes da CRP.

Segundo Jorge Miranda e Rui Medeiros, "a identidade pessoal é aquilo que caracteriza cada pessoa enquanto unidade individualizada que se diferencia de todas as outras pessoas por uma determinada vivência pessoal".[108] O direito à intimidade da vida privada tem subjacente um princípio da verdade pessoal, ou seja, cada pessoa deve viver a sua vida de acordo com os seus próprios princípios, com os valores com os quais se identifica. Este princípio, em última análise, também se encontra conectado ao princípio da proibição da não discriminação, previsto constitucionalmente no número

[107] FRA – European Union Agency for Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 22-23, [consultado a 11.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf .

[108] MIRANDA, Jorge; MEDEIROS, Rui (2017) – *Constituição Portuguesa Anotada Volume I*, 2ª edição revista, Universidade Católica Editora, p.444

2 do art. 3º da CRP, na medida em que o mesmo dispõe características que constituem a identidade pessoal de cada individuo[109].

A utilização de sistemas de reconhecimento facial em direto implicam uma recolha, uma comparação e posteriormente um armazenamento de imagens faciais numa base de dados para efeitos de identificação, acabando por afetar não apenas o direito à imagem das pessoas, mas também o direito à intimidade/privacidade[110], isto porque não falamos de intimidade apenas num contexto familiar, mas sim em espaços públicos, seja em estações ou em edifícios públicos, onde a pessoa continua no âmbito da sua esfera privada.

A capacidades que o reconhecimento facial tem de possibilitar o registo, a localização e os movimentos das pessoas levanta muitas questões no âmbito da privacidade, em particular quando se encontra associado ao armazenamento e processamento destes dados. A possibilidade de rastrear a localização representa que os governos ou autoridades que fazem uso desta tecnologia poderão estudar os hábitos, costumes, estilo de vida e movimentos associados a cada pessoa[111].

[109] Idem, p.444

[110] Seguindo esta ideia de recolha, tratamento e armazenamento de dados, o Tribunal Europeu no "CASE OF GAUGHRAN v. THE UNITED KINGDOM", processo 45245/15 de 13/02/2020, discutiu esta ideia abordando a possibilidade ou não de violação da intimidade da vida privada. No caso em apreço o requerente queixou - se da conservação por tempo indeterminado dos seus dados (no caso em concreto era o seu perfil de ADN, as suas impressões digitais e a sua fotografia) por tempo indeterminado constituindo uma interferência desproporcional e injustificada no direito ao respeito pela sua vida privada e familiar. O Tribunal Europeu mencionou que as autoridades públicas só poderiam interferir no exercício deste direito nos termos da lei e se tal fosse necessário numa sociedade democrática, no interesse da segurança nacional, da segurança pública ou do bem-estar económico do país, para a prevenção da saúde ou da moral ou para a proteção dos direitos e liberdades de outrem. O requerente foi condenado a uma infração menor sendo os seus dados biométricos conservados ao abrigo que disposições que não estabeleciam qualquer distinção em função da natureza ou gravidade da infração e ao qual o mesmo não tinha qualquer possibilidade de solicitar a supressão dos dados. Os Estados dispõem de uma margem de apreciação limitada para determinar os limites de conservação dos dados biométricos das pessoas condenadas. Em relação à questão de saber se as razões que foram invocadas pelas autoridades nacionais a fim de justificar a medida de conservação por tempo indeterminado eram "pertinentes e suficientes" o governo alegou que quanto mais dados fossem conservados, mais se prevenia a criminalidade, não obstante o Tribunal Europeu entendeu que o argumento apresentado para a conservação por tempo indeterminado equivaleria, na prática, a justificar a conservação de informações sobre toda a população e os seus familiares falecidos o que seria excessivo e irrelevante. Dessa forma o Tribunal entendeu que o Estado ultrapassou a margem de apreciação aceitável a este respeito tal como a conservação que constituía uma interferência desproporcionada no direito do requerente ao respeito pela vida privada não podendo ser considerada numa sociedade democrática violando dessa forma o artigo 8º da Convenção. [consultado a 08.01.2025]. Disponível na internet: https://hudoc.echr.coe.int/fre?i=001-200817.

[111] DUSHI, Desara (2020) - *The use of facial recognition technology in EU law enforcement: Fundamental rights implications* in Global Campus, South East Europe, p.6. [consultado a 21.01.2025]. Disponível na internet: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

O grau de intrusividade dos sistemas de reconhecimento facial e a violação da junção dos direitos à privacidade e à proteção de dados tem variações consoante a sua utilização em concreto, o que significa que em alguns casos a própria legislação nacional de cada Estado pode limitar a sua utilização ou mesmo proibir totalmente a sua utilização[112] sempre que a decisão tenha sido tomada por meio de um processo democrático[113].

O reconhecimento facial conjugando o avanço da biométrica permite de forma constante recolher dados altamente sensíveis e pessoais conduzindo a resultados cada vez mais invasivos para a privacidade individual e para a proteção de dados pessoais previsto no art. 1º da Carta dos Direitos fundamentais da União Europeia que estabelece que todos os cidadãos da União Europeia têm direito à proteção dos seus dados pessoais e no número 1 do art. 16º do Tratado sobre o Funcionamento da União Europeia (TFUE).

O direito à intimidade da vida privada e a proteção dos dados pessoais é uma questão fulcral nomeadamente nos casos em que esse tratamento de dados é realizado sem o consentimento das pessoas em causa como é o caso do reconhecimento facial que em diversos casos obtém a aquisição de dados com ausência total de consentimento prévio ficando o mesmo privado de qualquer forma ou poder de controlo sobre a divulgação das suas informações pessoais[114]. O tratamento de dados deve ser submetido a um teste de necessidade e proporcionalidade, deve ter subjacente uma base jurídica clara e um objetivo legitimo.

Para este efeito temos o Regulamento geral sobre a proteção de dados (RGPD) da União Europeia enuncia, desde logo, nas disposições gerais no art. 1º as regras relativas à proteção de dados pessoais tende sempre subjacente os direitos e liberdades

---

[112] O IEEE: Public Safety Technology em *Ethical Considerations in the Use of Facial Recognition for Public Safety* refere que existem medidas que têm como fim a proteção da intimidade/privacidade apesar da eficiência ser muitas vezes colocada em causa. Algumas jurisdições têm implementado formas de sinalização clara que permite informar as pessoas quando tencologias de reconhecimento facial estão operacionais. Outros medidas foram mais rigorosas e implementaram políticas rigorosas de retenção de dados, limitando um período de tempo pelo qual as informações biométricas podiam ser armazenadas. [consultado a 03.02.2025]. Disponível na internet: https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety.

[113] Council of Europe (2021) - *Guidelines on facial recognition*, p.8. [consultado a 13.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

[114] CURRAO, Elettra (2021) - *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance* in Diritto Penale e Uomo (DPU) - Criminal Law and Human Condition, p.11, [consultado a 14.11.2024]. Disponível na internet: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

fundamentais em particular no direito à proteção dos dados pessoais. Relativamente ao tratamento dos dados biométricos vem dispor nos termos do art- 9º número 2 al. G o seguinte:

> "se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados"[115].

O que significa que o processo tanto de recolha como de tratamento e armazenamento de dados deve estar em conformidade com a legislação da União Europeia[116] norteando os princípios fundamentais em matéria de proteção de dados. De acordo com os princípios jurídicos da proteção de dados, o tratamento das imagens faciais deve seguir os seguintes princípios:

a) Um dos princípios é a licitude, lealdade e a transparência – as informações claras e a prestação transparente é importante quando falamos dos sistemas de reconhecimento facial em direto na medida em que por norma as imagens são captadas em locais públicos através de câmaras sem que haja o consentimento das pessoas em causa. O RGPD inclui disposições que permitem garantir estes princípios exigindo um tratamento equitativo, com informação adequada em relação ao titular dos dados
b) Cumprir uma finalidade determinada, explicita e legitima, não sendo possível posteriormente ser tratados de forma contrário a essas finalidades pré-determinadas
c) Cumprir as exigências de minimização, exatidão, limitação da conservação, segurança e responsabilidade dos dados[117].

[115] Cfr. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

[117] Cfr. Art. 5º do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

Os responsáveis pela análise e tratamento dos dados devem tomar as medidas adequadas para fornecer as informações adequadas sobre o tratamento dos dados, de forma concisa, transparente e inteligível, segundo o número 1 do art. 12º do RGPD.

Visto que a extração de modelos biométricos a partir de imagens digitais acarreta consigo o tratamento de dados sensíveis, é essencial que exista uma base jurídica segura que pode variar tendo em conta os diferentes setores onde estes sistemas sejam utilizados. Em específico quando se trata de situações onde a utilização se baseia em imagens descarregadas da internet, seja através de redes sociais; sites de gestão de fotografias ou captadas através de câmaras de videovigilância não podem ser consideradas ações lícitas pela razão destes dados pessoais se demonstrarem disponíveis pelas pessoas em questão. É importante que o próprio legislador possa garantir que as bases de dados de imagens digitais inicialmente utilizadas para outros objetivos só possam usadas para retirar modelos biométricos e constituir sistemas biométricos quando for essencial para fins legítimos com carácter urgente, com previsão na lei, e que revista os critérios da necessidade e proporcionalidade a esses fins[118].

A necessidade de utilização dos sistemas de tecnologia de reconhecimento facial deve ser avaliada simultaneamente com o princípio da proporcionalidade em relação ao objetivo que pretende ser alcançado e calculando os possíveis impactos sobre os direitos das pessoas em causa. Deve, nesta medida ser criado um quadro jurídico aplicável ao tratamento de dados biométricos através do reconhecimento facial para os diferentes casos de utilização. Dessa forma, o quadro jurídico deverá conter para cada utilização diferente aspetos como uma explicação pormenorizada sobre a utilização especifica e qual o fim que pretende ser atingido com a utilização deste sistema; a fiabilidade e a precisão mínima do algoritmo a utilizar; o período de tempo pelo qual as fotografias utilizadas serão conservadas; garantias na utilização deste sistema; a rastreabilidade do processo e a possibilidade de controlo destes parâmetros[119].

Também na Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal (Convenção 108º+) dispõe no art. 6º que o tratamento de categorias especiais de dados como é o caso dos dados biométricos, só é permitido se esse tratamento tiver uma base jurídica que seja adequada e se o direito

[118] Council of Europe (2021) - *Guidelines on facial recognition,* p.9. [consultado a 14.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751
[119] Council of Europe (2021) - *Guidelines on facial recognition*, p.7. [consultado a 13.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

nacional de cada Estado consagrar garantias complementares e apropriadas, sendo as mesmas idóneas aos riscos e interesses inerentes tal como aos direitos e liberdades que se visa proteger[120]. Tem acontecido que em alguma legislação este tipo de tratamento é considerado expressamente proibido sendo a sua aplicação permitida a título excecional e em situações muito especificas, por exemplo com o consentimento explícito das pessoas; para proteção dos seus interesses fundamentais ou quando esse tratamento é indispensável para razões de interesse público mas sempre sob a reserva de garantias adequadas em relação aos riscos envolvidos[121].

É exigido que as pessoas sejam informadas sobre a identidade e os dados de contacto do responsável do tratamento dos dados; prazos de conservação, direito de solicitar o acesso aos dados armazenados, como o direito de apresentar queixa a uma autoridade de controlo nos termos do art. 13º do RGPD, não obstante são previstas exceções[122] a este artigo de forma a não prejudicar ou obstruir investigações em curso; proteção da segurança pública e segurança nacional.

O Tribunal Europeu Dos Direitos Humanos, no "Caso S. e Marper vs. Reino Unido",também dispôs que a proteção das informações e dos dados pessoais era fundamental para que cada pessoa pudesse usufruir do direito ao respeito pela vida privada e familiar, disposição legal que é garantida pelo art. 8º. Cada Estado deve no seu direito interno ressalvar proteções e garantias que sejam idóneas a evitar a utilização dos dados pessoais de forma incompatível com as garantias previstas neste artigo. Não obstante quando se trate de proteção de dados pessoais que se encontrem sujeitos a tratamentos automáticos nomeadamente para uso de fins policiais a necessidade de maiores garantias é ainda mais crucial. A legislação interna de cada Estado deve inclusive garantir que esses dados armazenados sejam pertinentes e não excessivos tendo em conta os objetivos que pretendem ser prosseguidos; além do mais devem ainda oferecer garantias que os dados são protegidos contra a utilização indevida e abusiva. Em relação à conservação dos dados destinados à identificação das

[120] Cfr. Convenção 108 + : Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal. Decisão do Comité de Ministros (128.ª sessão do Comité de Ministros, Elsinore, 18 de maio de 2018). [consultado a 13.01.2025]. Disponível na internet: www.coe.int/cm.
[121] Council of Europe (2021) - *Guidelines on facial recognition*, p.7, [consultado a 13.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.
[122] LISBOA, TRIBUNAL DA RELAÇÃO - Acórdão do Tribunal da Relação de Lisboa, processo 8777/21.3T8LSB.L1-7, relator: Luís Filipe Pires de Sousa, 14-09-2021, dispõe: "III–Segundo o TEDH, pode haver interesse legítimo na partilha de informações, mesmo que impliquem alguma devassa da privacidade ou intimidade de alguém, relativas a questões de saúde pública, administração da justiça, cumprimento das obrigações fiscais, criminalidade, proteção ambiental ou desporto".

pessoas em causa devem manter-se no período estritamente necessários para os fins relativamente aos quais esses dados são armazenados. É importante realçar que todas as considerações tecidas anteriormente são especialmente válidas no respeito à proteção de categorias de dados especiais mais sensíveis[123].

Estas situações são muito relevantes quando são utilizados sistemas de reconhecimento facial, porque no fundo e o que tem sido recentemente debatido para o uso destas tecnologias é que funcionem sem o consentimento informado ou optando por não o fazer, no caso de por exemplo se trate de suspeitos de crimes. Esta exceção/limitação do direito fundamental de ser informado e juntando o não acesso aos dados armazenados tem obrigatoriamente de ser fundamentado[124]. A violação de informações contidas em bancos de dados pode submeter as pessoas a outros crimes como roubo de identidade; perseguição ou outras formas de assédio.

Uma forma de equilibrar por um lado as preocupações com a ordem pública e com a segurança e por outro lado as questões relacionadas com os dados é aumentar o uso de tecnologias que aumentem a privacidade, isto é, alguns sistemas utilizam técnicas de criptografia assegurando que os dados faciais sejam anónimos e não possam estar associados a identidades individuais sem que haja autorização. Outra solução que pode no fundo assegurar estes direitos seria a limitação do uso do reconhecimento facial a situações especificas que comportassem alto risco ao invés de o implementarmos de forma universal. O que se pretende é que haja uma agregação de mecanismos/formas de salvaguarda tecnológica; restrições legais e supervisão pública que garanta que estes mecanismos são utilizados de forma correta respeitando os valores humanos e os princípios democráticos, ou seja, um sistema adequado que forneça proteções robustas para a privacidade de cada pessoa e segurança dos dados[125].

---

[123] TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, 4 de Dezembro de 2008, 30562/04 e 30566/04 "**CASE OF S. AND MARPER v. THE UNITED KINGDOM",** [consultado a 06.01.2025]. Disponível na internet: https://hudoc.echr.coe.int/fre?i=001-90051.

[124] FRA – European Union Agency for Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, p.25, [consultado a 13.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf .

[125] IEEE: Public Safety Tecnology: *Ethical Considerations in the Use of Facial Recognition for Public Safety*, [consultado a 03.12.2025]. Disponível na internet: https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety.

7.2 O DIREITO À PROTEÇÃO DA DIGNIDADE HUMANA

A dignidade da pessoa humana também é um direito suscetível de estar em risco com a tecnologia de reconhecimento facial. Como já fomos mencionando o reconhecimento facial tem subjacente pela sua própria natureza e características a afetação da esfera mais íntima das pessoas envolvidas, em particular, quando falamos da vigilância em tempo real em que o sistema tem a capacidade de captar milhões de imagens envolvendo um número indeterminado de pessoas mesmo que estas sejam completamente alheias à finalidade da atividade de identificação comportando um risco de sentirem uma violação da sua dimensão pessoal através de uma aquisição ilegítima dos seus dados. Desta forma, as pessoas podem sentir-se controladas acabando por limitar as suas atividades diárias e quotidianas inclusive as mais elementares[126].

7.3 DIREITO À IMAGEM

O direito à imagem é um dos direitos mais afetados no uso das tecnologias de reconhecimento facial, nomeadamente, pelos perigos que estão subjacentes a essa utilização como a impossibilidade das pessoas que são objeto da vigilância não se puderem pronunciar sobre o uso dos seus dados. Não obstante o facto de este direito ser em parte indisponível, a necessidade do consentimento da pessoa visada pretende também proteger outros direitos fundamentais que se encontram com ele interligados como os direitos à privacidade, ao bom nome e à reputação[127].

Segundo os autores Jorge Miranda e Rui Medeiros, “cada pessoa pode autodefinir a possibilidade de utilização, ou não, dos registos, por fotografia ou filme, da sua própria imagem”. Há um direito ao controlo da utilização dos registos da própria imagem exterior”[128].

---

[126] CURRAO, Elettra (2021) - *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance* in *Diritto Penale e Uomo* (DPU) - Criminal Law and Human Condition, p.11, [consultado a 14.11.2024]. Disponível na internet: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

[127] PEREIRA, Diana Silva; ALVES, Catarina Paulino; FERREIRA, Teresa - *O DIREITO À IMAGEM: TODA A IMAGEM TEM O SEU PREÇO* in Carlos Pinto de Abreu e Associados, p.2 [consultado a 18.11.2024]. Disponível na internet: https://carlospintodeabreu.com/public/files/35_societario_direito_imagem.pdf.

[128] MIRANDA, Jorge; MEDEIROS, Rui (2017) - *Constituição Portuguesa Anotada Volume 1,* p.451

Este direito encontra-se previsto constitucionalmente na nossa lei fundamental e dispõe o seguinte:

> "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação"[129].

Também de acordo com a jurisprudência:

> "O direito à imagem configura um bem jurídico-penal autónomo, tutelado em si e de per si, independentemente da sua valência do ponto de vista da privacidade/intimidade (...) Trata-se de um bem jurídico eminentemente pessoal com a estrutura de uma liberdade fundamental e que reconhece à pessoa o domínio exclusivo sobre a sua própria imagem".[130]

Para além do direito à imagem se encontrar constitucionalmente consagrado, também o código civil regula esta matéria dispondo que "O retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela; depois da morte da pessoa retratada, a autorização compete às pessoas designadas, segundo a ordem nele indicada"[131]. Ainda no que diz respeito ao consentimento, o retrato de uma pessoa não pode ser exposto sem o consentimento da mesma. Este consentimento será válido e eficaz respeitando os preceitos legais 81º e 340º do CC.

Nos termos do art. 81º do CC, temos o consentimento que pode distinguir-se do que se encontra nos termos do art. 340º do CC. Neste último, a pessoa que consente a autolimitação voluntária de um direito de personalidade não permite, a ingerência de terceiros se forem contrários à ordem pública. Este consentimento previsto neste artigo opera uma cláusula de exclusão de ilicitude, ou seja, aquele que pratica o ato não tem o direito de provocar o que acontece e que beneficia da tolerância daquele contra quem o ato foi praticado. Já o consentimento na previsão legal do art. 81º do CC dispõe que a restrição resulta de um contrato que é celebrado entre a pessoa a quem autoriza e

[129] Cfr. Art. 26º da CRP
[130] Cfr. ÉVORA, TRIBUNAL DA RELAÇÃO - Acórdão do Tribunal da Relação de Évora de 29-05-2012, processo número 253/07.3 JASTB.E1
[131] Cfr. Art. 79º número 1 do CC

quem a causa, sendo que quem beneficia do consentimento tem a possibilidade de exigir à outra parte os efeitos jurídicos relacionados com a execução[132].

Não obstante, o próprio legislador estatui algumas exceções a esta regra[133], permitindo, assim, em casos em concreto a captação e divulgação da imagem independentemente do consentimento do titular visado. As razões enunciadas abrangem as hipóteses de notoriedade – no caso em concreto referimo-nos à chamada "figura pública" cujo critério é definido tendo em conta a regularidade com que a pessoa surge, designadamente nos meios de comunicação ou pela função que ocupa, sendo que não se trata de qualquer cargo público, mas sim de um cargo ao qual esteja associado uma certa publicidade[134]; exigências relacionadas com a polícia ou de justiça – sendo uma referência que à partida parece ser insuficiente. A exceção poderá ser utilizada em casos de detenção pela prática de um crime, através da comunicação, seja de retratos-robô ou através do recurso de técnicas de reconhecimento facial. Contudo, há de cingir-se à prevenção de perigos [135].

Uma última razão deve-se ao próprio contexto em que a imagem é captada sendo o consentimento dispensado como uma imagem recolhida num local público. São situações que permitem excluir a tipicidade ou a ilicitude da conduta da pessoa que capta a imagem sem o consentimento. No entanto, é importante referir que para que a ilicitude seja afastada, supõe-se que a imagem da pessoa esteja integrada na imagem de um evento ou num espaço público, ou seja, tenha sido intercetada pela pessoa que captou a imagem[136], se, por exemplo, a objetiva de uma câmara for apontada para uma pessoa em específico que se encontre numa bancada de um estádio desportivo, apenas será possível fotografar ou filmar se a mesma consentir (seja de forma tácita ou expressa), porque é dado destaque àquela pessoa em concreto permitindo a sua individualização[137]. Como já foi mencionado, subjacente ao uso das tecnologias de

[132] GONZÁLEZ; José A.R. Lorenzo (2022) - *Reconhecimento Facial (FRT) e direito à imagem* in Revista da Faculdade de Direito da Universidade de Lisboa, Vol. LXIII nºs 1 e 2, pp. 581-582, [consultado a 18.11.2024], disponível na Internet: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Jose%CC%81-A.-R.-Lorenzo-Gonza%CC%81lez.pdf

[133] As exceções que se encontram previstas relativamente à não necessidade de consentimento da pessoa não tem aplicação se a captação ou divulgação da imagem significar o desrespeito à honra, reputação ou decoro da pessoa.

[135] Idem, pp. 584-585

[136] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial,* p.90

[137] GONZÁLEZ; José A.R. Lorenzo (2022) - *Reconhecimento Facial (FRT) e direito à imagem* in Revista da Faculdade de Direito da Universidade de Lisboa, Vol. LXIII nºs 1 e 2, p 585, [consultado a 18.11.2024].

reconhecimento facial, está essencialmente a individualização da pessoa de forma a permitir a sua identificação, razão pela qual não podemos enquadrá-la nesta disposição legal.

As questões levantam-se, essencialmente, pelo campo e âmbito de aplicação destas exceções e, devido à ausência de instrumentos legais explícitos que regulem a captação e a eventual difusão de imagens e à impossibilidade de as mesmas poderem ser incluídas nas exceções enunciadas e reguladas pelo art. 79º do CC existe possibilidade de afirmar que são ilícitas, era necessário que o legislador regulasse, por um lado, o direito à imagem e por outro lado os sistemas de reconhecimento facial, permitindo uma conciliação entre ambos. Desta forma, podemos concluir que o direito à imagem só pode ser posto em causa por situações que são legalmente tipificadas ou por razões de repressão criminal[138].

7.4 DIREITO DE AUTODETERMINAÇÃO DO TITULAR

A recolha e o tratamento de dados biométricos podem colocar em causa o direito à autodeterminação da pessoa afetada, uma vez que o tratamento dos dados é feito sem que a mesma tenha conhecimento, ou seja, sem a possibilidade de conhecer e decidir de forma autónoma a forma como as suas informações são adquiridas e armazenadas. A forma como estes sistemas operam parece contrária ao que se encontra previsto no regime de proteção de dados, uma vez que o titular em causa tem sempre conhecimento de todas as informações e a forma como os seus dados são armazenados[139]. De facto, a forma como estes sistemas funcionam sacrifica o direito a uma livre escolha do titular dos direitos em causa, pelo que não existe consentimento do responsável sendo que nada exclui o facto de que se a pessoa tivesse sido informada não teria recusado o seu consentimento[140].

Disponível na Internet: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Jose%CC%81-A.-R.-Lorenzo-Gonza%CC%81lez.pdf

[138] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial,* p.91

[139] Cfr. Art.14 número 2 alínea G do Regulamento (UE) n.º 679/2016 de 27 de Abril

[140] CURRAO, Elettra (2021) - *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance in Diritto Penale e Uomo* (DPU) - Criminal Law and Human Condition, p.12, [consultado a 22.11.2024]. Disponível na internet: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

7.5 PRECONCEITOS E DISCRIMINAÇÃO

A exatidão dos sistemas de reconhecimento facial tem sido colocada em causa, na medida em que a sua precisão pode ser influenciada por diversos fatores, por exemplo fatores ambientais; ângulos das câmaras e resolução de imagem podem afetar a correta identificação. A qualidade e a quantidade de dados treinados que são usados para desenvolver algoritmos são essenciais. Tem-se vindo a verificar nos sistemas reconhecimento facial que sistemas treinados com conjuntos de dados diversos e representativos têm um melhor desempenho em diferentes grupos demográficos.

Os problemas que têm surgido descrevem através de estudos que as taxas de precisão tendem a ser mais baixos em certos grupos demográficos em particular os seus resultados são menos exatos quando é utilizada para a identificação de pessoas com o tom de pele mais escuro o que significa que em casos de utilização destas tecnologias pelas autoridades policiais pode resultar numa probabilidade de aumento de pessoas pertencentes a minorias étnicas identificadas e processadas por crimes que não cometeram. A utilização dos sistemas de reconhecimento facial tendo apenas como objetivo determinar a cor da pele, a religião ou outras convicções, o sexo, a origem racial ou étnica, a idade, a saúde ou a condição social de uma pessoa deve ser proibida a não ser que a própria lei assegure salvaguardas adequadas para evitar qualquer risco de discriminação[141].

Existem dados que permitem explicar o motivo de grupos minoritários serem passiveis de uma identificação incorreta ou a uma identificação excessiva, o mesmo estabelecido por estudos empíricos que demonstram o preconceito racial associado aos sistemas de reconhecimento facial. De forma a comprovar esta situação, em 2019 um relatório do Instituto Nacional de Normas e Tecnologia[142] descobriu que as taxas de precisão são significativamente mais baixas em rostos afro-americanos e asiáticos e que tinham entre 10 a 100 vezes mais probabilidade de serem incorretamente identificados em comparação com pessoas de rosto claro. Estes dados são confirmados

[141] Council of Europe (2021) - *Guidelines on facial recognition*, p.8 [consultado a 13.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

por outros estudos que vieram a concluir que a taxa de erro na identificação de mulheres de pele escura era de cerca de 35%, o que significa que era cinquenta vezes superior à dos homens brancos.

A explicação subjacente para a taxa de erros na identificação resulta dos dados onde os algoritmos se baseiam para efetuar a correspondência, tendo sido verificado que em os conjuntos de dados para treinar algoritmos são em média compostos por pessoas de pele mais clara. Consequentemente, existe a probabilidade de que os problemas de exatidão estejam relacionados com a representação étnica dos dados que são utilizados para criar e treinar os algoritmos. É essencial que seja tomada em conta a representação racial nos conjuntos de dados utilizados para fazer a correspondência, de forma a não constituir uma forma de discriminação e racismo seja ela de forma intencional ou por omissão.

Por exemplo, numa investigação policial em Detroit no ano de 2020 Williams, um homem afro-americano foi detido por um furto numa loja. Subjacente a essa detenção estava uma identificação feita através de reconhecimento facial, mais tarde verificou-se que tinha existido um erro na correspondência feita por fotografia da sua carta de condução através de imagens de videovigilância do local do crime que se encontravam distorcidas. Este exemplo salienta os riscos que a utilização do reconhecimento facial pode ter na incorreta identificação, este caso é um dos vários que ocorreram nos Estados Unidos e que de facto vieram chamar à atenção para o risco de existirem preconceitos raciais na utilização do reconhecimento facial.

Uma forma de lidar com viés dos sistemas de reconhecimento facial exige uma intervenção multifacetada, o que significa diversificar os conjuntos de dados que são utilizados para treinar algoritmos, assegurando que os mesmos contenham amostras representativas de rostos, de diferentes etnias, géneros e idades[143].

7.6 DIREITO A UM PROCESSO JUSTO E EQUITATIVO

[143] IEEE: Public Safety Technology - *Ethical Considerations in the Use of Facial Recognition for Public Safety,* [consultado a 03.02.2025]. Disponível na internet: https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety.

É importante focarmos para além dos direitos fundamentais que são afetados pelas técnicas de reconhecimento facial entendermos a forma como as próprias garantias processuais podem ser afetadas. O processo justo e equitativo tem subjacente o princípio fundamental do Estado de Direito Democrático, ou seja, para além do direito de obter uma decisão num tempo razoável[144] também estão incluídos outros direitos como o direito na igualdade de armas, o direito ao contraditório, o direito à fundamentação das decisões, o direito ao conhecimento e à previsibilidade dos dados processuais, o direito à prova[145], entre outros[146]. A ideia de processo justo e equitativo traduz-se num equilíbrio entre por um lado a acusação e a defesa, permitindo que ambas as partes sejam detentoras da possibilidade de expor os seus fundamentos perante o tribunal e chegar a uma decisão final justa, sendo que a mesma só será possível se ambos os sujeitos processuais tiverem a possibilidade de exercer o contraditório ou seja, de contestar as provas contra si apresentadas[147].

A aquisição e o posterior tratamento de dados biométricos nomeadamente quando os mesmos são obtidos com fins subjacentes à prevenção da criminalidade ou a sua utilização posterior num processo penal também pode prejudicar de forma significativa o direito a um processo justo e equitativo[148].

Segundo a jurisprudência do Tribunal Constitucional a expressão:

---

[144] Cfr. Art. 20º número 4 da CRP

[145] LISBOA, TRIBUNAL DA RELAÇÃO - Acórdão do tribunal da relação de Lisboa, de 16-02-2016, processo 176/06.3TNLSB.L2-1 com o relator Rijo Ferreira, sobre este conceito vai no mesmo sentido e dispõe o seguinte: " O conceito de processo equitativo é um princípio fundamental de qualquer sociedade democrática, profundamente imbricado com o Estado de Direito (rule of law), não havendo fundamento para qualquer interpretação restritiva e que visa, acima de tudo, defendendo os interesses das partes e os próprios da administração da justiça, que os litigantes possam apresentar o seu caso ao tribunal de uma forma efetiva; tem como significado básico que as partes na causa têm o direito de apresentar todas as observações que entendam relevantes para a apreciação do pleito as quais devem ser adequadamente analisadas pelo tribunal, que tem o dever de efetuar um exame criterioso e diligente das pretensões, argumentos e provas apresentados pelas partes e que a justeza (fairness) da administração da justiça, além de substantiva, se mostre aparente (justice must not only be done, it must also be seen to be done)".

[146] Tribunal Constitucional (31 de Maio de 2017) Acórdãos 99.º volume, acórdão nº 260/17, processo número 527/13, relator: Conselheiro Fernando Vaz Ventura, p. 257

[147] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência artificial*, p.102

[148] No mesmo sentido o Parlamento Europeu aprovou na resolução de 6 de Outubro de 2021 relativamente ao uso de tecnologias de reconhecimento que embora estas tecnologias sejam bastante promissoras em termos de eficiência, precisão e comodidade, a sua aplicação implicava no entanto diversos riscos para os direitos fundamentais e para as democracias assentes num Estado de Direito. Relativamente à utilização destes sistemas no processo penal, entende que os Estados-Membros em conjunto com a União devem garantir responsabilidade na utilização destas tecnologias no âmbito da justiça e aplicação da lei de forma a garantir transparência e acautelar a proteção dos direitos fundamentais evitando situações de discriminação, parcialidade ou preconceitos, sendo que as opções políticas devem respeitar os princípios fundamentais como a necessidade e a proporcionalidade a fim de assegurar a constitucionalidade de um sistema equitativo e humano. [consultado a 06.01.2025]. Disponível na internet: https://www.europarl.europa.eu/doceo/document/TA-9-2021-10-06_PT.html#sdocta2.

> "processo equitativo unifica assim um grupo de garantias referentes ao modo como o processo deve ser configurado. Enquanto o direito à tutela jurisdicional justifica a existência do próprio processo, a exigência de que o processo equitativo limita às configurações possíveis do respetivo procedimento. De modo que a garantia do processo justo ou equitativo constitui o princípio constitucional que mais intensamente vincula o legislador na conformação das formas de processo"[149].

De facto, um dos receios que se coloca tem haver com a possibilidade desses dados puderem ser utilizados para dar início a uma investigação, a um processo penal ou em situações mais graves na aplicação de medidas preventivas restritivas da liberdade pessoal. Têm sido feitos estudos que demonstram que estes sistemas mantêm margens de erro, para além disso o funcionamento destes sistemas que é feito através da utilização de algoritmos não é frequentemente explicável também denominada como "opacidade dos sistemas de inteligência artificial" que pode ser traduzida como situações em que existe a dificuldade ou em casos mais graves, a impossibilidade de entender a forma como determinados algoritmos atuam/optam por uma determinada escolha ou desenvolvem conclusões especificas, o que acaba por não permitir que o sujeito não consiga entender passo a passo de como funcionam e operam estes sistemas. A obscuridade e a impossibilidade de rastreamento do funcionamento dos sistemas de reconhecimento facial prejudicam o direito a um processo justo e a proteção judicial na medida em que não é possível contestar algo que não temos acesso, que não conhecemos[150], situações em que por exemplo existe a comparação de dois dados biométricos sem que haja a intervenção de um operador especializado não permitindo a possibilidade de exercer o contraditório.

De facto, podemos pensar em situações que se destinem, por exemplo, à identificação do sujeito que praticou um ilícito. A verdade é que, tratando-se de um processo justo e equitativo, deve ser assegurado à defesa a possibilidade do resultado que foi obtido pelo *software*, o que por vezes é negado pelo sistema frustrando a

[149] TRIBUNAL CONSTITUCIONAL (31 de Maio de 2017) Acórdãos 99.º volume, acórdão nº 260/17, processo número 527/13, relator: Conselheiro Fernando Vaz Ventura, p. 257

[150] CURRAO, Elettra (2021) - *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance in Diritto Penale e Uomo (DPU)* - Criminal Law and Human Condition, p.13, [consultado a 19.11.2024]. Disponível na internet: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

possibilidade de contestar a prova. No entanto de forma a equilibrar a restrição é o resultado dado pelo *software* ser submetido a uma validação por um operador especializado na área.

De facto, podemos concluir que existe restrições que podem ser verificadas quando o sistema atua por si só, sem qualquer supervisão de forma a verificar o resultado obtido, não obstante e como já foi referido a forma de "igualar" e permitir o respeito pelas garantias processuais é fazer intervir um sujeito qualificado na área[151].

7.7 DIREITO À LIBERDADE DE EXPRESSÃO, REUNIÃO E MANIFESTAÇÃO

Para além dos direitos fundamentais anteriormente citados, o uso das tecnologias de reconhecimento facial também pode afetar o direito à liberdade de expressão, reunião e manifestação nomeadamente quando os mesmos operam em tempo real. De facto a liberdade de expressão prevista no art. 37º da CRP traduz-se num direito fundamental de exprimir e divulgar o seu pensamento, é dos direitos fundamentais da democracia, encontrando-se igualmente previsto no número 1 do art.10º da CEDH "compreendendo a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver qualquer ingerência de quaisquer autoridades públicas" e a liberdade de reunião previsto no art. 45º da CRP e previsto no art. 11º da CEDH permitindo a liberdade de reunião e associação de forma pacífica em lugares públicos desde que não sejam para fins contrários à lei. Ambas as liberdades de expressão e reunião estão abrangidas pelo regime de liberdades e garantias.

O recurso ao uso destas tecnologias como forma de processar imagens captadas através de câmaras de vídeo vigilância são suscetíveis de interferir com a liberdade de expressão e de reunião na medida em que um dos aspetos necessários ao exercício desta liberdade é o anonimato[152].

[151] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência artificil*, pp.102-103

[152] O tribunal da Alemanha veio declarar ilegal a publicação de imagens que tivessem sido captadas em contexto de manifestações através de redes sociais em consequência dos efeitos negativos para a liberdade de associação – Cfr. FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2019) Facial recognition technology: fundamental rights considerations in the context of law enforcement, p. 29,

Quando estes sistemas são utilizados por autoridades de controlo em eventos/acontecimentos sociais podem tornar-se eventualmente instrumentos de repressão ou de outra forma, uma restrição a esses eventos. De facto, os sistemas de reconhecimento facial em especial em tempo real permitem captar e armazenar todas as imagens, não apenas as de pessoas já conhecidas por autoridades policiais o que pode de alguma forma restringe ou compromete a liberdade de pensamento e de reunião levando as pessoas a renunciar desses direitos fundamentais de forma a evitar estar incluído de forma injustificada num arquivo das forças de autoridade[153].

O facto de as pessoas terem conhecimento que estão a ser observadas por estes sistemas acaba por criar um efeito negativo levando a que as mesmas alterem o seu comportamento, sendo que essa alteração se pode traduzir em não expressarem os seus pensamentos da mesma forma ou num desencorajamento na participação em manifestações sendo contrários à liberdade de expressão e afetando de igual forma a liberdade de reunião[154]. O direito de reunião permite que as pessoas cooperem e comuniquem de forma coletiva e pacífica para a formação da sua sociedade, no entanto o uso do reconhecimento facial pode de alguma forma gerar um fenómeno de efeitos inibidores. Os efeitos de arrefecimento ocorrem quando as pessoas modificam o seu comportamento por motivos de preocupação com os sistemas de vigilância e com a possibilidade das consequências que podem advir se o comportamento for observado. Estes efeitos de arrefecimento são variados, podem por exemplo influenciar os locais de pesquisa; podem influenciar o que se lê; os locais que se frequenta. Estes efeitos inibidores afetam a forma como os indivíduos desenvolvem a sua identidade/personalidade. O próprio desenvolvimento da personalidade depende de fatores como a experimentação, a discussão, o debate e o desafio[155].

[consultado a 22.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf .

[153] CURRAO, Elettra (2021) Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance in Diritto Penale e Uomo (DPU) - Criminal Law and Human Condition, p.13, [consultado a 22.11.2024]. Disponível na internet: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

[154] FRA – European Union Agency for Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 29-30, [consultado a 22.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

[155] MURRAY, Daragh (2024) - *Netherlands Quarterly of Human Rights: Facial recognition and the end of human rights as we know them?* Volume 42, Issue 2, pp. 150-152 in SageJournals [consultado a 22.11.2024]. Disponível na internet: https://journals.sagepub.com/doi/epub/10.1177/09240519241253061.

É necessário que as autoridades no uso das tecnologias de reconhecimento facial sejam transparentes e que exista legislação que regule de forma a não comprometer o exercício destes direitos[156].

Neste contexto da utilização destes sistemas de reconhecimento facial poderem interferir com os direitos acima referidos apresentamos agora um acórdão do Tribunal Europeu dos Direitos Humanos *Glukhin v. Rússia* onde foi discutido a compatibilidade do reconhecimento facial com o direito ao respeito pela vida privada e a liberdade de expressão.

O acórdão em causa reporta uma situação que ocorreu em Moscovo de uma condenação administrativa pelo facto de não ter existido uma notificação às autoridades sobre a intenção de realizar uma manifestação individual com a "utilização de um objeto desmontado". No decorrer da investigação foi utilizado tecnologias de reconhecimento facial a fim de tratar dos dados pessoais do requerente.

No caso em apreço um ativista político, denominado como Konstantin Kotov em 12 de Agosto de 2019 foi detido pela polícia e acusado de repetição de violação de regras de "eventos públicos". Segundo as informações o requerente teria viajado segurando uma faixa que mencionava que enfrentaria até 5 anos de prisão. Segundo os relatórios policiais com o auxílio das unidades anti extremismo da polícia e através das gravações das câmaras CCTV que se encontravam instaladas na estação de metro conseguiu identificar o requerente. O requerente foi então acusado de infração administrativa por violação do procedimento estabelecido para realização de eventos públicos pelo facto de não ter apresentado uma notificação prévia às autoridades locais.

A 23 de Setembro de 2019, o Tribunal Distrital de Meshchanskiy de Moscovo tendo maioritariamente por base as capturas de ecrã do Telegram e as capturas de ecrã das gravações de videovigilância da estação de metro condenou o recorrente. Não concordando com a decisão o recorrente interpôs vários recursos, na qual baseava a sua contestação na ilegalidade das atividades de busca realizadas para o identificar, no

[156]FRA – European Union Agency for Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, pp. 29-30, [consultado a 22.11.2024]. Disponível na internet: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf .

contexto em que a Lei das Atividades de busca operacional não permitia a realização das atividades efetuadas para infrações administrativas tornando as provas obtidas inadmissíveis. Alegou igualmente que a situação violava o princípio da parcialidade e que a sua condenação por uma manifestação pacífica teria violado o seu direito à liberdade expressão, para além de que não houve qualquer alegação que demonstrasse que tinha sido criado algum risco quer fosse para a ordem pública, para a vida ou saúde de terceiros. A 30 de Outubro de 2019, o Tribunal da Cidade de Moscovo confirmou a condenação de recurso, justificando a sua decisão na violação do procedimento para a realização de eventos públicos, em particular por não ter apresentado uma notificação prévia.

O requerente apresentou queixa ao Tribunal Europeu dos Direitos Humanos referindo que existia uma violação dos direitos de liberdade de reunião e associação e direito à privacidade, argumentando que as buscas que tinham sido realizadas não eram legais, inclusive a lei relativa às atividades de investigação operacional (n. 144-FZ de 12 de agosto de 1995 - "OSAA") que estabelece os objetivos das atividades de busca operacional não possibilitava a realização de investigações de infrações administrativas; além disso a manifestação pacífica não acarretou nenhum risco para a ordem pública nem para a vida de terceiros não tendo sido efetuado qualquer avaliação sobre os possíveis riscos colocados pela manifestação a solo nem verificado se era necessário prendê-lo ou condená-lo . Por último, a sua condenação teve subjacente imagens que foram captadas através de sistemas de reconhecimento facial sem posteriormente a intervenção de uma autoridade que legitimasse a recolha dos seus dados.

Relativamente à liberdade de expressão do requerente o Tribunal dos Direitos Humanos considerou que a manifestação que foi feita pelo requerente foi indiscutivelmente pacífica e não perturbadora. A infração pela qual resultou a condenação consistiu apenas na não notificação às autoridades da manifestação individual não tendo por base mais qualquer outro elemento incriminatório. No mesmo seguimento também não foi provado que as ações praticadas pelo requerente causassem qualquer perturbação na vida normal ou noutras atividades que excedesse o que era normal nas circunstâncias. Também não houve alegações no sentido das suas ações representarem qualquer perigo para a ordem pública ou para a segurança. As autoridades não demonstraram grau de tolerância necessária em relação a manifestação a sua única preocupação foi a necessidade de punir o comportamento

ilegal o que, à luz da convenção e nos termos do art. 10º não é consideração suficiente, não existindo dessa forma razões suficientes que justifiquem a interferência do direito à liberdade de expressão do requerente, violando dessa forma o art. 10º da Convenção.

O requerente argumentou igualmente a violação do tratamento dos dados pessoais, incluindo a utilização de sistemas de reconhecimento facial violando o direito ao respeito da vida privada. Nesses termos invocou o art. 8º da Convenção que dispõe no seu número 2 que:

> "As autoridades públicas só podem interferir no exercício deste direito nos termos da lei se tal for necessário numa sociedade democrática, no interesse da segurança nacional, da segurança pública ou do bem-estar económico do país, para a prevenção da desordem ou da criminalidade, para a proteção dos direitos e liberdades de outrem"[157].

Relativamente ao uso de sistemas de reconhecimento facial o tribunal reconheceu que o sistema de reconhecimento facial foi utilizado, alegando que é essencial que na implementação desta tecnologia de reconhecimento facial exista regras detalhadas que regulem o alcance e a aplicação destas medidas, assim como mecanismos de salvaguarda contra a possibilidade de abuso e arbitrariedade, sendo estas garantias maiores quando o uso destas tecnologias for "em tempo real". Assumiu igualmente ter dúvidas relativamente às disposições de requisitos de "qualidade do direito", ou seja, a legislação nacional permite o tratamento de dados pessoais "no âmbito da administração da justiça", um conceito demasiado amplo. Não houve qualquer justificação, nem foi apresentado exemplos da interpretação e aplicação na prática administrativa e restritiva, o que parece que é permitido o tratamento de dados biométricos com a ajuda do reconhecimento facial em qualquer processo judicial, na medida em que a legislação nacional não impõe quaisquer limitações a esta natureza. O governo não apresentou nenhuma referência relativamente às garantias que estão subjacentes ao uso das tecnologias de reconhecimento facial, nem procedimentos de autorização, nem quaisquer mecanismos de controlo de supervisão.

Embora o Tribunal de Justiça julgue incontestável que os esforços na luta contra a criminalidade, em particular a criminalidade organizada e o terrorismo que são crimes com os quais as sociedades europeias atualmente se têm deparado e que, em grande

[157] Cfr. Convenção Europeia dos Direitos Humanos, art. 8º número 2

medida dependem do uso de técnicas e meios de investigação invasores. A questão que se colocou é se os dados biométricos por tecnologia de reconhecimento facial foram justificados nos termos do art. 8 paragrafo 2 da convenção, sendo que essa análise é determinada através de saber se foram “necessários numa sociedade democrática”.

No caso em apreço a polícia recolheu e armazenou as imagens do requerente e através delas extraiu e processou os dados biométricos com o apoio da tecnologia de reconhecimento facial. O tribunal considera estas medidas são muito intrusivas, particularmente no que diz respeito à tecnologia de reconhecimento facial ao vivo, o uso desta tecnologia “ao vivo” é necessário estar justificada como “necessária em uma sociedade democrática”. Os dados pessoais que foram tratados tinham inclusive informações sobre a participação do requerente no protesto contendo as suas opiniões políticas, podendo então ser enquadradas nas categorias de dados sensíveis às quais é necessária uma maior proteção. O tribunal considerou que o recurso às tecnologias de reconhecimento facial foi altamente intrusivo para identificar e prender o requerente da manifestação pacifica sendo que estas situações poderão ter um efeito inibidor em relação à liberdade de expressão e de reunião, sendo que o uso do reconhecimento facial a fim de localizar e prender o requerente enquanto o mesmo viajava de metro não correspondia a uma “necessidade social premente”.

Em suma, o tribunal terminou a sua fundamentação determinando que a utilização do reconhecimento facial foi altamente intrusiva no contexto do exercício do requerente na sua liberdade de expressão ao abrigo da Convenção, não obstante demonstrou ainda a incompatibilidade com os valores e ideais de uma sociedade democrática, existindo, portanto, uma violação do artigo 8º da convenção. Este acórdão do Tribunal Europeu demonstra a importância da necessidade de regulamentação de forma clara e proporcional no uso de sistemas de reconhecimento facial pelas autoridades de forma a evitar restrições injustificadas aos direitos e liberdades fundamentais como a privacidade e a liberdade de expressão. A não regulamentação e a ausência de salvaguardas e garantias adequadas podem significar violações a esses direitos conforme o que foi interpretado pelo Tribunal Europeu.

8. RESTRIÇÃO DOS DIREITOS FUNDAMENTAIS

É importante após descrevermos quais os direitos que podem ser afetados no uso dos sistemas de reconhecimento facial, explicar a possibilidade de restrição dos mesmos. Como sabemos o uso destas tecnologias e a sua eventual aplicação no processo penal para concretização dos fins processuais como a realização da justiça e a descoberta da verdade material implica uma restrição dos direitos.

Como foi descrito no capítulo anterior temos vários direitos que são restritos, desde logo o próprio direito à imagem com particular incidência quando se trata de sistemas "em tempo real" onde a imagem da pessoa é captada e armazenada sem qualquer consentimento ou conhecimento das pessoas em causa. Em consequência desse direito temos também o próprio direito à informação, a possibilidade de a pessoa ter consciência e puder ser informada e o direito à autodeterminação, ou seja, sem que de alguma forma possa controlar e decidir como as suas informações são tratadas. De igual forma temos o direito à liberdade de expressão, liberdade de manifestação e de reunião que implica que as pessoas obstem de se encontrar, de tomar certas atitudes ou opiniões por conta de terem consciência de que estão a ser vigiadas e que, daí pode resultar consequências para si mesmos, ou seja, efeitos inibidores que começam a ter cada vez mais peso no exercício e na prática destes direitos.

Relativamente à possibilidade de limitação e restrição de direitos fundamentais é possível afirmar que os mesmos não são direitos absolutos nem ilimitados mesmo quando falamos de direitos, liberdades e garantias. Não obstante é importante realçar que os limites que são feitos aos direitos fundamentais resultam, na maior parte das situações num "conflito" entre por um lado valores que são próprios dos direitos ou entre esses e outros valores comunitários no contexto do sistema constitucional[158].

Estas tecnologias de reconhecimento facial restringem estes direitos, que mesmo sendo direitos fundamentais não são tidos como direitos absolutos, podendo em algumas situações existir a possibilidade de serem limitados, restritos[159]. Não obstante

[158] ANDRADE, José Carlos Vieira de (2019) - *Os Direitos Fundamentais na Constituição Portuguesa* de 1976, 6ª edição, Edições Almedina, pp.261-262

[159] O mesmo entendimento é mencionado no Acórdão do Supremo Tribunal de Justiça, processo 96A901, 23.04.1996 que dispõe o seguinte: " Os direitos fundamentais não são absolutos nem ilimitados, pois que a própria Constituição admite a sua restrição, como decorre do preceituado nos ns. 2 e 3 do artigo 18. Posto é que tais restrições visem salvaguardar outros direitos ou interesses constitucionalmente protegidos, não diminuam a extensão e o alcance do conteúdo essencial dos preceitos constitucionais e respeitem o princípio da proporcionalidade". [consultado a 07.01.2026]. Disponível na internet:

essa possibilidade de restrição é um poder excecional, não apenas pelo facto de precisar de ser autorizado – também denominado como reserva de lei que é a exigência que permite uma restrição legítima dos direitos fundamentais, mas essencialmente porque não se justifica como uma regra, o que significa que nessas situações cabe ao legislador justificar a necessidade da restrição tendo por base situações ou casos em concreto impondo o sacrifício do direito fundamental[160].

Nos termos do art. 18º número 2 o legislador autorizou a possibilidade de restringir determinados direitos em alguns parâmetros ou para determinadas finalidades, dispondo o seguinte: "A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos", restrições também denominadas como restrições legais. Segundo os autores Jorge Miranda e Rui Medeiros:

> "para que se possa falar com propriedade em restrição é necessário que em primeiro, esteja definido com o mínimo de precisão, qual o objeto que se pretende restringir. E, juridicamente é óbvio que num direito fundamental não cabe tudo o que semanticamente poderia lá caber, existindo comportamentos ou pretensões que manifestamente não se encontram cobertas pela proteção concedida pela norma constitucional"[161].

A restrição de direitos fundamentais opera quando existe um confronto com direitos ou interesses constitucionalmente tutelados na constituição. Estes limites podem ter caráter absoluto o que significa que se impede um determinado fim ou o exercício de um direito ou pode ter um caráter relativo, ou seja, um condicionamento, um requisito cautelar relativamente ao qual depende o exercício do direito. É importante referir que este condicionamento não implica, no entanto, uma redução no âmbito material do direito, afetando por vezes uma disciplina ou uma limitação na liberdade do exercício do direito ou um ónus[162].

---

https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a893c17476226d7a802568fc003b4c0d?OpenDocument.

[160] ANDRADE, José Carlos Vieira de (2019) - *Os Direitos Fundamentais na Constituição Portuguesa* de 1976, p.284

[161] MIRANDA, Jorge, MEDEIROS, Rui (2017) - *Constituição Portuguesa Anotada Volume 1*, p.255

[162] Idem, pp. 255-256

A constituição determina um conjunto de condições de validade das leis restritivas, como o âmbito geral e abstrato; a impossibilidade de efeitos retroativos; a necessidade de as restrições serem necessárias à salvaguarda de outros direitos ou interesses legalmente protegidos, sendo proibido que essa restrição interfira na diminuição da extensão e do alcance do conteúdo essencial dos preceitos constitucionais[163]. O preceito constitucional do número 2 do art. 18º da CRP deve desta forma ser entendido como a consagração do princípio da proporcionalidade em sentido amplo, proibindo restrições que não sejam adequadas, necessárias e proporcionais aos direitos, liberdades e garantias ainda que essas restrições não afetem o núcleo essencial (absoluto) dos direitos.[164] Quando nos referimos a este limite absoluto do número 3 do art. 18º da CRP, o entendimento é que o mesmo corresponde a um princípio basilar de um Estado de Direito Democrático e que corresponde à dignidade da pessoa humana devendo ser encarado como um limite absoluto a essa restrição.

Daqui não podemos retirar que em relação à previsão legal do art. 18º que seja ilegítima a restrição que seja idónea a atingir o núcleo essencial de cada direito, deve entender-se como uma restrição não ao direito, mas sim ao preceito constitucional como norma de valor e garantia. Segundo o autor José Carlos Vieira de Andrade: "o que o legislador não pode, sob pena de ultrapassar este limite absoluto, é destruir ou restringir gravemente a liberdade física em geral ou a intimidade do cidadão comum"[165].

Em certas situações o valor da dignidade da pessoa humana pode ser de tal forma acentuada que implica que não possa existir a violação em nenhuma situação individual sem que ao mesmo tempo o conteúdo essencial desse preceito não seja também afetado, exemplo disso são o direito à vida; o direito à integridade física; o direito à identidade pessoal. Ao invés, temos por contrapondo outros direitos que por incidirem em aspetos representativos da vida doas pessoais já é possível em situações excecionais a sua anulação parcial[166].

Como já foi referido previamente, de acordo com a disposição legal do art. 18º número 2 da CRP, a restrição só pode operar por lei e com o fim de salvaguardar um

[163] Cfr. Artigo 18º números 2 e 3 da CRP
[164] ANDRADE, José Carlos Vieira de (2019) - *Os direitos Fundamentais na Constituição Portuguesa de 1976*, 6ª Edição. Edições Almedina, pp. 280-281
[165] Idem, pp. 282-283
[166] Idem, p.283

direito fundamental ou um interesse legalmente protegido. No entanto, para essa restrição acontecer é necessário respeitar algumas condições, desde logo o princípio da proibição do excesso ou princípio da proporcionalidade em sentido amplo na sua tripla vertente: o princípio da adequação que impõe que a restrição seja conforme à prossecução dos fins declarados pela lei; o princípio da necessidade que impõe que não sejam aplicadas restrições desnecessárias à prossecução dos fins pretendidos pelos preceitos legais o que significa que só serão exigíveis quando não exista a possibilidade de utilizar outros meios menos coativos e o princípio da proporcionalidade em sentido estrito, as restrições devem seguir uma forma de justa medida e não devem ser excessivas[167].

A diversidade de meios ocultos de investigação idóneos a causarem prejuízos de forma acentuada nos direitos fundamentais em particular a intimidade da vida privada; a privacidade implica que o aplicador do direito tenha um cuidado redobrado devido à tendência progressiva na utilização destes meios. A utilização desses meios em particular se o seu uso for por um período prolongado é passível de produzir um dano que "excede o resultante da soma desses meios", sendo incompatível com as exigências inerentes ao princípio da dignidade humana. É necessário a conformidade com os requisitos de proporcionalidade aferidos não apenas na análise de cada um dos meios que são utilizados, mas também nas consequências que o seu uso fará na esfera jurídica das pessoas visadas[168].

Após tudo o que foi referido anteriormente sobre a restrição dos direitos, é agora importante colocarmos esta temática da restrição no uso das tecnologias do reconhecimento facial.

É importante termos presente que qualquer restrição tem de ser assegurada por testes de legitimidade e, se for bem-sucedida só deve ter aplicação se for mesmo necessária e em circunstâncias proporcionais, ao invés se esta tecnologia for usada de forma desproporcional resultará em sentimentos de opressão e medo, de falta de liberdade podendo conduzir a mudanças forçadas de comportamento em espaços públicos com vigilância. Desta forma é crucial encontrar um ponto de equilíbrio entre por

[167] SUPREMO TRIBUNAL DE JUSTIÇA - Acórdão do Supremo Tribunal de Justiça, processo número 96A901 de 23-04-1996**.** [consultado a 8.01.2025]. Disponível na internet: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a893c17476226d7a802568fc003b4c0d?OpenDocument.

[168] ALBERGARIA, Pedro Soares de (2024) - *Comentário Judiciário Do Código De Processo Penal Tomo II, Artigos 124 a 190º*. 4ª edição. Edições Almedina, p.70

um lado o aumento da segurança que estes sistemas de reconhecimento facial podem garantir e as medidas tomadas[169].

A restrição de direitos liberdades e garantias previstas no art. 18º número 1 da CRP só será legalmente admissível para fins de investigação criminal na medida em que se verificar uma conjuntura de requisitos e condicionalismos[170] como a reserva de lei formal; o princípio da proporcionalidade em sentido amplo e a reserva de juiz[171] consagrados constitucionalmente[172].

Em Portugal, a jurisprudência tem abordado esta questão da restrição dos direitos fundamentais pretendendo um equilíbrio entre a necessidade de procurar a verdade material e a prossecução dos fins processuais e por outro lado a proteção dos direitos fundamentais dos cidadãos cujos seus direitos são colocados em causa, providenciando que qualquer condicionamento feito aos mesmos seja adequado, justificado e proporcional[173].

Por exemplo e partindo de jurisprudência que tem sido adotada relativamente ao uso de mecanismos e métodos mais sofisticados embora também mais prováveis de afetação de direitos fundamentais os tribunais têm seguido um determinado entendimento que os permite prosseguir os fins processuais e os princípios basilares do processo penal português, mas também salvaguardar a ingerência nos direitos fundamentais das pessoas[174].

---

[169] DUSHI, Desara (2021) - *The use of facial recognition technology in EU law enforcement: fundamental rights implications* in Global Campus, South East Europe, p. 6. [consultado a 21.01.2025]. Disponível na internet: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

[170] O mesmo entendimento é seguido pelo TRIBUNAL CONSTITUCIONAL – Acórdão número 155/2007, processo 695/06 que dispõe: " (...) Da vasta jurisprudência constitucional sobre a matéria decorre, em síntese, que qualquer restrição de direitos, liberdades e garantias só é constitucionalmente legítima se (i) for *autorizada pela Constituição* (artigo 18º, nº 2, 1ª parte) (ii) estiver suficientemente *sustentada em lei da Assembleia da República ou em decreto-lei autorizado* (artigo 18º, nº 2, 1ª parte e 165º, nº 1, alínea b), (iii) visar a *salvaguarda de outro direito ou interesse constitucionalmente protegido* (artigo 18º, nº 2, *in fine*); (iv) for *necessária* a essa salvaguarda*, adequada* para o efeito *e proporcional* a esse objetivo (artigo 18º, nº 2, 2ª parte); (v) tiver *carácter geral e abstrato*, *não* tiver *efeito retroativo* e não *diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais* (artigo 18º, nº 3, da Constituição)". [consultado a 29.01.2025]. Disponível na internet: https://www.tribunalconstitucional.pt/tc/acordaos/20070155.html.

[171] Cfr. Arts. 18 números 2 e 3; artigo 32 nº4 e artigo 165º número 1 alínea b) da CRP

[172] SILVA, Sandra Oliveira e (2021) - Legalidade da Prova e Provas Proibidas, pp. 545-591

Esta questão não é abordada desta forma apenas em Portugal, também a nível Internacional a legislação em matéria de direitos humanos exige que qualquer decisão que interfira com direitos humanos tenha de estar em conformidade com a lei; tenha de ser legitimo e de ser necessária conforme os princípios de uma sociedade democrática, o qual é referido no art. 29º número 2º da Declaração Universal dos Direitos Humanos que dispõe:

> "No exercício destes direitos e no gozo destas liberdades ninguém está sujeito senão às limitações estabelecidas pela lei com vista exclusivamente a promover o reconhecimento e o respeito dos direitos e liberdades dos outros e a fim de satisfazer as justas exigências da moral, da ordem pública e do bem-estar numa sociedade democrática".

Pensando na aplicação do reconhecimento facial, o que está em conflito é restrição de direitos como o direito à intimidade privada; o direito à imagem; a privacidade por um lado e o interesse comunitário e da administração da justiça por outro. A jurisprudência tem tido uma orientação no sentido de entender:

> "nada obsta a que o legislador estabeleça limites àqueles direitos fundamentais do recorrente para assegurar a execução e cumprimento da justiça penal, isto é, para assegurar uma justa exigência da ordem pública e do bem-estar geral, desde que, obviamente, os limites ou restrições não destruam ou afetem o conteúdo essencial daqueles direitos"[175].

Para a prossecução das finalidades do processo penal, e respeitando os condicionalismos impostos pela restrição de direitos fundamentais, a jurisprudência por exemplo no acórdão 254/99 dispôs que era possível a restrição do direito à intimidade da privada com previsão no art. 25º número 1 da Constituição se, fosse de interesse à descoberta da verdade material ou para fins de prova como por exemplo em situações de interceção e gravação de comunicações telefónicas. No entanto é importante quando se faz esta avaliação entre a restrição e os fins processuais entender se a medida será idónea à prossecução do fim; se a medida significou uma "menor desvantagem possível para a posição jusfundamental" e por fim se o resultado é ou não proporcional à carga coativa que comporta.

[175] Cfr. ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL número 155/2007, processo 695/06, [consultado a 29.01.2025]. Disponível na internet: https://www.tribunalconstitucional.pt/tc/acordaos/20070155.html.

Quando falamos no uso de tecnologias de reconhecimento facial, cujo objetivo é a captação de imagens e a sua posterior comparação com dados existentes em bancos de dados com o objetivo de uma identificação considero que mesmo ainda que este meio de prova possa afetar a esfera privada das pessoas, a restrição é passível de ser efetuada, desde que respeite os princípios basilares de um Estado de Direito. O Tribunal Europeu dos Direitos Humanos acerca do respeito pela vida privada dispôs no caso *Van der Velden v. the Netherlands*[176]. No caso em apreço, foi apresentado uma situação de recolha de dados pessoais em concreto amostras biológicas para retirar o ADN, sendo que o entendimento do tribunal foi que a obtenção do material biológico através do uso de uma zaragatoa na boca, a conservação desse material e posterior uso para determinar o perfil constituiriam uma ingerência no direito à vida privada. O art. 8º número 1 da Convenção Europeia dos Direitos humanos dispõe que: "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência", o que significava que tendo em conta o caso em apreço colidia com o art. 8º, não obstante esta restrição pode encontrar-se justificada desde que a sua ingerência esteja prevista na lei; seja necessária para assegurar a segurança pública, o bem-estar do pais; a ordem; a prevenção de crimes, proteção da saúde ou moral ou ainda a proteção de terceiros.

Ainda no contexto da possibilidade de restrição do à intimidade da vida privada também temos o acórdão do Tribunal Europeu no caso Klass e outros v. Alemanha[177] que analisou a questão da vigilância secreta de cidadãos determinando no caso em apreço que não existiria uma interferência por parte de uma autoridade pública no exercício deste direito, exceto se fosse conforme a legislação e respeitasse o princípio da necessidade numa sociedade democrática e tivesse como fim a segurança do país. No relatório, a comissão entendeu que vigilância secreta que se encontrava prevista na legislação alemã constituiria uma interferência no exercício do direito que se encontra previsto no art. 8º, primeiro paragrafo. A questão em análise foi se essa interferência se encontrava ou não justificada nos termos do número 2 do art. 8 que previa exceções, tendo de ser interpretado de forma restritiva. A vigilância secreta dos cidadãos,

[176] Cfr. ACÓRDÃO DO TRIBUNAL EUROPEU DOS DIEEITOS HUMANOS: case *Van der Velden v. the Netherlands,* processo 29514/05, 07/12/2006. [consultado a 29.01.2025]. Disponível na internet: https://hudoc.echr.coe.int/eng?i=001-78858.

[177] Cfr. ACÓRDÃO DO TRIBUNAL EUROPEU DOS DIREITOS HUMANOS: case of Klass and others, processo 5029/71, 06/09/1978, [consultado a 29.01.2025]. Disponível na internet: https://hudoc.echr.coe.int/fre?i=001-57510.

característica de um estado policial, só será admitida como aceitável à luz dos princípios da convenção se forem estritamente necessários a fim de garantir e salvaguardar instituições democráticas. No caso em apreço o tribunal começou por indagar se no caso em concreto essa vigilância que tinha sido operado pelo Estado Alemão tinha previsão legal; determinou em seguida se os requisitos do art. 8 número 2 tinham sido verificados que segundo o governo era "necessária numa sociedade democrática no interesse da segurança nacional" e "para prevenção de desordem ou crime" e para a "proteção dos direitos e liberdades e terceiros". O tribunal enunciou dois factos importantes aos quais também podemos relacionar com o uso do reconhecimento facial que tem haver primeiramente com os avanços técnicos dos próprios meios no caso em concreto de espionagem e consequentemente de vigilância e um segundo aspeto sobre a maior incidência de o crimes na Europa que têm ocorridos nos últimos anos nomeadamente crimes como o terrorismo. Os Estados devem ser capazes de combater essas ameaças assegurando assim a segurança e, dessa forma o Tribunal de Justiça tem aceitado a possibilidade de existirem legislações que permitem poderes de vigilância secreta sobre telecomunicações desde que de forma excecional e tendo sempre em consideração a necessidade numa sociedade democrática; no interesse da segurança dos Estados e para a prevenção dos crimes.

Não obstante o Tribunal de Justiça alerta que apesar dos Estados deterem uma discricionariedade ela é limitada na medida em que usada de forma incorreta pode significar a destruição da democracia, dessa forma seja qual for o sistema de vigilância adotado têm de ser asseguradas medidas adequadas e eficazes contra abusos. A apreciação feita é relativa na medida em que depende do caso em concreto; da natureza; do alcance e da duração das medidas e dos motivos necessários. Estas decisões demonstram a difícil tarefa que as jurisprudências enfrentam para equilibrar por um lado a prossecução dos fins processuais e por um lado garantir que qualquer restrição que seja feita aos direitos fundamentais seja necessária, proporcional e justificada numa sociedade democrática. É um outro exemplo que, apesar da vigilância secreta aos cidadãos implicar uma ingerência no direito à vida privada, no entanto, pode ter justificação por razões de segurança e prevenção do crime, desde que sejam asseguradas as garantias necessárias contra possíveis abusos ou más condutas.

Em relação ao direito à imagem que também é colocado em causa no uso do reconhecimento facial a jurisprudência portuguesa têm ponderado entre por um lado o

direito à imagem e a necessidade de restrições tendo por fim a prossecução de fins do processo penal, admitindo essa possibilidade desde que essa limitação seja necessária tendo em conta o contexto apresentado; seja justificada e proporcional. O acórdão do Tribunal Constitucional discutiu a possibilidade de restrição do direito à imagem numa situação em concreto onde tinham sido obtidas fotografias através de um sistema de videovigilância num local de acesso público sem o consentimento das pessoas visadas. Tendo em conta o caso em apreço o tribunal apreciou a questão no sentido de entender:

> "Sobre o recurso a estas imagens, a jurisprudência tem-se pronunciado maioritariamente, no sentido de que os fotogramas obtidos através de sistema de videovigilância existente em local de livre acesso ao público, não constituem meios proibidos de prova desde que exista causa justificativa para a sua obtenção, designadamente no âmbito da investigação da prática de ilícito criminal, posto que não está em causa a violação de direitos pessoais da pessoa visionada, mormente do direito à intimidade da vida privada e familiar, não dizendo respeito as referidas imagens, ao núcleo duro da vida privada das pessoas visionadas"[178].

De facto, e sendo o direito à imagem importante no âmbito dos sistemas de reconhecimento facial, o acórdão veio salientar que, apesar da sua importância em certas situações ele pode ceder aos fins processuais como a eficiência da justiça e a procura da verdade material. Também o acórdão do Tribunal da Relação do Porto entende que o CC consagra a possibilidade do consentimento não ser necessário se a reprodução da imagem se encontrar no âmbito do interesse público. No caso em concreto entendeu-se que o direito à imagem não podia prevalecer sobre a liberdade de imprensa e liberdade de expressão tidos como pilares fundamentais numa sociedade democrática, não tendo, dessa forma, uma natureza absoluta estando assim sujeita às limitações estabelecidas pela lei[179].

[178] Cfr. ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL, número 606/2024, processo 440/2024 de 28 de Junho de 2024, [consultado a 31.01.2025]. Disponível na internet: https://www.tribunalconstitucional.pt/tc/acordaos/20240506.html.

[179] Cfr. PORTO, TRIBUNAL DA RELAÇÃO - Acórdão do Tribunal da Relação do Porto, processo número 7251/22.5T8PRT.P1 de 08-05-2023, [consultado a 31.01.2025]. Disponível na internet: https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/8c246bf5f321c363802589d4002ff5da?OpenDocument.

No que diz respeito ao armazenamento de dados biométricos, o Tribunal de Justiça da União Europeia, dispôs no processo C-205/21 de 26 de Janeiro de 2023 quando confrontado com a possibilidade de retenção de dados biométricos sublinhou a importância desta questão devidos aos riscos significativos que estão correlacionados ao tratamento de dados sensíveis em particular no âmbito de prevenção de crimes ou ameaças à segurança pública. É essencial que a recolha desses dados seja estritamente necessária devendo ser interpretado "no sentido de que define condições reforçadas de licitude do tratamento desses dados sensíveis" e proporcional à realização dos objetivos que se pretende prosseguir. No entanto, deve conter as garantias necessárias e estar previsto no direito nacional ou no direito da União Europeia, no entanto é essencial que as finalidades a atingir constituam uma ingerência menos gravosa possível nos direitos e liberdades do titular dos dados em causa[180]. Em Portugal, temos o art. 35º da CRP que protege o direito à proteção dos dados pessoais entendendo que esses dados devem ser tratados de forma leal; para fins específicos; com o consentimento do titular em causa ou com outro fundamento legitimo previsto na lei. Também o Regulamento Geral sobre a Proteção de dados clássica nos termos do art. 9º categorias especiais de dados pessoais que estão sujeitas a um elevado nível de proteção, o que significa que normalmente o tratamento desses dados não é permitido exceto situações especificas como defesa de direitos em processos penais ou obrigações legais.

Em suma, no âmbito do processo penal é juridicamente admissível restringir direitos fundamentais. A descoberta da verdade material que corresponde à reconstrução de factos passados e a realização dos fins do processo penal como a justiça e a prevenção dos crimes admitem essa restrição. Contudo, essa restrição não é arbitrária nem absoluta. O quadro constitucional impõe, como já mencionámos anteriormente, que qualquer limitação aos direitos fundamentais deve respeitar o princípio que dispõe que a restrição só é aceitável quando necessária, adequada e proporcional à salvaguardar outros direitos e interesses constitucionalmente protegidos (art. 18 número 2 da CRP), bem como o princípio da dignidade da pessoa humana. Não obstante, estes princípios orientadores têm de ser igualmente garantidas medidas legais

[180] ACÓRDÃO DO TRIBUNAL DE JUSTIÇA, no processo C-205/21, 26/01/2023, [consultado a 03.01.2025]. Disponível na internet: https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-01/cp230016pt.pdf

e eficazes contra possíveis abusos, assegurando que qualquer atuação que exceda esses limites comprometa a validade do processo ou dos atos nele praticados.

9. O USO DO RECONHECIMENTO FACIAL NA INVESTIGAÇÃO

A utilização do reconhecimento facial nas investigações policiais traz novas tecnologias e pode ser potencialmente aplicada a várias situações. Os aplicadores da lei utilizam este sistema para fins de identificação e autenticação; no primeiro caso, a atividade de identificação que também pode ser designada como "um para muitos" baseia-se na procura da identidade de uma pessoa; pelo contrário a atividade de autenticação também conhecida como "um para um" consiste em verificar a identidade de alguém em relação a um documento de identidade[181].

São vários os países que ao redor do mundo têm adotado e aplicado técnicas de reconhecimento facial, cada um com a sua própria regulamentação e finalidade.

Segue-se um conjunto de situações nos Países Baixos que permitem demonstrar a forma como a tecnologia de reconhecimento facial é utilizada nas investigações policiais. Como primeira situação temos o controlo de identidade fronteiriço – os agentes de fronteira utilizam os controlos de identidade para detetar e eventualmente deter fugitivos ou pessoas procuradas que sejam objeto de aviso vermelho válido pela INTERPOL e estejam registados na base de dados criminal da mesma. Os avisos vermelhos publicados pela INTERPOL a pedido dos países membros e as informações publicadas são igualmente armazenadas em base de dados e tornadas acessíveis a todos os países membros. Ao controlar a identidade das pessoas que atravessam a fronteira, os agentes de fronteira podem solicitar à INTERPOL que a imagem facial de uma pessoa controlada seja comparada com as imagens faciais de criminosos e pessoas desparecidas armazenadas no sistema de reconhecimento facial da INTERPOL (IFRS). A fotografia da pessoa é então convertida numa imagem de sonda, de seguida, os examinadores faciais da INTERPOL efetuam uma pesquisa no IFRS e é fornecida uma lista de potenciais imagens candidatas fornecidas pelo sistema.

[181] BERIDZE, Irakli; BUTTERFIELD, Kay Firth; BIK, Marjolein Smit-Arnold; GOUT, Cyril (2021) - *A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigation*s in World Economic Forum, pp. 7-9 [consultado a 20.10.2024]. Disponível na internet: https://unicri.it/sites/default/files/202110/A%20Policy%20Framework%20for%20Responsible%20Limits%20on%20Facial%20Recognition%20.pdf.

Posteriormente é analisada e comparada a imagem da sonda com as imagens candidatas. Se a conclusão for positiva, informam o Gabinete Central Nacional da INTERPOL e o Centro Nacional da INTERPOL e os agentes de fronteira. Outro exemplo onde o reconhecimento facial é utilizado pelos órgãos de investigação é a procura ativa de um terrorista num espaço público. Esta situação é um caso de utilização potencial, mas ainda não foi utilizada pela polícia neerlandesa. Após um ataque terrorista e quando o terrorista se encontra em fuga, as autoridades policiais podem apreender o circuito fechado para recolher uma imagem de sonda do terrorista. A imagem da sonda é comparada com outras imagens recolhidas a partir de imagens separadas de CCTV localizadas em sítios onde existe a probabilidade do fugitivo estar ou onde o fugitivo esteve temporariamente presente. Esta comparação pode conduzir a uma potencial correspondência e que se for positiva será enviada para as patrulhas da polícia que podem efetuar uma paragem e verificação com base nesse alerta[182].

Também nos Estados Unidos, a utilização por parte dos órgãos policiais do sistema de reconhecimento facial em investigações criminais tornou-se uma prática bastante comum, não obstante o número de detenções, acusações, acordos judiciais e condenações daí resultantes seja desconhecido, estima-se que seja na ordem das dezenas, se não centenas de milhares. Em 2016, pelo menos um quarto das 15.000 agências de aplicação da lei tanto estaduais como locais do país tinham acesso à tecnologia de reconhecimento facial e metade dos adultos americanos estava registado numa base de dados de reconhecimento facial destinada ao uso em investigações criminais. Em 2020, pelo menos 20 agências federais faziam uso deste sistema para fins de aplicação da lei, com intenção da expansão da sua utilização até 2023. Os departamentos da polícia entendem que o reconhecimento facial é uma tecnologia que lhes permite resolver os crimes de forma mais rápida; permite encontrar pessoas desparecidas e suspeitos e manter a comunidade mais segura[183].

No Canadá no início de 2020 surgiu uma controvérsia quando foi descoberto que as entidades policiais tinham aceitado uma “espécie” de um teste gratuito de tecnologia de reconhecimento facial de uma empresa americana *Clearview AI*. De facto, este

[182] Idem, pp. 10-13
[183] GARVIE, Clare (2022) - *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*, Center on Privacy & Technology at Georgetown Law, pp. 5-6, [consultado a 30.10..2024]. Disponível na Internet: https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

software recorre a uma grande base de dados com cerca de milhões de imagens que são retiradas da internet e de redes sociais para identificar pessoas, com ou sem o consentimento das mesmas. As questões que posteriormente foram levantadas evidenciaram que decisões sobre a aquisição e implementação dos sistemas de reconhecimento facial pelos serviços da polícia quer fosse a nível municipal, provincial e federal eram singulares, não regulamentados e secretos. A grande questão prendeu-se com os problemas e com os riscos, pelo facto de os órgãos policiais conseguirem aceder aos dados de reconhecimento facial nomeadamente em matéria de privacidade e discriminação (como por exemplo, a seleção de comunidades racializadas, a imprecisão, a parcialidade e o âmbito alargado das informações recolhidas para a base de dados de referência), sem que houvesse a devida supervisão, regulamentação para resolver e identificar as questões legais e éticas[184].

Mais recentemente, precisamente em Setembro de 2024, foi publicado pela Comissão dos Direitos Civis dos Estados Unidos o relatório "The Civil Rights Implications of the Federal Use of Recognition Technology", que pretendeu dar uma resposta à utilização crescente da tecnologia de reconhecimento facial pelo governo federal. Atualmente não existem leis ou regulamentos federais que expressamente autorizam ou limitem o uso desta tecnologia e, a partir de julho de 2024, não existe uma política oficial e padronizada publicada para o uso federal do reconhecimento facial. Esta comissão vem chamar à atenção para que qualquer agência que utilize estes sistemas deva ter uma política de utilização que esteja publicamente disponível, além de que devem garantir que essa utilização está em conformidade com a política governamental. Os vendedores de TRF que fornecem soluções ao governo federal devem proporcionar aos seus utilizadores uma formação contínua, apoio técnico e atualizações de *sofware* garantindo que os seus sistemas mantêm uma elevada precisão em todos os grupos demográficos e em contextos reais de utilização. Os beneficiários federais que utilizem estes sistemas de reconhecimento facial devem apresentar resultados verificados no que respeita à exatidão e ao desempenho em termos demográficos[185].

[184] HILL, Dallas; O´CONNOR, Christopher D; SLANE, Andrea (2022) - *Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making* in International Journal of Police Science & Management, Vol. 24(3) 325–335, pp 1 e 2, [consultado a 31.10.2024]. Disponível na Internet: https://journals.sagepub.com/doi/pdf/10.1177/14613557221089558 .
[185] United States Commission On Civil Rights (2024) - *The Civil Rights Implications of the Federal Use of Facial Recognition Tecnology*, pp. 4-5. [consultado a 30.10.2024]. Disponível na internet: https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

No entanto, e voltando ao cerne da questão que é a utilização do reconhecimento facial, também é evidenciado neste relatório que a aplicação desta tecnologia pelas forças policiais é um dos exemplos mais relevantes. Embora o reconhecimento facial tenha sido utilizada para ajudar nas investigações criminais, a verdade é que a sua utilização suscita e acarreta preocupações em matéria de privacidade e exatidão, nomeadamente, quando aplicados a minorias raciais, levando a casos de detenções injustas na sequência da utilização do reconhecimento facial.

É importante realçar que ao longo dos anos, algumas cidades e Estados aprovaram legislação que proibia ou restringia a utilização do reconhecimento pelos agentes de autoridade, mas que com o passar do tempo acabou por inverter o curso. Por exemplo, em 2020, em Nova Orleans foi aprovada uma portaria que proibia a polícia de fazer uso dos sistemas de reconhecimento facial, no entanto, em Julho de 2022 foi determinado que os agentes policiais poderiam através de solicitação de um superior utilizar o *sofware* para investigações de crimes violentos. O mesmo aconteceu no Estado de Virgínia que proibiu que a polícia local utilizasse o reconhecimento facial em 2021 e em 2022 promulgou uma lei permitindo a sua utilização em algumas situações. No mesmo seguimento Califórnia aprovou legislação, nomeadamente uma lei de três anos em 2020 que proibia que as forças policiais de fazerem uso do reconhecimento facial, entretanto a proibição já expirou e o estado tem desenvolvido vários projetos em diversas divisões destinados a regular a utilização do reconhecimento facial pelas forças policiais[186].

A China também é um grande exemplo de um país que desde cedo estabeleceu objetivos muito ambiciosos no desenvolvimento do reconhecimento facial. Para além de utilizar as técnicas de reconhecimento facial para perseguir criminosos o governo também designou o reconhecimento facial como uma tecnologia de "eleição" em muitos regulamentos que exigiram que os organismos públicos fizessem uso deste sistema para verificação de identidade. Estes sistemas de reconhecimento facial são fortemente encorajados e, em muitos casos, obrigatórios para facilitar a verificação da identidade em muitas questões como o reconhecimento notarial; obtenção de cartas de condução

[186] GARZA, Rochelle M.; NOURSE, Victoria F.; ADAMS. J. Christian; GILCHRIST, Stephen; HERIOT, Gail L.; JONES, Mondaire; KIRSANOW, Peter N.; MAGPANTAY, Glenn D., MORALES, Mauro (2024) - *The Civil Rights Implications of the Federal Use of Facial Recognition Technology* in United States Commission on Civil Rights, Statutory Enforcement Report, Washington DC, p. 29, [consultado a 2.11.2024]. Disponível na Internet: https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf .

ou a conceção de benefícios sociais aos residentes. O rápido desenvolvimento e a ampla adoção do reconhecimento facial tornaram a China num líder mundial neste domínio.[187]

No entanto, e tal como aconteceu noutros países, a utilização destes sistemas suscitou sérias preocupações em matéria de privacidade. Embora muitos comentadores indiquem que a cultura chinesa é mais tolerante em relação às violações da privacidade do que nos países ocidentais e embora a cultura chinesa seja a favor do reconhecimento facial devido a uma maior segurança ou conveniência tem existido vários debates alargados sobre a justificação e o âmbito adequado da adoção do reconhecimento facial no país. A China tem estado a trabalhar no desenvolvimento de um quadro regulamentar para estes sistemas desde 2020, embora tenha subjacente melhorar substancialmente a proteção dos dados pessoais, tem havido riscos e desafios crescentes para proteger os dados dos cidadãos, e embora as leis e regulamentos atuais tenham restringido a aplicação do reconhecimento facial em algumas circunstâncias, estas restrições podem funcionar mal quando a tecnologia é instalada pelo governo ou quando é implantada com o objetivo de proteger a segurança pública[188].

10. A MATERIALIZAÇÃO DO RISCO DE ERRO EM SITUAÇÕES DE RECONHECIMENTO FACIAL

Apesar das precauções que nos últimos anos têm sido tomadas no uso das tecnologias de reconhecimento facial, têm existido situações em que por via da utilização destas tecnologias têm existido condenações de pessoas inocentes.

Um caso documentado de prisão injusta devido ao uso de tecnologias de reconhecimento facial foi o de Robert Williams. Em janeiro de 2020, foi preso ao pé da sua casa sem que lhe fosse explicado qual o motivo da sua detenção. Ele foi acusado de roubar milhares de dólares em relógios Shinola, porque foi utilizado o sistema de

[187] LEE, Jyh-Na; ZHOU, Peng (2024) - *FRT Regulation in China* in Cambridge University Press, pp. 242, [consultado a 4.11.2024]. Disponível na internet: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D0FA408D7A063C4E97E52558D90D03D0/9781009321198c18_242-252.pdf/frt-regulation-in-china.pdf.

[188] LEE, Jyh-Na; ZHOU, Peng (2024) - *FRT Regulation in China* in Cambridge University Press, p. 243, [consultado a 4.11.2024]. Disponivel na internet: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D0FA408D7A063C4E97E52558D90D03D0/9781009321198c18_242-252.pdf/frt-regulation-in-china.pdf

reconhecimento facial que comparou a fotografia do assaltante com a fotografia vencida da carta de condução associando que fossem a mesma pessoa. Robert Williams ficou detido pelo período de 30 horas[189].

Um outro caso decorreu no ano de 2021 quando em Chicago um homem chamado Michael Williams foi preso por um assassinato em primeiro grau. Essa detenção teve com base um alerta do *shotspotter*[190] que foi recebido pela polícia. Com base num alerta de um vídeo de segurança silencioso que demonstrava um vídeo de um carro num cruzamento ele acabou preso pelo período compreendido de 1 ano sem que a polícia e os procuradores explicassem a razão do mesmo no envolvimento do crime; sem que existisse qualquer testemunha do homicídio e nem terem sido encontradas nenhumas evidências físicas que o pudessem ligar ao crime. Além disso, o uso de sistemas como a *shotspotte* que pretende triangular a localização de um disparo através de um algoritmo de inteligência artificial e de uma rede de microfones, numa investigação realizada pela *Associated Press*, demonstrou frequentemente que era possível que estes sistemas não registassem tiros ao vivo ou confundissem outros sons com tiros, comprovando a não confiabilidade estatística destes meios. O que sucedeu é que o Sr. Williams passou quase um ano na prisão antes do caso ser arquivado[191].

Outra situação de má identificação ocorreu com Porcha Woodruff, uma esteticista e estudante de enfermagem que ficou em choque quando a polícia lhe informou que estaria presa por um crime de sequestro de carro que não cometeu. O que permitiu à polícia chegar à sua identificação foi o uso de tecnologias de reconhecimento facial de forma a executar uma imagem de um suspeito através de um banco de dados, sendo que a foto da Sra. Woodruff se encontrava entre as devolvidas. Após a sua deteção sucedeu um interrogatório de 11 horas no centro de detenção de Detroit. Um mês depois do sucedido o promotor rejeitou o caso com base em insuficiências evidentes[192].

---

[189] STANFORD, Alyxaundria (2024) - *Artificial Intelligence Is Putting Innocent Peaple at Risk of Being Incarcerated* in innocence Project. [consultado a 14.11.2024]. Disponível na internet: https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/

[190] Podem ser definidos como sistemas de deteção, localização e análise forense de disparos de armas.

[191] SWARNS, Christina (2023) - *When Artificial Intelligence Gets It Wrong* in innocence Project, [consultado a 25.11.2024]. Disponível na internet: https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/

[192] SWARNS, Christina (2023) - *When Artificial Intelligence Gets It Wrong* in innocence Project. [consultado a 25.11.2024]. Disponível na internet: https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/

Estes casos têm demonstrado situações mais preocupantes quando se trata de situações que envolvam pessoas negras ou asiáticas. Um estudo do *National Institute of Standards and Technology*[193] demonstrou que existia a probabilidade de 10 a 100 vezes mais de serem identificadas de forma errada do que em relação a pessoas brancas. Para além disso, outros estudos refutaram esta ideia descobrindo que os algoritmos tinham dificuldade em situações em que era necessário distinguir entre estruturas faciais e tons de pele mais escuros[194]

A questão que se coloca é até que ponto é que estas tecnologias de reconhecimento facial não se sobrepõem à vida e à liberdade de pessoas que são erroneamente identificadas. Não obstante os avanços que têm sido alcançados através de testes e melhoramento de algoritmos e riscos de precisão, estas situações continuam a ocorrer, sendo necessário tentar encontrar um equilíbrio no uso destas tecnologias.

11. REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL PELA UNIÃO EUROPEIA

Foram vários os esforços que têm vindo a ser feitos de forma a regulamentar os avanços na inteligência artificial e a utilização crescente da mesma no nosso quotidiano. Associada a essa utilização começam a surgir questões relacionadas com a segurança, a privacidade, a ética e o respeito pelos direitos fundamentais.

Em 2021, foi apresentado e aprovado pela Comissão Europeia a lei de Inteligência Artificial da União Europeia (doravante, AI Act) que teve como objetivo pertinente a utilização no espaço da União Europeia da inteligência artificial de uma forma segura, transparente e responsável, tratando inclusive de sistemas que podem ser de baixo risco como de alto risco ou mesmo de risco inaceitável, impondo exigências dependendo do sistema em especifico de forma a proteger a segurança e os direitos fundamentais dos cidadãos[195].

---

[193] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee (2019) - *Face Recognition Vendor Test (FRVT) Part 3: Demographic* Effects in National Institute of Standards and Technology, [consultado a 25.11.2024]. Disponível na internet: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[194] Idem

[195] BARROS, Gabriel Osório de (2024) - *Regulamentação da Inteligência Artificial na União Europeia: Uma análise do AI Act* in Gabinete de Estratégia e Estudos do Ministério da Economia, pp.4-5. [consultado a 29.11.2024]. Disponível na internet: https://www.gee.gov.pt/pt/?option=com_fileman&view=file&routed=1&name=GEE_Em%20An%C3%A1lise

Para além da lei de inteligência artificial, a União Europeia demonstrou apoio a orientações éticas elaboradas por um grupo de peritos de alto nível, que dispõe que inteligência artificial de confiança deve basear-se em três componentes fundamentais:

1) Deve ser garantida a legalidade, de forma a permitir o respeito da legislação aplicável;
2) Deve ser garantido respeito por valores e princípios éticos;
3) Deve ser sólida tanto na dimensão técnica como social, na medida em que os sistemas de inteligência artificial podem, ainda que de forma não intencional, causar danos.

Tendo subjacente os três valores enunciados, o grupo de peritos desenvolveu os sete requisitos que têm de ser respeitados pelas aplicações de inteligência artificial para que possam ter um valor de confiança:

I. Têm de fazer parte integrante dos sistemas de inteligência artificial a supervisão e o controlo humano para que sejam respeitados os valores e os direitos fundamentais;
II. Tem de existir segurança e robustez, de forma a garantir uma segurança do sistema a ataques e por outro lado a fiabilidade dos mesmos;
III. É importante garantir a privacidade dos dados e a sua subsequente governação, de forma a garantir a integridade dos dados e o acesso aos mesmos;
IV. É essencial a componente de transparência nos sistemas de inteligência artificial, garantindo a rastreabilidade, o registo de todas as decisões que são tomadas por estes sistemas, a explicabilidade e a comunicação. É importante que estejam claras e presente as capacidades e as limitações do sistema;
V. Os sistemas de inteligência artificial devem eliminar sistemas de má conduta, de forma a evitar situações de preconceito e de discriminação; devem garantir um acesso e uma acessibilidade a todos, permitindo igualmente a participação das partes interessadas – equidade;
VI. Bem-estar social e ambiental, incluindo o respeito pelo meio ambiente; um impacto que estes sistemas podem ter na sociedade; a democracia;

Regulamento%20da%20Inteliq%C3%AAncia%20Artificial.pdf&folder=estudos-e-seminarios%2Fartigos&container=fileman-files .

VII. Por fim temos, a responsabilização, este último requisito pressupõe que existam meios de responsabilidade pelos sistemas de inteligência artificial e pelos seus resultados[196].

O regulamento da inteligência artificial (Regulamento (EU) 2024/1689) estabelece o primeiro quadro jurídico em matéria de Inteligência artificial (IA) a nível mundial.

As disposições jurídicas que foram tomadas em relação à IA de forma simplistas podem ser enunciadas como:

I. Promover uma resposta, tendo em conta os riscos que os sistemas de inteligência artificial podem criar;
II. Proibir utilizações de IA que demonstrem riscos inaceitáveis;
III. Estabelecer listas de pedidos que demonstrem alto risco;
IV. Determinar regras claras para as aplicações de IA que sejam identificados como alto risco;
V. Determinar exigências, em específico de risco elevado para responsáveis de implantação de aplicação de IA, como os fornecedores;
VI. Impor avaliações antes de qualquer aplicação de IA ser colocado no mercado ou em serviço;
VII. Após a colocação de aplicações de IA, a possibilidade de aplicação de medidas coercivas;
VIII. Instituir uma direção de governação no âmbito europeu e nacional.

11.1. ABORDAGEM BASEADA NO RISCO

A lei de inteligência artificial procura promover uma proteção quer seja a nível da saúde, da segurança, como no exercício dos direitos fundamentais; na democracia e no Estado de direito. É importante realçar que todos os sistemas e aplicações de IA que fomentem comportamentos perigosos, que possam ser uma ameaça à segurança e aos direitos e liberdades fundamentais são proibidos.

[196]Comissão Europeia, Direção-Geral de Redes de Comunicações, Conteúdos e Tecnologia. (2019). - *Orientações éticas para uma IA de confiança*, Escritório de Publicações, pp.17-25 [consultado a 29.11.2024]. Disponível na internet: **https://data.europa.eu/doi/10.2759/2686** .

A abordagem baseada no risco pode distinguir-se entre risco elevado; risco limitado e risco mínimo ou nulo, tendo diferentes requisitos e obrigações consoante a categoria.

Os sistemas são considerados de alto risco porque constituem um maior risco, sendo que esta classificação tem em conta o perigo de dano como a probabilidade de ocorrência. A tecnologia de IA que é tida como de risco elevado inclui infraestruturas críticas em que haja um risco para a vida e saúde das pessoas; situações como o acesso ao ensino ou formação profissional; a aplicação da lei que possa colocar em causa direitos fundamentais (por exemplo, no âmbito do processo penal a averiguação da fiabilidade das provas); a aplicação da justiça (por exemplo, recorrer a sistemas de inteligência artificial para procurar decisões judiciais); questões relacionadas com o controlo fronteiriço, asilo e migração (recorrer a mecanismos de IA para analisar os vistos); acesso ao emprego (por exemplo, para processos de recrutamento fazer uso de aplicações de IA para análise do CV) e serviços públicos e privados essenciais.

Como são considerados sistemas de alto risco, o *AI ACT* de forma a proteger eventuais riscos pré-definiu algumas obrigações como elevados níveis de robusteza, segurança e exatidão; regras de supervisão humana de forma a controlar a atuação destes sistemas e reduzir os eventuais riscos; o responsável pela aplicação deve conceder informações claras e adequadas; qualidade nos dados que são introduzidos nos sistemas de forma a não serem produzidos resultados discriminatórios e minimização dos riscos; possibilidade de rastreabilidade dos resultados; informação suficiente que permita explicar todos os aspetos sobre o sistema e a sua finalidade para que possam ser avaliadas pelas autoridades e sistemas que sejam adequados a avaliação e redução dos riscos.

As situações de risco limitado estão ligadas a riscos em razão da falta de transparência na utilização de sistemas de inteligência artificial. Por exemplo, quando são utilizados robôs de conversação. Nesse caso, é exigido que as pessoas sejam informadas de que estão a relacionar-se com uma máquina de forma a terem uma perceção e de comunicarem o interesse ou não. O mesmo acontece, por exemplo, quando através da IA são criados textos com o fim de informar sobre assuntos de interesse público, aí também deve existir a informação de que foi gerado artificialmente.

O *AI ACT* estabelece regras de transparência de forma a verificar que as pessoas sejam sempre informadas fomentando, assim, a confiança.

Depois ainda temos situações de risco mínimo ou nulo sendo a maioria dos sistemas atualmente utilizados na União Europeia. Esta categoria compreende exemplos como jogos de vídeo com IA e filtros de spam.

11.2. PROIBIÇÕES E RESTRIÇÕES

A lei da inteligência artificial visa promover uma utilização segura dos sistemas de inteligência artificial e previu algumas proibições, de forma a projetar os direitos e a segurança dos cidadãos:

I. A utilização de sistemas de inteligência artificial onde sejam utilizadas técnicas sublimares e manipulativas que possam influenciar a consciência e o comportamento da pessoa, prejudicando a sua capacidade de tomar uma decisão informada;
II. É proibida a utilização de sistemas que explorem a vulnerabilidades de grupos de pessoas específicos como crianças ou pessoas que sofram de deficiências de forma a causar às mesmas danos materiais ou psicológicos;
III. São proibidos sistemas de avaliação ou de classificação por autoridades públicas ou privadas que resultem num tratamento injusto e discriminação de pessoas singulares ou grupos de pessoas, devido ao seu comportamento social; às suas caraterísticas de personalidade ou pessoais;
IV. É proibido usar a inteligência artificial para avaliar qual o risco de uma pessoa futuramente praticar crimes, tendo por base características da personalidade;
V. Proíbe-se igualmente sistemas de inteligência artificial que criam ou expandam bases de dados de reconhecimento facial tendo subjacente a recolha aleatória de imagens faciais;
VI. Não é permitido o uso de sistemas de inteligência artificial que infiram emoções de pessoas no âmbito do trabalho e instituições educativas, com exceção de quando for indicado para fins médicos ou de segurança;
VII. É proibido o uso de sistemas para fins de categorização biométrica que classifiquem as pessoas para deduzir a sua raça; opiniões políticas; filiação sindical; convicções religiosas e filosóficas; vida sexual ou orientação sexual;

VIII. Não é permitido o uso de sistemas de identificação biométrica em tempo real em espaços acessíveis ao público para efeitos de aplicação da lei, com exceção de casos específicos[197].

12. ADMISSIBILIDADE DO RECONHECIMENTO FACIAL NO PROCESSO PENAL

Quando falamos em finalidades do processo penal falamos da realização da justiça e a procura da verdade material. Segundo o autor Germano Marques da Silva a verdade significa que "o tribunal obteve a *certeza jurídica* de que os factos alegados ocorreram e só após a aquisição dessa certeza adquire o poder de aplicar a sanção que a lei comina para o agente dos factos provados e que foram objeto da acusação"[198], ou seja, a verdade material é a reconstrução de um facto passado.

Não obstante este fim da descoberta da verdade não é absoluto, o que significa que só pode ser prosseguido de forma válida[199] o que implica, designadamente, que o seja com respeito dos direitos fundamentais das pessoas envolvidas[200]. Este respeito envolve várias garantias como a proibição de certos meios de prova[201], não podendo ser consideradas provas que tenham sido obtidas através de tortura, de coação, ofendendo integridade física ou moral[202] [203].

---

[197] Cfr. REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO de 13 de junho de 2024, artigo 5º número 1, alíneas de a) – h)

[198] SILVA, Germano Marques Da (2017) - *Direito Processual Penal Português, Noções e Princípios Gerais; Sujeitos Processuais; Responsabilidade Civil conexa com a Criminal; Objeto do processo* vol.1, 2º edição, UCP Editora, p. 25

[199] O mesmo entendimento é referido pelo Juiz de Direito João de Matos-Cruz Praia (2019) em *Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e reconstituição do facto* in julgar online que dispõe: " A finalidade do processo penal não é a descoberta da verdade a qualquer custo, mas a sua prossecução através dos meios processualmente admissíveis à luz do princípio da dignidade da pessoa humana (art. 1.º da Constituição da República Portuguesa/CRP), ainda que isso possa conduzir, e muitas vezes por certo conduz, à impossibilidade de acesso à intitulada verdade "material" ou histórica", p.4 [consultado a 09.12.2024]. Disponível na internet: https://julgar.pt/wp-content/uploads/2019/12/20191209-ARTIGO-JULGAR-Proibi%C3%A7%C3%B5es-de-prova-em-processo-penal-Jo%C3%A3o-Praia.pdf.

[200] Temos como exemplo o acórdão do Supremo Tribunal de Justiça de 03-03-2010 com o processo 886/07.8PSLSB.L1.S1, que refere: " Os princípios constitucionais da busca da verdade material e da realização da justiça, mesmo em matéria de funcionalidade da justiça, penas e da tutela de valores, têm limites, impostos pela dignidade e pelos direitos fundamentais das pessoas, que se traduzem processualmente nas proibições de prova". [consultado a 06.12.2024]. Disponível em: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument.

[202] Cfr. Art. 32º número 8 da CRP e artigo 126º número 1 do CPP

[203] SILVA, Germano Marques Da (2017) - *Direito Processual Penal Português, Noções e Princípios Gerais; Sujeitos Processuais; Responsabilidade Civil conexa com a Criminal; Objeto do processo*, p.25

É normal que com o avanço da tecnologia, em particular ao nível da inteligência artificial, surjam novos mecanismos, seja a nível de formas de investigação, novos mecanismos de identificação, como é o caso do reconhecimento facial e que exista a intenção de os tentar transpor para o ordenamento jurídico de forma a melhorar a eficácia, o tempo e o próprio sistema. No entanto, é necessário perceber até que ponto é que essas "inovações" podem ser validamente aplicadas no nosso processo penal.

A forma de analisar a possibilidade de aplicação no nosso ordenamento jurídico será começar por um princípio fundamental previsto no art. 126º do CPP, que dispõe sobre a legalidade da prova e que vem dispor o seguinte: "são admissíveis as provas que não forem proibidas por lei".

Segundo Sandra Oliveira e Silva:

> "proibir a utilização de certos meios probatórios, quis o legislador também delimitar (negativamente) o elenco das provas *admitidas* em processo penal – a fórmula «são admissíveis as provas que não forem proibidas» tem aqui o sentido de que não são admitidos apenas os meios probatórios tipificados, mas todos os meios de prova que não forem proibidos mesmo sendo atípicos"[204].

Por sua vez, de acordo com Pedro Soares de Albergaria, por métodos podemos entender como:

> "os caminhos a percorrer para se atingir determinado fim – e, por decorrência a proibição tem o sentido de delimitar negativamente os *modus* de aquisição de certo conhecimento no processo. São, neste sentido, verdadeiros limites à descoberta da verdade material ou, talvez melhor, o respeito pela proibição é critério da verdade validamente adquirida no processo"[205].

[204] SILVA, Sandra Oliveira e (2011) - *Legalidade da Prova e Provas Proibidas* in Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, pp. 545 – 591. [consultado a 09.12.2024]. Disponível na internet: https://repositorio-aberto.up.pt/bitstream/10216/133333/2/49978.pdf

[205] ALBERGARIA, Pedro Soares de (2024) - *Comentário Judiciário Do Código De Processo Penal*, *Tomo II, Artigos 124 a 190º*. 4ª edição. Edições Almedina, p.52

De facto, o regime geral é o da admissibilidade de todas as provas que não forem proibidas por lei, não existindo uma regra de taxatividade de meios de prova nem de meios de obtenção de prova [206].

Segundo Fernando Gama Lobo:

> "mas como não há liberdades absolutas, haverá sempre que aferir da legalidade de uma prova, ou se se preferir, da sua não ilegalidade processual. E esse juízo alcança-se, não só pelas vias ordinárias (v.g. art.126º) mas também da Constituição, quando estabelece o regime dos direitos, liberdades e garantias dos cidadãos (v.g. arts. 24º a 47º da CRP)".[207]

A inexistência de previsão legal especifica para determinadas modalidades probatórias é complementada por critérios substantivos gerais decorrentes do art. 340º do CPP, permitindo que o juiz aceite outros meios de prova que não estejam expressamente previstos, desde que sejam idóneos, pertinentes e necessários à formação da convicção judicial. Embora inexista um critério formal previamente estabelecido na lei, a sua validade está sujeita a regras fundamentais que regem a atividade probatória, como o principio da legalidade, o princípio do contraditório, o respeito pelos direitos fundamentais ou a necessidade e utilidade da prova para a descoberta da verdade material. Não obstante, quando a utilização de um meio de prova imponha uma maior intrusão nos direitos de um suspeito a mesma deve ser prevista por lei expressa[208] (nos termos do art. 26º números 1 e 2 da CRP).

A não taxatividade teve subjacente a incapacidade do legislador em conseguir antever os próprios progressos tecnológicos, deixando em aberto a possibilidade de serem tipificados outros meios de prova, o que significa que o legislador pode tanto recorrer a meios probatórios que tenham sido tipificados na lei ou escolher outro, desde que não seja proibido por lei. A afirmação de que serão admissíveis provas que não sejam proibidas por lei deve ser interpretada sempre tendo em conta a estrutura do

[206] LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado*, p.234
[207] Idem, p.234
[208] ALBUQUERQUE, Paulo Pinto de (2023) - *Comentário do Código de Processo penal à luz da Convenção Europeia dos Direitos Humanos*, p.486

nosso processo penal, o que significa, designadamente, que deve ser sempre balanceada com os direitos do arguido [209].

A ideia que está subjacente às hipóteses previstas no preceito legal do art. 126º do CPP é a violação dos direitos e liberdades fundamentais, sendo essa garantia mais acentuada em direitos que têm uma maior conexão com o princípio fundamental da dignidade da pessoa humana (art. 1º da CRP), como são os casos da integridade física e moral, da intimidade da vida privada, da proibição de violação do domicilio e da correspondência e das telecomunicações, assim como o direito à imagem e à palavra[210].

A liberdade de escolher outros meios probatórios não significa a aceitação de qualquer um, pelo contrário, como se trata de meios que não se encontram tipificados, devem, ao invés, sujeitar-se a parâmetros de validade mais rigorosos[211].

A admissibilidade de fazer uso de meios de prova atípicos pressupõe não apenas a inexistência de uma proibição legal, mas também que não haja um meio probatório que se encontre tipificado e que seja capaz de alcançar o mesmo resultado. Se existir um meio de obtenção de prova típico que seja adequada ao caso em particular, então esse meio de prova deve ser seguido rejeitando a aplicação da prova atípica [212]. A ideia é a de que, sempre que exista um meio de obtenção de prova que se encontre tipificado na lei e que seja adequado ao caso concreto, a utilização deste deve ser preferido, sendo dessa forma rejeitada a utilização desse meio atípico. Não obstante, isso não significa que os meios atípicos sejam totalmente excluídos, eles têm é de respeitar os vários requisitos, desde logo não podem ser proibidos por lei, devem ser necessários à descoberta da verdade material e à demonstração de que essa prova não pode ser suprida através de um meio que já se encontra tipificado na lei. Por outro lado, deve ser proporcional ao fim que se pretende atingir (tem subjacente a ideia do sacrifício dos direitos fundamentais e a ideia de não puder ser obtido de forma excessiva ou abusiva) e, deve respeitar as garantias de defesa. O que se pretende é assegurar que não seja

[209] SILVA, Sandra Oliveira e (2011) - *Legalidade da Prova e Provas Proibidas* in Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, pp. 545 – 591, [consultado a 09.12.2024]. Disponível na internet: https://repositorio-aberto.up.pt/bitstream/10216/133333/2/49978.pdf
[210] ALBERGARIA, Pedro Soares de (2024) - *Comentário Judiciário Do Código De Processo Penal*, *Tomo II, Artigos 124 a 190º*, p.53
[211] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial,* p. 108
[212] SILVA, Sandra Oliveira e (2011) - *Legalidade da Prova e Provas Proibidas* in Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, pp. 545 – 591, [consultado a 09.12.2024]. Disponível na internet: https://repositorio-aberto.up.pt/bitstream/10216/133333/2/49978.pdf

possível recorrer a esses meios de prova quando os mesmos tenham como fim contornar o sistema de direito probatório.

Ora, ainda que o reconhecimento facial e a prova por reconhecimento tipificada na nossa lei tenham em princípio o mesmo fim último – a identificação de uma pessoa, os seus fins instrumentais divergem. A utilização do reconhecimento facial opera como uma forma de investigação automatizada, fazendo uso de algoritmos e bases de dados, enquanto a prova por reconhecimento traduz-se numa forma de produção de prova onde alguém, através da recuperação da memória, descreve uma pessoa que esteve envolvida num ilícito criminal[213]. Embora ambos se destinem à identificação os contextos em que se inserem, são diferentes, tal como as implicações jurídicas, nomeadamente ao nível das garantias de defesa, controlo judicial e fiabilidade.

A ideia central é que reconhecimento facial e, tendo por base a ideia de que estamos sempre na presença de um meio de produção de prova atípico a constituir, não seria considerado um desvio ou numa violação da prova por reconhecimento tipificada no nosso ordenamento jurídico. Não obstante, para a sua admissão e valoração estariam subjacentes as limitações previstas no art. 126º do CPP, em particular a demonstração da necessidade e idoneidade no apuramento dos factos, sendo esse juízo confiado ao julgador

Se pensarmos na aplicação desta regra em relação aos sistemas de reconhecimento facial talvez seja difícil de cumprir, uma vez que estes sistemas continuam a suscitar vários problemas no modo como funcionam, na sua fiabilidade e nos seus resultados[214].

No mesmo seguimento e nos termos dos princípios que norteiam o nosso processo penal, nomeadamente o princípio do contraditório, para a admissibilidade de qualquer meio de prova, sobretudo tratando-se de uma prova atípica ou não expressamente prevista na lei, exige-se que seja plenamente assegurado o direito ao contraditório. Este entendimento é mais relevante no caso de provas atípicas quando, por exemplo, resultem da utilização de novas tecnologias cuja natureza e fiabilidade podem acarretar mais dúvidas suscitando assim um maior escrutínio.

[213] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial*, p.109
[214] Idem, p.110

O princípio do contraditório tem previsão legal no art. 355º número 1 do CPP e no art. 32 número 5 da CRP, e consiste no direito que assiste às partes processuais de participar ativamente na formação da prova, na discussão dos factos, nos argumentos jurídicos e reagir a todos os atos e provas que possam influenciar a decisão judicial. Em termos práticos, ninguém pode ser condenado ou prejudicado por uma decisão judicial sem que sobre ela tenha tido a possibilidade de se pronunciar sobre os elementos da decisão em que se baseia[215]. A finalidade do princípio do contraditório é a de garantir a paridade de armas entre a acusação e a defesa e assegurar a transparência e legitimidade da decisão judicial sendo que a decisão só será justa se tiver subjacente a ela a participação das partes na formação da prova e na discussão jurídica dos factos. Relativamente à natureza das provas e ao princípio do contraditório o autor Fernando Gama Lobo dispõe:

> "A norma estabelece o princípio geral de que todas as provas que serviram à convicção do tribunal, têm de ser produzidas (criadas, geradas, originadas...) ou examinadas (analisadas, revistas, inspecionadas) em audiência. As provas produzidas em audiência são aquelas que resultaram da discussão do *thema probandum*. As examinadas, são aquelas que pertencem à prova pré-constituída"[216].

[215] O mesmo entendimento é referido pelo SUPREMO TRIBUNAL DE JUSTIÇA - Acórdão do Supremo Tribunal de Justiça de 07-11-2007, processo 07P3630 que dispõe: "O princípio do contraditório – com assento constitucional no art. 32.º, n.º 5, da CRP – impõe que seja dada oportunidade a todo o participante processual de ser ouvido e de expressar as suas razões antes de ser tomada qualquer decisão que o afete, designadamente que seja dada ao acusado a efetiva possibilidade de contrariar e contestar as posições da acusação".
V – "A construção da verdadeira autonomia substancial do princípio do contraditório leva a que seja concebido e integrado como princípio ou direito de audiência, dando «oportunidade a todo o participante processual de influir através da sua audição pelo tribunal no decurso do processo»".
VI – "A densificação do princípio deve, igualmente, relevante contributo à jurisprudência do TEDH, que tem considerado o contraditório um elemento integrante do princípio do processo equitativo, inscrito como direito fundamental no art. 6.º, § 1.º da CEDH".
VII – "Na construção convencional, o contraditório, colocado como integrante e central nos direitos do acusado (apreciação contraditória de uma acusação dirigida contra um indivíduo), tem sido interpretado como exigência de equidade, no sentido em que ao acusado deve ser proporcionada a possibilidade de expor a sua posição e de apresentar e produzir as provas em condições que lhe não coloquem dificuldades ou desvantagens em relação à acusação".
XI – "O princípio do contraditório tem, assim, uma vocação instrumental da realização do direito de defesa e do princípio da igualdade de armas: numa perspetiva processual, significa que não pode ser tomada qualquer decisão que afete o arguido sem que lhe seja dada a oportunidade para se pronunciar." [consultado a 10.12.2024]. Disponível na internet: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/134027f113c83ddb802573a000501952?OpenDocument.
[216] LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado, anotação do artigo 355º*, p.781

Na utilização de sistemas de reconhecimento facial, a exigência de que todas as provas que fundamentam a convicção do legislador sejam produzidas e examinadas em audiência para a confrontação e debate dos elementos probatórios, configura um grande desafio, visto que o arguido não tem possibilidade de controlar a fiabilidade das provas contra si apresentadas.

Como sabemos, no reconhecimento facial, no momento em que são comparadas as imagens, não existe conhecimento por parte do identificado, é feito de forma oculta. O mesmo não se pode dizer quando falamos na utilização da prova por reconhecimento usada no nosso processo penal, pela razão de que, apesar desta prova depender da recordação/memória da testemunha ocular, existe todo um formalismo, toda uma exigência de forma a reduzir a probabilidade de erro, além de que o suspeito se encontra presente, podendo controlar o decorrer da diligência[217]. A forma de permitir que este princípio fosse assegurado era o legislador tipificar medidas que assegurassem os resultados destes sistemas, por exemplo através de testes de confiabilidade, permitindo testar os resultados através de avaliações rigorosas que indicassem os índices de acerto e as suas taxas de erro, realizações de auditorias através de peritos ou instituições especializadas de forma a verificar a segurança dos dados e a ausência de viesses que pudessem comprometer a identificação ou a sua verificação através da corroboração por outros meios e elementos de prova como perícias técnicas, depoimentos e imagens de segurança.

Quando falamos dos métodos proibidos de prova, é possível autonomizar dois núcleos diferentes[218] de provas proibidas, dependendo da natureza dos direitos fundamentais que estão em causa[219]. O autor Manuel da Costa Andrade sobre os métodos proibidos de prova entende:

> "A coberto dos métodos proibidos de prova prescreve a lei processual os atentados mais drásticos à dignidade humana, mais capazes de comprometer a identidade e a representação do

[217] SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência artificial,* p. 110

[218] O mesmo entendimento é referido no SUPREMO TRIBUNAL DE JUSTIÇA - Acórdão do Supremo Tribunal de Justiça de 20-09-2006, processo 06P2321 que dispõe o que seguinte: "XXIV - Nos termos do art. 126.º do CPP, os métodos proibidos de prova são de duas categorias, consoante a disponibilidade ou indisponibilidade dos bens jurídicos violados: os absolutamente proibidos, pelo uso de tortura, coação ou em geral ofensas à integridade física ou moral - n.ºs 1 e 2 -, que não podem em caso algum ser utilizados, mesmo com o consentimento dos ofendidos, e os relativamente proibidos - n.º 3 -, que respeitam ao uso de meios de prova com intromissão na correspondência, na vida privada, domicílio ou telecomunicações, sem consentimento do respetivo titular". [consultado a 11.12.2024]. Disponível na internet: https://diariodarepublica.pt/dr/detalhe/acordao/06p2321-2006-89075175.

> processo penal como processo de um Estado de Direito e, por vias disso, abalar os fundamentos daquela *Rechtskultur* sobre que assenta a moderna consciência democrática"[220]

A primeira parte da norma dispõe que são métodos inadmissíveis em processo penal as provas que forem obtidas mediante tortura, coação, ofensa à integridade física e moral e outras formas graves de ilicitude, consagrando desta forma o princípio da proibição de meios obtidos por métodos absolutamente proibidos. A utilização destes métodos atenta contra a violação de direitos indisponíveis, consubstanciando-se numa violação intolerável e insanável na ordem jurídica[221]. Nestas situações, não existe a possibilidade de exceção ou justificação legal para a sua utilização, visto que afetam direitos fundamentais indisponíveis como a vida, a integridade física ou moral e a dignidade da pessoa humana[222], que se traduze em direitos inalienáveis e intransigíveis, estando protegidos constitucionalmente de forma absoluta, pelo que qualquer prova obtida através dos mesmos é nula, não permitindo qualquer ponderação nem justificação jurídico-penal, afetando a validade global do processo e a prova.

A segunda parte refere-se às provas que foram obtidas através da intromissão da vida privada, domicílio, correspondência ou telecomunicações, sendo que o que as distingue da primeira é o facto de a proibição só existir quando a intromissão se revelar "abusiva"[223], quando efetuada fora dos casos previstos na lei ou sem que haja intervenção judicial[224], ou ainda quando desnecessária, desproporcional ou destrutiva dos direitos[225]. Essas provas só podem ser utilizadas nos termos expressamente previstos na lei ou se houver consentimento do lesado na medida em que estamos

---

[220] ANDRADE, Manuel Da Costa (2022) - *Sobre As Proibições De Prova Em Processo Penal*, 2ª edição, Gestlegal, p.217

[221] LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado, anotação do artigo 126º*, p. 238

[222] No mesmo sentido SUPREMO TRIBUNAL DE JUSTIÇA – Acórdão do Supremo Tribunal de Justiça, de 20-09-2006, processo 06P2321 dispõe da mesma opinião: XXVI – "Os métodos absolutamente proibidos de prova, por se referirem a bens absolutamente indisponíveis, determinam que a prova seja fulminada de nulidade insanável, a qual está consagrada na expressão imperativa "não podendo ser utilizadas", usada no art. 126.º, n.º 1, do CPP". XXVII – "Com efeito, há casos de atentados extremos à pessoa humana em que os direitos fundamentais comportam uma dimensão tal que, em vista da proteção do cidadão ante o Estado e como forma de assegurar a sua subsistência e a convivência em segurança e polidireccionada dos cidadãos, com respeito pela dignidade respetiva e o justo equilíbrio entre a contribuição de todos e cada um para o bem comum, os meios de prova obtidos com violação daqueles é intolerável". [consultado a 11.12.2024]. Disponível na internet: https://diariodarepublica.pt/dr/detalhe/acordao/06p2321-2006-89075175.

[223] SILVA, Sandra Oliveira e (2011) - *Legalidade da Prova e Provas Proibidas* in Revista Portuguesa de Ciência Criminal, Ano 21, n.º 4, pp. 545 – 591. [consultado a 10.12.2024]. Disponível na internet: https://repositorio-aberto.up.pt/bitstream/10216/133333/2/49978.pdf

[224] Cfr. Art. 34º números 2 e 3 da CRP

[225] Cfr. Art.18 números 2 e 3 da CRP

perante direitos disponíveis. Em relação aos meios relativamente proibidos, os mesmos estão à disponibilidade do titular e, nessa medida, o consentimento é importante para a validade das provas que foram obtidas com a violação desses direitos. Se as provas forem obtidas sem que haja o consentimento do titular em causa estaremos perante uma nulidade relativamente sanável, isto é, quando falamos da violação destes direitos estamos a referir-nos a direitos de personalidade que não ameaçam a dignidade da pessoa humana como o que acontece nos métodos absolutamente proibidos. Neste quadro jurídico, a violação de um direito sem o consentimento é menos grave daí a ficar submetido a um regime de nulidade sanável[226], sendo que é o titular do direito em causa que se entender, porque está no seu âmbito de disponibilidade, propor uma ação neutralizadora invocando a nulidade nos prazos tipificados na lei. O resultado que daí advém é o de que a prova será considerada inválida[227].

A questão que se coloca é de saber de que forma é que poderíamos relacionar os meios de prova absolutamente proibidos e os meios de prova relativamente proibidos numa perspetiva de direito a constituir, visto que o reconhecimento facial não tem aplicação no nosso ordenamento jurídico. Como sabemos, o reconhecimento facial consiste numa forma de identificação biométrica tendo por base caraterísticas faciais. Como meio absolutamente proibido poderia considerar-se quando o reconhecimento facial se realizasse de uma forma clandestina ou sem o consentimento, quando implicasse uma vigilância em massa e discriminatória (aspeto relativamente ao qual é proibido pela Jurisprudência Europeia) e se fosse aplicado com ausência de base legal e sem garantias de proteção dos direitos fundamentais nesse caso a aplicação do reconhecia facial violaria o art. 126 do CPP, traduzindo-se num meio de prova obtido por métodos proibidos por lei sendo inadmissível. Numa perspetiva de meio relativamente proibido poder-se-ia admitir nas situações em que a sua utilização fosse aplicada a casos específicos com uma base legal clara, demonstrando-se como uma prova essencial que de outra forma não seria possível obter, onde existisse uma autorização judicial fundamentada para a sua utilização e por fim existisse o respeito

[226] Neste Sentido, SUPREMO TRIBUNAL DE JUSTIÇA - Acórdão do Supremo Tribunal de Justiça de 20-09-2006, processo 06P2321 consagra o mesmo entendimento: XXVII – (...) "Há, no entanto, outros em que, mediante certos condicionalismos, não repugna admitir a sua violação, abandonando o legislador ordinário aquela tutela absoluta e incontornável, para cair numa inadmissibilidade meramente relativa de tais meios de prova, como forma de salvaguardar «valores de irrecusável prevalência e transcendentes aos meros interesses da perseguição penal»"

[227] LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado,* anotação do artigo 126, pp. 242-243

pelas garantias das pessoas submetidas a esses meios. O reconhecimento facial nessa situação estaria submetido a condições semelhantes ao regime das escutas telefónicas que é admissível apenas em situações excecionais e reguladas na lei, tal como dispõe o acórdão do Tribunal da Relação de Coimbra de 11-05-2016, processo número 98/14.4TANZR-A.C1 que dispõe:

> "Havendo razões para crer que o recurso às escutas telefónicas não só se mostra indispensável para a descoberta da verdade, como a prova seria, de outra forma, impossível ou muito difícil de obter, justifica-se a requerida intercepção e gravação das comunicações telefónicas, assim como se justifica a recolha de imagens pois os resultados de investigação que se pretendem com a realização de tal diligência não são passíveis de ser alcançados através do recurso a outros meios de produção de prova"[228].

Como sabemos atualmente a ausência de regulação legal especifica não permite que o reconhecimento facial seja considerado um meio de prova licito, na medida em que para além da falta de regulação colide com direitos fundamentais, o que significa que até que exista um enquadramento legal próprio que regule a sua utilização de forma cautelosa estaremos perante um meio de prova absolutamente proibido.

De facto, no ordenamento português vigora o princípio da liberdade da prova, segundo o qual são admissíveis todos os meios de prova não proibidos por lei. Não obstante e tratando-se de um princípio que não possui carater absoluto, são-lhe impostos limites que decorrem do próprio CPP, da CRP e de outros instrumentos jurídicos de proteção de direitos fundamentais. Neste quadro, importa evidenciar que o uso de meios probatórios que não se encontrem tipificados na lei e que impliquem a restrição ou compressão de direitos fundamentais como o que acontece com o reconhecimento facial carece de fundamento legal e garantias adequadas. A conjugação do princípio da liberdade da prova com as imposições legais permite constatar que não é admissível a utilização de meios de prova não previstos na lei sem que haja normal legal que os preveja e que defina claramente o seu âmbito, os seus limites e as garantias das pessoas afetadas pelos mesmos.

[228] Neste sentido, COIMBRA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Coimbra, de 11-05-2016, processo número 98/14.4TANZR-A.C1, disponível em: https://www.dgsi.pt/jtrc.nsf/-/8A6512B455A490DD80257FB60032DA8B

Se pensarmos no meio de prova do reconhecimento facial, a sua utilização afeta uma multiplicidade de direitos fundamentais, sobretudo quando falamos de sistemas de reconhecimento facial “em tempo real”, colocando dessa forma sérias questões quanto à sua compatibilidade com os direitos fundamentais. O art.125 do CPP, apesar de consagrar o princípio da liberdade da prova, não significa que a mesma seja interpretada de forma isolada, na medida em que o sistema português impõe limites claros à admissibilidade da prova, em particular quando estejam em causa direitos fundamentais. Neste contexto de análise, o facto de não existir uma proibição expressa no art. 125º do CPP não significa a legitimidade na utilização do reconhecimento facial como meio de prova, contrariamente tendo em conta o impacto que significa para os direitos fundamentais e a ausência de um regime legal que defina as condições e limites da sua aplicação deve entender-se que esta tecnologia é incompatível com o processo penal português.

O progresso científico tem impulsionado a crescente utilização de novas formas de aquisição de provas, inovações que oferecem novas possibilidades para a descoberta da verdade material, permitindo uma investigação mais rápida e eficaz. Não obstante, a principal dificuldade reside em alcançar o equilíbrio entre a eficiência das novas tecnologias e a proteção dos direitos fundamentais. É uma necessidade cada vez mais constante a regulação do uso destas novas tecnologias que têm sido desenvolvidas com incidência em princípios como a transparência, o controlo jurisdicional e o respeito pelas garantias fundamentais de forma a evitar o progresso cientifico ainda que essenciais não se sobreponha aos direitos fundamentais.

Era essencial que o legislador pudesse intervir na regulação destes sistemas, de forma clara, adequada e pormenorizada, impondo as condições necessárias para que se pudesse fazer uso destas tecnologias de forma a não prejudicar as pessoas que são objeto das mesmas. Além de que, devido à agressão que estes sistemas impõe nas pessoas, talvez fosse importante circunscrever o seu uso apenas a situações mais graves e, colocar outros meios probatórios típicos que pudessem corroborar a fiabilidade destes sistemas para assim tentar contornar os erros que estes sistemas proporcionam, garantindo igualmente o contraditório. Segundo o autor Costa de Andrade e à qual concordo: “<< [s]ó uma lei expressa, clara e determinada, especificamente reportada à técnica em causa, definidora e delimitadora da respetiva medida de invasividade e

devassa, pode legitimar a sua utilização como meio de obtenção de prova em processo penal>>"[229].

13. ORIENTAÇÕES PARA O USO DO RECONHECIMENTO FACIAL

Como sabemos, no mundo atual e com os progressivos avanços da inteligência artificial temos assistido à crescente utilização das tecnologias de reconhecimento como tendência no auxílio da investigação criminal.

São várias as preocupações que têm sido levantadas no uso do reconhecimento facial, pelo que face à ausência de um regime jurídico era importante refletir-mos numa ótica de direito a constituir acerca de condições, limites e garantias necessárias à admissibilidade desta tecnologia. Assim, é essencial que a utilização destes sistemas seja regulada de forma a ser coerente com as proteções constitucionais, o que implica que existam leis, regras e políticas que possam controlar o uso destes sistemas, sob pena de levar a uma vigilância em massa e. consequentemente, a uma violação dos direitos humanos. Por conseguinte, uma das recomendações seria a implementação de uma regulamentação e uma política detalhada, onde o reconhecimento facial pudesse ser enquadrado, beneficiando a investigação criminal e o sistema de justiça penal, mas que salvaguardasse e garantisse a defesa dos direitos humanos. O desenvolvimento e a utilização do reconhecimento facial não pode ser visto de forma dissociada da necessidade de proteção dos direitos fundamentais. No entanto e dada a complexidade técnica, são essenciais políticas que contenham uma cooperação interdisciplinar entre, por um lado, técnicos/peritos em direitos humanos e peritos nas áreas do desenvolvimento tecnológico. Esta abordagem deve ser algo contínuo e estruturado ao longo de todas as fases de aplicação desta tecnologia, desde a conceção, como na fase de avaliação e certificação, a fase de integração dos sistemas nas práticas das autoridades de investigação até a monotorização e fiscalização.

Na medida em que estas tecnologias fazem uso de dados pessoais, seja a recolha ou o tratamento de imagens faciais, devem estar em conformidade com os princípios de

[229] ANDRADE, Manuel Da Costa (2009) - "*Bruscamente no verão passado", A Reforma Do Código de Processo Penal. Observações críticas sobre uma lei que podia e devia ter sido diferente*. Coimbra Editora.

proteção de dados da legislação europeia, em particular com a diretiva da proteção geral dos dados na União Europeia[230].

13.1. AUTORIDADES RESPONSÁVEIS PELA APLICAÇÃO DA LEI E UTILIZAÇÃO PERMITIDA

A utilização e o tratamento de dados biométricos tendo por base a utilização do reconhecimento facial independentemente de o ambiente em causa ser controlado ou não, deve ter limitações, nomeadamente, a fins de aplicação da lei.

Não obstante e sendo estes sistemas muito intrusivos os mesmos devem ser efetuados apenas por autoridades exclusivamente competentes. Em particular quando falamos do uso destes sistemas para prossecução de objetivos legítimos pelas autoridades policiais como a prevenção, a deteção e a investigação de outros crimes e, sabendo que a utilização das mesmas acarreta consigo riscos para os direitos humanos é importante que seja definida uma lista exaustiva compreendendo quais os fins legítimos relativamente aos quais esta tecnologia pode ser utilizada e não uma lista aberta que os próprios Estados possam modificar[231], sendo crucial regulamentações cuidadosas e detalhadas que não permitam margem para interpretações erróneas. A ausência de uma regulamentação pode significar que cada Estado tem liberdade total para utilizar e abusar da utilização destes sistemas[232].

Cada Estado pode igualmente prever na sua legislação, consoante os fins sejam de identificação ou verificação tomando em consideração os riscos e o impacto que poderá ter na afetação de direitos e tendo subjacente que as imagens recolhidas sejam feitas de forma legal prever diferentes testes de necessidade e proporcionalidade

[230] DUSHI, Desara (2020) - *The use of facial recognition technology in EU law enforcement: fundamental rights implications* in Global Campus, South East Europe, pp. 5-6. [consultado a 21.01.2025]. Disponível na internet: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

[231] DUSHI, Desara (2020) - *The use of facial recognition technology in eu law enforcement: fundamental rights implications* in Global Campus, South East Europe, p. 6. [consultado a 21.01.2025]. Disponível na internet: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

[232] Idem, p. 10. . [consultado a 21.01.2025]. Disponível na internet: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

consoante o objetivo que pretendem prosseguir. É importante que a legislação preveja parâmetros e normas claras que devem ser aplicadas pelas autoridades responsáveis quando criam bases de dados para fins específicos, legítimos e explícitos de aplicação da lei, como por exemplo casos de risco para a segurança pública ou suspeita de infrações graves[233].

Relativamente à utilização permitida e considerando a potencialidade de intrusão que estas tecnologias podem ter, é essencial uma regulamentação que defina a utilização especifica do reconhecimento facial de uma forma consistente com esses direitos e que proporcione as garantias necessárias. Em contexto de aplicação da lei, a forma de assegurar a proteção dos direitos podia basear-se igualmente em proteções desenvolvidas para outras técnicas de investigação, como vigilância das comunicações, sendo as regras diferentes consoante o caso de utilização por exemplo se estes sistemas são utilizados para autenticar a identidade de alguém; análise forense ou vigilância[234]. Essa base jurídica deve ter em conta a própria vulnerabilidade das pessoas em causa; o ambiente em que são utilizadas e os próprios fins tendo sempre subjacente a conexão estrita dos princípios da necessidade e da proporcionalidade.

13.2 QUALIDADE E REPRESENTATIVIDADE DOS DADOS E ALGORITMOS UTILIZADOS

As entidades que utilizam estes sistemas de reconhecimento facial devem tomar medidas de forma a garantir que os dados são exatos. É essencial que estes sistemas sejam testados de forma a identificar e eliminar disparidades de exatidão em particular a variações demográficas da cor da pele; sexo; idade não permitindo nesta medida discriminações involuntárias.

[233] Council of Europe (2021) - *Guidelines on facial recognition,* pp. 10-11 [consultado a 14.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

[234] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 2. [consultado a 14.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY.

Ademais é importante também garantir a qualidade dos dados e a competência dos algoritmos que são utilizados por isso deverão ser fomentados através de conjuntos de dados sintéticos tendo por base fotografias de diversas pessoas do género masculino e feminino, com diferentes cores de pele; diferentes morfologias; de várias idades e captadas de diferentes ângulos[235].

Em relação à durabilidade dos dados que são recolhidos, devemos entender que é importante a renovação regular dos dados de forma a por um lado treinar e melhorar os algoritmos utilizados nestes sistemas.

A conservação dos dados também tem sido objeto de grande preocupação, ou seja, a captação de imagens para um determinado fim e posteriormente serem usadas para outro objetivo que não tenha sido pré-determinado inicialmente sem o consentimento das pessoas em causa e sem transparência. A fim de evitar estas situações devem ser definidas normas claras que esclareçam quando é que as imagens podem ser armazenadas, qual o período de tempo desse armazenamento e quais as condições em que as imagens captadas podem ser utilizadas[236].

Existe sempre uma percentagem de fiabilidade associada a cada algoritmo de desenvolvimento, o que significa que é necessário um acompanhamento e registo da sua evolução, nos casos em que haja uma deterioração da fiabilidade do mesmo é indispensável o uso de fotografias mais recentes de forma a treinar o sistema evitando consequências associadas a alterações na forma do rosto como o envelhecimento ou outras modificações como tatuagens ou *piercings*[237].

13.3 FIABILIDADE DE INSTRUMENTOS UTILIZADOS

[235] Council of Europe (2021) - *Guidelines on facial recognition*, p. 15 [consultado a 15.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.
[236] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 2. [consultado a 15.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY.
[237] Council of Europe (2021) - *Guidelines on facial recognition*, p. 16 [consultado a 15.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

A eficácia dos algoritmos influencia a fiabilidade das ferramentas que são utilizadas, sendo que a eficácia dos mesmos resulta de várias condições como os falsos positivos e os falsos negativos, a influencia das diferentes luzes, a pouca fiabilidade quando as fotografias do rosto são captadas de outros ângulos, com grandes distâncias e o impacto das coberturas faciais (como máscaras). Tendo em consideração que estamos perante sistemas de reconhecimento facial que têm um grande impacto nos direitos das pessoas que a ele são sujeitas deve ser assegurado um elevado nível de fiabilidade.

13.4 INTERVENÇÃO HUMANA

A utilização destes sistemas de reconhecimento facial como já pudemos afirmar acarretam consigo alguns problemas um deles é a inferência que podem ter nos direitos e liberdades relativamente às pessoas que são sujeitas aos mesmos, nesse sentido é imprescindível que haja regulamentação que vise proteger essas pessoas contra a possibilidade de erros dos algoritmos. Um dos mecanismos que permita garantir essa proteção é assegurar que haja uma pessoa envolvida na revisão das correspondências tomadas pelos *softwares* de reconhecimento facial[238].

Para entendermos a aplicação prática destes sistemas, a análise comparada é fundamental para a construção de possíveis respostas jurídicas perante os desafios que têm vindo a ser colocados pelas tecnologias de reconhecimento facial e para uma melhor formulação de políticas públicas e legislação nacional. É particularmente valioso recorrermos ao conhecimento comparado visto que estes sistemas ainda se encontram num domínio em construção. Estas tecnologias dada a sua complexidade técnica e o potencial impacto que pode ter nos direitos fundamentais exigem uma reflexão transversal que ultrapasse as fronteiras do direito nacional.

São diversos Estados que tentaram regulamentar o reconhecimento facial incluindo a intervenção humana. Washington tentou colocar em prática esta medida e

[238] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 9. [consultado a 15.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY.

exigiu que os operadores que fizessem uso de sistemas de reconhecimento facial tomassem decisões que tivessem impactos significativos para as pessoas, garantindo que essas decisões fossem objeto de revisão humana. O que a legislação pretendeu foi que houvesse uma supervisão do funcionamento ou revisão das decisões do sistema através de operadores humanos devidamente formados.

Também na legislação do Louisiana implementou-se um requisito semelhante, no entanto, não forneceu uma definição de análise humana considerável.

Já a legislação proposta no Minnesota e no 116º Congresso dos Estados Unidos determinaria que as agência de aplicação da lei não poderiam ter contacto com qualquer pessoa que teria sido identificada por um sistema de reconhecimento facial, exceto se um agente tivesse examinado o resultado.

No estado de Utah a legislação exigia que quaisquer possíveis correspondências tivessem de ser examinadas por dois funcionários diferentes. O que se pretende é que cada um deles concorde que a pessoa que foi identificada pelos sistemas de reconhecimento facial é a correspondência provável antes dos resultados serem enviados a uma agência de aplicação de lei.

A proposta de regulação através da intervenção humana permite de alguma forma assegurar as pessoas de danos que possam resultar dos algoritmos. uma forma de puder reduzir essas probabilidades e diminuir o seu risco é assegurar que existe uma intervenção do ser humano na revisão das correspondências geradas pelos *softwares* de reconhecimento facial. As legislações que têm adotado estes mecanismos de segurança consideram que os funcionários devem ser devidamente formados antes de terem uma autorizaram de operar ou rever as decisões que resultam destes sistemas.

O Estado de Washington por exemplo impõe que os funcionários das agências que trabalham com os sistemas de reconhecimento facial tenham uma formação frequente, sendo que esta abrange a explicação das capacidades e limitações do próprio sistema, a interpretação e atuação em relação às correspondências do sistema. No estado do Utah a lei proíbe que sejam efetuadas buscas por pessoas responsáveis

que não tenham tido formação sobre como proceder à comparação de reconhecimento facial e que não tenha terminado o teste de preconceitos implícitos[239].

13.5 PRINCÍPIO DA NECESSIDADE

Um dos princípios importantes quando falamos do uso dos sistemas de reconhecimento facial é o princípio da necessidade que está relacionado com a ideia de que o reconhecimento facial só pode ser utilizado quando existir uma necessidade especifica e deve ser limitado ao estritamente necessário tendo em consideração o fim legítimo e específico que se visa atingir. Este princípio também tem ligação a uma ideia de proporcionalidade[240], ou seja, o uso destes sistemas só deve operar quando os outros meios tradicionais de investigação não forem idóneos para atingir os mesmos objetivos, no fundo é uma priorização dos meios típicos e menos intrusivos já existentes na legislação de cada Estado.

O princípio da necessidade também pode ser visto no âmbito da investigação no uso destes sistemas, ou seja, no sentido de a legislação só permitir recorrer a este meio para fins de investigação como um elemento adicional. A identificação através destes sistemas só pode ser usada numa acusação ou numa fase de julgamento se existir outras provas que possam corroborar os resultados apresentados por esses sistemas[241]. Este princípio também é referido no âmbito do tratamento de dados previsto na diretiva da União Europeia[242] que dispõe que os mesmos devem ser objeto de um

[239] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, pp. 9-10. [consultado a 16.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY.

[240] A Jurisprudência do Reino Unido sobre esta ideia de proporcionalidade e necessidade, entendeu no caso Bank Mellat do Supremo Tribunal que era necessário estabelecer uma série de testes que permitisse avaliar se a interferência nos direitos das pessoas era justificado. Os responsáveis pelo tratamento de dados, devem considerar se o seu objetivo é suficientemente importante que justifique o tratamento dos dados biométricos e a interferência na vida privada das pessoas; e por último se houve um equilíbrio justo entre os interesses do responsável pelo tratamento; os direitos do indivíduo e os interesses da coletividade. É importante avaliar a importância do objetivo por um lado e o equilíbrio de interesses o que muitas vezes pode ser uma questão delicada. Cfr. Information Commissioner's Office: The use of live facial recognition technology in public places (2021), p. 36, [consultado a 10.02.2025]. Disponível na internet: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

[241] MEZZOMO, Maria Luiza (2024) - *O Uso Do Reconhecimento Facial Na Investigação Criminal E Na Segurança Pública*. Edições Almedina, pp. 97-98

[242] Cfr. Arts. 4º e 5º da DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016

tratamento lícito; recolhidos para fins pré-determinados e legítimos; sendo limitados ao mínimo necessário em relação aos objetivos que visam alcançar. Não obstante este princípio também é aferido relativamente aos prazos de conservação dos dados pessoais que dispõe de um limite adequado a partir do qual os dados devem ser excluídos quando já não houver justificação legítima para os fins que foram recolhidos. Se pensarmos na aplicação deste princípio ao uso do reconhecimento facial isto significa, que o rosto da pessoa identificada para fins de investigação criminal só pode manter-se armazenada até ao cumprimento da sanção pelo facto do fim não se demonstrar mais necessário e sob pena da imagem ser utilizada para outros fins não legítimos[243].

13.6 REQUISITOS DE TESTE

Para assegurar a fiabilidade dos sistemas de reconhecimento facial algumas leis e regulamentos exigiram que os operadores que fizessem uso desses sistemas fossem obrigados a testarem a fim de determinar o seu desempenho e verificar se as taxas de exatidão variavam ou não consoante os diferentes grupos demográficos. Por exemplo no Estado de Washington é exigido que as agências examinem e façam testes antes destes sistemas puderem ser usados para tomar decisões que possam resultar em consequências legais ou outras repercussões que afetem significativamente as pessoas alvo desses sistemas. Também no Minnesota foi proposto e no 116º Congresso dos EUA a obrigação de criar um procedimento para testar de forma autónoma qual o desempenho destes sistemas no desenvolvimento de operações e indagar se existiam diferenças de performance entre diferentes grupos demográficos, sendo obrigadas a informar sobre quaisquer diferenças demográficas que fossem detetadas durante os testes[244].

No mesmo sentido em 2019 a proposta de *Algorithmic Accountability* teria prescrito que a Comissão Federal do Comércio aprovasse normas que impusessem a todos os operadores de sistemas de alto risco que incluiria os sistemas de

[243] MEZZOMO, Maria Luiza (2024) - *O Uso Do Reconhecimento Facial Na Investigação Criminal E Na Segurança Pública*. P.99

[244] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 6 [consultado a 22.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY

reconhecimento facial a realizar testes de precisão, parcialidade; riscos de segurança dos algoritmos e repercussões no âmbito da privacidade. Os testes realizados teriam de ser feitos em condições operacionais, ou seja, era examinado os níveis de desempenho de um algoritmo num conjunto de imagens pré-selecionadas configuradas para avaliar a forma como o algoritmo age numa determinada situação especifica em particular imagens de pessoas com máscaras faciais; imagens mal iluminadas; imagens em ângulos diferentes; imagens de pessoas que pertencem a determinados grupos sociais e pessoas de diferentes idades. Já os testes operacionais, teriam por base a possibilidade de permitir que as agências recolham informações sobre o desempenho real dos sistemas no contexto de utilização, sendo que este último tem um desempenho inferior quando comparado com os testes realizados em laboratórios na medida em que estão sujeitos a fatores como o comportamento imprevisível do sujeito e erros do operador[245].

13.7 RESTRIÇÕES NA UTILIZAÇÃO DOS SISTEMAS DE RECONHECIMENTO FACIAL

Outra medida importante seria a implementação em disposições legais de restrições na utilização dos sistemas de reconhecimento facial. Já existem inclusivamente alguns regulamentos onde são enumerados de forma explicita quais as circunstâncias onde os operadores podem usar estes sistemas e por outro lado apresentando as situações relativamente às quais está vedada essa utilização.

Por exemplo, no Hawai foi apresentado um projeto de lei que apenas permitia o uso das tecnologias de reconhecimento facial para criar um ajustamento de fotografias para testemunhas oculares ou para equiparar fotografias de câmaras de vigilância com registos de detenção (sem identificações estatais). No entanto e já tendo mencionado que estes sistemas podem ser bastante invasivos alguns Estados colocaram restrições no que concerne aos tipos de infrações praticadas, identificando quais delas é que se pode fazer uso reconhecimento facial para investigar. Por exemplo no Utah a polícia só pode usar o reconhecimento facial a fim de prestar auxílio à investigação de crimes

[245] Idem, p.6

dolosos e violentos, outros Estados como Louisiana e Massachusetts atualmente também estão a ponderar colocar normas que apliquem restrições semelhantes.

No que diz respeito à afetação dos direitos fundamentais que estes sistemas podem ter, também foi feito regulamentos que proíbem essa interferência, em particular o Estado de Washington proibiu as agências de utilizar o FRT tendo por base a religião, a raça, o género, a filiação política ou alguma outra caraterística relacionada com o individuo. Seguindo esta ideia também a legislação no Arizona não permitia utilizações que tivessem por base causas discriminatórias identificadas ou que tivessem um impacto diferente em qualquer comunidade[246].

13.8 CONTROLO E AUDITORIA DOS SISTEMAS DE RECONHECIMENTO FACIAL

A utilização de sistemas de reconhecimento facial implica que exista mecanismos precisos que controlo e de autoria que permitem assegurar que são utilizados de acordo com os preceitos legais; a proteção dos direitos fundamentais e a proteção dos dados pessoais . É assim importante garantir mecanismos que permitam que estes sistemas sejam usados respeitado princípios éticos, com segurança e respeitando os direitos das pessoas que por eles são afetadas. Cada Estado ao autorizar o uso destes sistemas deve também acautelar mecanismos de controlo e, terá de ser acompanhada por uma avaliação sobre os efeitos da privacidade. As auditorias realizadas aos sistemas para analisar o seu desempenho e a sua exatidão também devem ser públicos, assim como a exigência de um relatório anual sobre a sua utilização.

13.9 PROTEÇÃO DOS DIREITOS DAS PESSOAS

Já fomos mencionando o quão o reconhecimento facial pode afetar os direitos fundamentais das pessoas e, visto que estes sistemas têm por base o tratamento de

[246] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 6 [consultado a 23.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY

dados pessoais é garantido nos termos do art. 9º da Convenção 108+ o direito de acesso; o direito à informação; o direito de oposição e o direito de retificação. É importante mencionar que em princípio não será permitido qualquer restrição aos direitos a não ser em situações excecionais – como encontrar-se prevista na legislação; respeitar o conteúdo essencial dos direitos e liberdades fundamentais; ser uma medida necessária e proporcional e ter um objetivo específico como se encontra previsto no art. 11º da Convenção[247]. Nas situações em que são impostas limitações aos direitos, as autoridades responsáveis pela aplicação da lei têm um dever de informar as pessoas em causa de, se quiserem, apresentarem queixa às autoridades de controlo e a possibilidade de recorrerem da decisão.

Se na utilização destes sistemas ocorrer um erro ou uma falsa correspondência existe a possibilidade de as pessoas em causa solicitarem a retificação a fim de evitar novamente uma falsa correspondência. No mesmo sentido se o uso das tecnologias de reconhecimento facial tiverem como objetivo a tomada de decisão tendo apenas em conta o tratamento automatizado e, se afetar a pessoa em causa esta tem o direito de não permitir que esse tratamento seja realizado sem o seu consentimento. Também nos termos do art. 9 nº1 alínea a) da Convenção se, na utilização do reconhecimento "em tempo real" os operadores agirem tendo apenas por base os resultados que foram obtidos por estas tecnologias e, portanto, significa que a decisão tomada foi exclusivamente automatizada e nessa medida pode afetar significativamente os direitos das pessoas também pode ser solicitado que a opinião da pessoa em causa seja tida em consideração[248].

Ainda que, seja delimitado através de normas e regulamentos proibições e restrições no uso de tecnologias de reconhecimento facial e seja um passo importante é igualmente importante que sejam previstas sanções ou procedimentos que obstem contra o uso abusivo; a negligência e condutas incorretas. Algumas propostas vieram adicionar diferentes repressões que diferiam consoante a gravidade e a natureza da violação. São vários os regulamentos que impõe que qualquer informação recolhida ou obtida de forma ilegal através dos sistemas de reconhecimento facial seja eliminada, inclusive nesses processos as políticas têm permitido os queixosos sejam indemnizados com montantes pré-definidos de forma a compensar os danos reais ou punitivos. Não

[247] Cfr. Convenção 108 + Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal
[248] Council of Europe (2021) - *Guidelines on facial recognition*, p. 27 [consultado a 24.01.2025]. Disponível na internet: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

obstante a possibilidade de compensação de danos, algumas propostas de legislação podem aplicar multas e sanções por violações às entidades públicas ou privadas, sendo que valores podem ser diferentes consoante a violação que está em causa, se foi por negligência, de forma imprudente e negligente. É essencial que o desenvolvimento do reconhecimento facial seja acompanhado por regras e controlo de forma a garantir a segurança pública, os direitos fundamentais e a privacidade[249].

13.10 PRINCÍPIO DA TRANSPARÊNCIA E EQUIDADE

Um dos principais pilares que pode orientar a implementação e o uso responsável do reconhecimento facial é o princípio da transparência garantindo a confiança pública na medida em que quanto mais a população for informada mais confiança pode desenvolver em relação a estas tecnologias permitindo assim uma maior aceitação; a proteção de direitos fundamentais e a conformidade com a legislação em vigor, as bases legais utilizadas; as formas de armazenamento no fundo e aplicando ao reconhecimento facial permite que as pessoas tenham a perceção de quem coleta os seus dados pessoais; qual o objetivo de o fazer; os benefícios e riscos associados a essa colheita e quais os seus direitos quando são usados estes sistemas. Este princípio tem previsão legal na Diretiva número 2016/680 da União Europeia[250] que dispõe nos termos do art. 12º número 1 a exigência de uma comunicação clara utilizando linguagem clara e simples e o respeito do tratamento dos dados de forma concisa e inteligível. No mesmo sentido, e relativamente ao tratamento de dados pessoais, também temos o Regime Geral da Proteção de Dados Pessoais[251] que dispõe que os tratamento de dados pessoais deve ser licito, leal e transparente.

As condições de transparência podem compreender consultas públicas; disponibilização de informações às pessoas de como é que a tecnologia está a ser utilizada e relatórios anuais[252].

---

[249] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, p. 6 [consultado a 23.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY.

[250] Cfr. Diretiva ((UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de Abril de 2016

[251] Cfr. Art. 5º número 1 do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia n.º 679/2016, de 27 de Abril

[252] LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape* by the Center for Strategic and International Studies, pp.14-15

De forma a efetivar e garantir a transparência têm sido aprovados diversos atos legislativos, por exemplo obrigando que os operadores de reconhecimento facial demonstrem de forma publica a forma como estes sistemas estão a ser usados e geridos. Estas medidas têm incidência em três âmbitos na implementação e operação do reconhecimento facial. A primeira fase é o procedimento de aquisição, algumas normas impuseram que fossem comunicadas uma política de utilização e uma análise sobre os impactos dos mesmos antes da sua implementação.

Temos nos Estado de Washington normas que exigiam a apresentação de um relatório pormenorizado sobre o operador do reconhecimento facial; as suas finalidades; a área de implementação e uma gestão dos dados obtidos com o objetivo de entender como as informações seriam utilizadas e posteriormente armazenadas. Estas informações teriam de ser apresentados num espaço de 90 dias antes da efetivação destes sistemas sendo publicado e atualizado de dois em dois anos. No estado do Arizona também foram estabelecidas exigências igualmente semelhantes. Neste seguimento também foi aprovado algumas normas que requeriam que os operadores informassem e colaborassem com as comunidades de forma a prestar e explicar a forma como estes sistemas iriam operar antes da sua implementação. O Estado de Washington e a cidade de Seatle adotaram esta norma requereram que os operadores realizassem consultas às comunidades antes da implementação. O mesmo aconteceu nas legislações propostas em Nova Jersey e no Arizona onde existe a obrigação da realização de audiências públicas antes da utilização do reconhecimento facial[253].

A segunda fase para a regulamentação da transparência é o período onde o reconhecimento facial está a ser a funcionar ou a captação de imagens que estão a ser captadas e que podem porventura ser utilizadas pelo reconhecimento facial. Exemplos práticos deste segundo momento é por exemplo no Utah exige-se que as pessoas sejam sempre informadas quando houver a captação de imagens para os sistemas de reconhecimento facial.

A terceira fase é assegurar que com a implementação destes sistemas, os seus resultados sejam disponibilizados ao público e a todas as pessoas afetados. Muitos regulamentos conseguiram alcançar este terceiro objetivo implementando que as agências que utilizavam ou efetuavam pesquisas de reconhecimento facial elaborassem relatórios públicos em cada ano que continha aspetos da forma como estes sistemas

[consultado a 28.01.2025]. Disponível na internet: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210929_Lewis_FRT_UsePrinciplesLegislative_1.pdf?VersionId=LYP6ru3V4nvo8kGyt.T5GDyxXRfBAJhY

[253] Idem, pp.7-8

foram utilizados. Estes relatórios podem integrar aspetos que contenham informações sobre número de buscas efetuadas assim como o número de detenções e condenações decorrentes das buscas; número de correspondências; os crimes e suspeitos que se encontram a ser investigados e as queixas/denúncias efetuadas contra o sistema.

Também foram tomadas medidas no âmbito da investigação criminal onde foi exigida que informações acerca de buscas realizadas através do reconhecimento facial fossem transmitidas aos arguidos, por exemplo o Estado de Washington obriga que os arguidos sejam informados sobre a utilização do reconhecimento facial em tempo útil antes da realização da audiência de julgamento embora não especifique o conteúdo das informações divulgadas. Também na legislação de Louisiana qualquer pessoa que seja detida devido a uma investigada efetuada pelo reconhecimento facial tem de ser informada no prazo de 48 horas com direito a saber qual o objetivo da busca; a base de dados utilizada; e os pormenores compreendidos na ordem judicial de autorização[254].

É importante referir que a utilização destes sistemas pode potenciar resultados discriminatórios levando a consequências como injustiças com base no género, sexo, raça, incapacidade ou deficiência, idade e outros aspetos demográficos. Para além disso ainda existe riscos de discriminação e enviesamento no processo de criação das listas de observação. É importante que os responsáveis na aplicação destes sistemas e consequente tratamento de dados tomem medidas que permitam prevenir este risco como por exemplo ponderar os riscos de enviesamento, de discriminação e tratamento justo dos diferentes grupos demográficos durante as várias fases do processo de conceção, adjudicação ou aquisição de sistemas de reconhecimento facial, o que significa que sempre que for necessário ou se demonstre justificado, deve ser pedido garantias aos fornecedores, justificar e registar as suas decisões sobre as questões; inspecionar os resultados produzidos pelo sistema, compreendendo quaisquer indícios de parcialidade ou discriminação e adaptação da abordagem com base nas conclusões e averiguar se o sistema é adequado para a utilização[255].

Em suma, estes princípios são muito importantes no sentido em que permitem mitigar os impactos negativos destes sistemas, prevenindo possíveis abusos, promovendo a confiança e assegurando a proteção de dados pessoais e dos direitos das pessoas em causa.

[254] Idem, pp.7-8
[255] Information Commissioner's Office (2021) - *The use of live facial recognition technology in public places*, p. 39. [consultado a 10.02.2025]. Disponível na internet: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

13.11 CONSENTIMENTO

Os sistemas de reconhecimento facial quando operam lidam com a coleta de dados biométricos sensíveis o que significa que é necessário o consentimento das pessoas em causa, de forma a garantir um controlo de cada um sobre as suas informações e a proteção dos seus dados. Associado ao consentimento está o facto da pessoa ser informada de forma adequada antes de prestar o seu consentimento; o consentimento ser atual, para um fim concreto; voluntário e consciente. O que acontece é que a própria natureza do reconhecimento facial não permite cumprir todas estas etapas acabando por serem captados dados sem que haja um consentimento expresso das pessoas afetadas. Nem sempre é suficiente existir uma indicação ou aviso da utilização do reconhecimento facial para demonstrar que a pessoa consentiu[256].

Antes da utilização dos sistemas de reconhecimento facial devem ser ponderadas algumas questões. Existe vários tipos de consentimentos: o consentimento informado – o que significa que deve existir uma informação para que a pessoa quando frequenta um espaço onde o reconhecimento facial opera seja avisado que será retirada uma imagem ao seu rosto e consequentemente serão retirados os seus dados biométricos com o objetivo de estabelecer se à uma possível correspondência fazendo essa comparação com um banco de dados. Devem ser inclusive prestadas informações de quais as consequências/ações que podem ocorrer se houver uma correspondência. Temos também o consentimento voluntário que consiste no facto das pessoas puderem decidir ou não que seja captada uma imagem do seu rosto; o consentimento atual e específico que dispõe que deve ser assegurado o consentimento para recolher, utilizar ou revelar os dados; o consentimento por capacidade que é baseado na consciência de consentir, neste caso podem interferir aspetos relacionados com a idade ou deficiências. Por fim temos o consentimento implícito que por norma não deve ser invocado para obter informações que contenham informações sensíveis e, que caso haja um mau uso do mesmo pode trazer consequências para as pessoas. Existem no entanto situações muito especificas que permitem a coleta das informações sem o consentimento como por exemplo situações em que possa estar em causa a segurança pública; investigação

[256] Australian Government: Office of the Australian Information Commissioner (2024) - *Facial recognition technology: a guide to assessing the privacy risks,* [consultado a 28.01.2025]. Disponível na internet: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks.

de crimes graves desde que obviamente esteja legalmente autorizado ou quando haja um interesse legítimo. No entanto existe situações onde é necessário um mandado ou uma autorização do tribunal para que possam ser utilizados[257].

É assim essencial serem estabelecidas regras que sejam equilibradas e coerentes com os princípios e garantias constitucionais; proporcionando que os titulares dos dados possam controlar as suas próprias informações. Dessa forma é importante que os próprios Estados e organizações provenham condutas práticas e acessíveis que respeitem os direitos fundamentais.

[257] Idem

14. CONCLUSÕES

Esta dissertação teve como objetivo estudar o reconhecimento facial por algoritmos de inteligência artificial, caracterizando-o, discutindo o seu funcionamento e a possibilidade de este poder ser utilizado no Direito Processual Penal Português.

Procedeu-se a uma análise das limitações e das fragilidades associadas à prova por reconhecimento, que são de extrema importância, na medida em que um reconhecimento errado pode ter repercussões muito grandes. Embora este meio de prova continue a ser muito importante (e utilizado) para identificar os responsáveis pelas práticas de um crime, assumindo um valor probatório elevado na convicção do julgador, existem fragilidades. Desde logo em aspetos relacionados com a memória humana, tais como a incapacidade de reconstrução de um facto passado (o próprio processo de recuperação de um facto passado que esteja armazenado na nossa memória pode sofrer interferências, alterando as informações armazenadas e traduzindo -se nas chamadas memórias falsas) *a unconscious transference* e o *yes effect*.

Desta forma, e perante estas limitações e a dúvida constante quanto à confiabilidade da prova por reconhecimento, começou a suscitar interesse a procura por meios de prova mais objetivos e tecnicamente mais avançados. Com o avanço da tecnologia, foram surgindo novas alternativas envolvendo a inteligência artificial, em particular, o reconhecimento facial, que se baseia numa análise algorítmica de imagens captadas por câmaras de videovigilância com imagens constantes em bancos de dados.

É de fácil compreensão o interesse pelo reconhecimento facial por via de algoritmos de inteligência artificial pelas vantagens e progressos que estes sistemas proporcionam, desde a rapidez na identificação, procedimentos de identificação pouco invasivos e facilidade nos resultados. Tudo isto contribui para os próprios fins do processo penal (como a descoberta da verdade material), que pode ter várias vantagens na medida em que não depende da memória humana e permite resultados mais fidedignos.

À primeira vista, parecem bastante eficientes e vantajosos, no entanto, estes instrumentos podem ser bastante problemáticos, desde logo pelas relevantes taxas de erro e inexatidão dos *softwares* que são utilizados por estes sistemas. As próprias condições ambientais como a iluminação, a baixa resolução das imagens, a baixa

precisão em certos grupos demográficos, em particular pessoas com cor de pele mais escura, traduzindo-se em situações de preconceitos e discriminação. Alterações na aparência também podem condicionar o reconhecimento, como o envelhecimento, a utilização de maquilhagem, mudanças no cabelo ou a utilização de máscara.

A todas as desvantagens enumeradas anteriormente, junta-se ainda o impacto que estas tecnologias podem ter na restrição de direitos fundamentais, sendo esta situação ainda mais grave quando nos referimos a tecnologias "em tempo real", o que significa que são instalados sistemas de reconhecimento facial e que são captadas, analisadas e comparadas imagens de todas as pessoas que passaram naquele local de videovigilância, afetando um número incalculável de pessoas. Tais procedimentos contendem de forma relevante com direitos fundamentais como o direito à imagem, o direito de autodeterminação, à proteção dos dados pessoais, ou os direitos à liberdade de expressão, reunião e manifestação.

Estudou-se, adicionalmente, a possibilidade de aplicação do reconhecimento facial por algoritmos de inteligência artificial no processo penal português. Partiu-se do regime do artigo 126º do CPP (métodos proibidos de prova), que admite provas e meios de prova de que não sejam proibidas por lei, tendo subjacente o princípio da não taxatividade. A primeira questão colocada foi a de que apenas se poderia admitir um meio de prova que não estivesse já tipificado e que não fosse idóneo a alcançar esse resultado. Nesse capítulo (capítulo 12) foi referido que, de facto, quando falamos da prova por reconhecimento, a ideia subjacente também é permitir a identificação de uma pessoa.

No entanto, entendemos igualmente que o fim não se afigura o mesmo, na medida em que neste meio de prova temos a recuperação através da memória de uma pessoa de um facto que ocorreu no passado. Ao invés, no reconhecimento facial, o fim último também é a identificação, mas essa identificação é feita de forma automatizada através da comparação de imagens, daí entendermos que não se trata de um desvio à figura do reconhecimento facial que se encontra prevista no nosso ordenamento jurídico. Pese embora o exposto, encontramos outras questões que na reflexão da admissibilidade do reconhecimento facial à luz do processo penal começaram a surgir. São estas a impossibilidade de exercer o princípio do contraditório, um princípio que é central no processo penal, ou seja, a possibilidade de reagir contra as provas que são

contra si apresentadas. Sabe-se que o arguido não tem possibilidade de ter esse controlo, até porque, na maioria das vezes, este reconhecimento é feito de forma oculta e, portanto, não era possível que este princípio fosse assegurado a não ser que o legislador pudesse vir a intervir garantindo a fiabilidade dos resultados através de outros meios de prova e desse oportunidade ao arguido de se pronunciar sobre essas provas.

A utilização de sistemas de reconhecimento facial como meio de prova no processo penal deve ser considerada inadmissível à luz do ordenamento jurídico português. O reconhecimento facial ao implicar a recolha e o tratamento de dados biométricos representa uma restrição aos direitos fundamentais. De acordo com o art. 18º número 2 da CRP, as restrições apenas serão legitimas quando contenham uma base legal e obedecem a critérios de necessidade, adequação e proporcionalidade. Nesta situação, tratando – se de um meio atípico, ausente de previsão legal especifica que o regule de forma clara, transparente e garantistico impede que o mesmo possa ser admitido como meio de prova válido no processo penal.

Apesar de ser um assunto bastante controverso devido às grandes implicações que estes sistemas podem suscitar, e de forma a regulamentar estes sistemas, também a União Europeia veio regulamentar a forma como estes sistemas podem ser utilizados, categorizando-os consoante o maior ou o menor risco e impondo restrições e obrigações. Em relação a proibições específicas do reconhecimento facial, impõe a proibição de utilização de sistemas de identificação biométrica à distância “em tempo real” para fins de aplicação da lei em espaços acessíveis ao público, exceto em situações muito excecionais previstas e devidamente autorizadas por uma autoridade judicial ou administrativa independente. Também dispõe de um aspeto importantíssimo que se relaciona com a criação de bases de dados de reconhecimento facial ao qual proíbe expressamente a criação ou expansão de bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais da internet ou de sistemas de videovigilância, visando proteger os direitos fundamentais e a proteção dos dados pessoais vendando a utilização não autorizada de dados biométricos para fins de reconhecimento facial.

Entende-se, face ao exposto, que a resposta à questão de investigação desta dissertação passa pela distinção entre direito constituído (o que existe no nosso ordenamento jurídico atualmente) e o direito a constituir. No direito constituído, dada a

ausência de uma lei específica que regule a sua aplicação, o princípio da legalidade e os riscos constitucionais e a sua implicação na restrição de direitos fundamentais, não é possível a aplicação do reconhecimento facial no ordenamento jurídico português. No entanto, numa perspetiva de direito a constituir e face ao crescimento sofisticado da criminalidade e ao avanço tecnológico, é necessário adotar meios mais organizados e estratégicos. Da mesma forma, seria importante fazer uso de meios também mais desenvolvidos que pudessem acompanhar essa evolução.

Os sistemas de reconhecimento facial (por algoritmos de inteligência artificial), pelas grandes vantagens que deles podemos retirar, podem ser um importante contributo para esta progressão sem, contudo, esquecer que poderão colidir com princípios fundamentais do estado de direito democrático. Conclui-se, por conseguinte, que a única forma de dar uso aos mesmos seria ao estipular situações muito específicas e excecionais estritamente permitidas pelo legislador e de forma a não comprometer os direitos fundamentais, acompanhado de um rigoroso controlo jurídico e constitucional em particular em matéria de direitos fundamentais. A a sua utilização deve ser balizada por critérios de necessidade, adequação e proporcionalidade, garantindo que serve finalidades legitimas, não comprometendo o equilíbrio processual entre as partes.

Estes sistemas seriam tidos não como meios de prova autónomos, mas sim auxiliares e operando como auxílio aos meios de prova já tipificados por lei. Para a sua formulação, poderíamos ter como referência os desenvolvimentos legislativos e regulamentares tanto a nível nacional como a nível europeu como o Regulamento de Inteligência Artificial da União Europeia 2024/1689 e com exigências legais rigorosas garantindo um equilíbrio por um lado pelos fins do processo penal e por outro os direitos fundamentais subjacentes a um Estado de Direito democrático.

De igual forma, seria importante adotar orientações para o uso destes sistemas como são implementados noutros países que usam sistemas de reconhecimento facial, como legalidade e regulamentação o que significa bases legais e seguras, com diretrizes específicas para a sua utilização; princípios como a necessidade e proporcionalidade, ou seja, estes sistemas pelo perigo que representam só deveriam ser utilizados quando se demonstrasse que eram absolutamente necessários para atingir fins legítimos e não acessíveis com outros meios de prova.

Adicionalmente, importa garantir transparência na sua utilização, utilizando meios de divulgação que permitissem explicar a forma como estes sistemas operam; a supervisão e responsabilização pelos órgãos competentes de forma a evitar usos inadequados e abusos e proteção de dados pessoais criando formas de assegurar que os dados biométricos fossem armazenados em locais seguros impedindo que fossem utilizados para outros fins e criando políticas de retenção e exclusão de dados, a fim de garantir que os dados não eram armazenados de forma indefinida.

Em suma, a integração cautelosa e regulada dos sistemas de reconhecimento facial poder contribuir para uma justiça mais rápida, eficiente e tecnologicamente mais evoluída sem abdicar dos valores estruturantes do Estado de Direito democrático.

BIBLIOGRAFIA

ALBERGARIA, Pedro Soares de (2024) - *Comentário Judiciário Do Código De Processo Penal Tomo II, Artigos 124 a 190º*. 4ª edição, Coimbra: Almedina

ALBUQUERQUE, Paulo Pinto de (2023) - *Comentário do Código de Processo penal à luz da Convenção Europeia dos Direitos Humanos*, Volume 1. 5ª edição atualizada, UCP editora.

ALVES, Bruno (2012) – *A Prova por Reconhecimento em Processo Penal*. Fronteira do Caos

ANDRADE, José Carlos Vieira de (2019) - *Os Direitos Fundamentais na Constituição Portuguesa* de 1976. 6ª edição, Coimbra: Almedina

ANDRADE, Manuel da Costa (2009) - "*Bruscamente no Verão Passado", A Reforma Do Código de Processo Penal. Observações críticas sobre uma lei que podia e devia ter sido diferente*. Coimbra editora

ANDRADE, Manuel da Costa (2022) – *Sobre as Proibições de Prova em Processo penal*. 2ª edição, Gestlegal

ANTUNES, Maria João (2023) – *Direito Processual Penal*. 5ª edição – Reimpressão 2025, Coimbra: Almedina

FERMINO, Júlia Klehm; AGUIAR, Lúcia Frota Pestana de (2024) – *Direito Animalista: A Natureza e Além*. Dialética Editora

GONZÁLEZ, José Alberto (2019) – *Código Civil Anotado – Volume 1*. 2ª edição, Quid Juris

LOBO, Fernando Gama (2022) - *Código de Processo Penal Anotado.* 4ª edição, Coimbra: Almedina

MENDES, Paulo Sousa; PEREIRA, Rui Soares (2020) - *Novos desafios Da Prova Penal.* Coimbra: Almedina

MEZZOMO, Maria Luiza (2024) *O Uso Do Reconhecimento Facial Na Investigação Criminal E Na Segurança Pública.* Coimbra: Almedina

MIRANDA, Jorge; MEDEIROS, Rui (2017) – *Constituição Portuguesa Anotada Volume I*. 2ª edição revista, Universidade Católica Editora

ROCHA, Manuel Lopes; PEREIRA, Rui Soares (2020) – Inteligência Artificial & Direito. Reimpressão 2024, Coimbra: Almedina

RODRIGUES, Anabela Miranda (2022) - *A inteligência Artificial no Direito Penal*. Coimbra: Almedina

RODRIGUES, L. Barbosa (2021) – *Manual de Direitos fundamentais e de Direitos Humanos*. Quid Juris

SANTOS, Hugo Luz Dos (2022) - *Inteligência Artificial e Processo Penal*. Nova Causa: Edições Jurídicas

SILVA, Francisca Oliveira (2024) - *Prova por Reconhecimento e Inteligência Artificial.* Coimbra: Almedina

SILVA, Germano Marques Da (2017) - *Direito Processual Penal Português, Noções e Princípios Gerais; Sujeitos Processuais; Responsabilidade Civil conexa com a Criminal; Objeto do processo.* vol.1, 2º edição, UCP Editora

SILVA, Germano Marques da (2011) - *Curso de Processo Penal II*. 5ª edição, Verbo

Sindicato dos Magistrados do Ministério Público (2024) - *Revista do Ministério público 177*

SOUSA, Luís Filipe Pires de (2020), *Prova Testemunhal – Noções da Psicologia do Testemunho*. 2ª edição, Coimbra: Almedina

JURISPRUDÊNCIA:

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS - Acórdão do Tribunal dos Direitos Humanos de 06/09/1978, processo número 5029/71, disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57510%22]}.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS - Acórdão do Tribunal Europeu dos Direitos Humanos de 07/12/2006, processo número 29514/05. Disponível em: https://hudoc.echr.coe.int/eng?i=001-78858.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS – Acórdão do Tribunal Europeu dos Direitos Humanos, de 04-07-2023, processo número 11519/20. Disponível em: https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS – Acórdão do Tribunal Europeu dos Direitos Humanos, 4-12-2008, processo 30562/04 e 30566/04, disponível em: https://hudoc.echr.coe.int/fre?i=001-90051.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS – Acórdão do Tribunal Europeu dos Direitos Humanos de 13/02/2020, processo 45245/15, disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200817%22]}.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA - Acórdão do Tribunal de Justiça da União Europeia de 26-01-2023, processo número C-205/21. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-01/cp230016pt.pdf.

SUPREMO TRIBUNAL DE JUSTIÇA – Acórdão do Supremo Tribunal de Justiça de 20-09-2006, processo número 06P2321, Relator: Armindo Monteiro, disponível em: https://diariodarepublica.pt/dr/detalhe/acordao/06p2321-2006-89075175.

SUPREMO TRIBUNAL DE JUSTIÇA - Acórdão do Supremo Tribunal de Justiça, de 07-11-2007, processo número 07P3630, Relator: Henriques Gaspar, Disponível em: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/134027f113c83ddb802573a000501952?OpenDocument.

SUPREMO TRIBUNAL DE JUSTIÇA – Acórdão do Supremo Tribunal de Justiça de 11-03-1997, processo número 96A901, Relator: Fernando Fabião, disponível em: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/a893c17476226d7a802568fc003b4c0d?OpenDocument.

SUPREMO TRIBUNAL DE JUSTIÇA – Acórdão do Supremo Tribunal de Justiça, de 03-03-2010, processo número 886/07.8PSLSB.L1.S1, Relator: Santos Cabral, Disponível em: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25061d49157a048c8025770a002ed7d7?OpenDocument.

SUPREMO TRIBUNAL DE JUSTIÇA – Acórdão do Supremo Tribunal de Justiça, de 28-09-2011, processo número :22/09.6YGLSB.S2, Relator: Santos Cabral, disponível em: https://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25cd7aa80cc3adb0802579260032dd4a?OpenDocument.

TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional de 28-06-2024, número 606/2024, processo 440/2024. Relator: Conselheiro José António Teles Pereira Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20240506.html.

TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional de 2-03-2007, número 155/2007, processo número 695/06. Relator: Conselheiro Gil Galvão, disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20070155.html.

TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional de 4-05-1999, número 254/99, processo número 456/97, Relator: conselheiro Sousa e Brito, disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/19990254.html.

TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional de 31-05-2017, Acórdãos 99.º volume, acórdão nº 260/17, processo número 527/13, Relator: Conselheiro Fernando Vaz Ventura, disponível em: https://www.tribunalconstitucional.pt/tc/content/reserved/ebook_html5/tc_acordaos_0099/230/.

TRIBUNAL CONSTITUCIONAL – Acórdão do Tribunal Constitucional de 11-05-2023, número 240/2023, processo 175/2022, Relatora: Conselheira Mariana Canotilho, disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20230240.html.

COIMBRA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Coimbra de 10-11-2010, processo 209/09.1PBFIG.C1, Relator: Paulo Guerra, disponível em: https://www.dgsi.pt/jtrc.nsf/-/8FA09BD5C06877AA802577EE0041E7F1

ÉVORA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Évora de 24-09-2024, processo 2/23.9GCPSR.E1, Relator: Edgar Valente, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/31e50b61c5f2e84480258baf002a954d?OpenDocument.

ÉVORA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Évora de 10.04.2018, processo número 29/12.6GDSTC.E2, Relator: Gilberto Cunha, disponível em: https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/70c8accba0741c528025827b0050c5a3?OpenDocument.

ÉVORA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Évora de 29-05-2012, processo número 253/07.3 JASTB.E1, Relator: Martinho Cardoso, disponível em:https://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/341f5e5d5b6f39f580257de10056f84c

LISBOA, TRIBUNAL DA RELAÇÃO - Acórdão do Tribunal da Relação de Lisboa, de 16-02-2016, processo 176/06.3TNLSB.L2-1, Relator: Rijo Ferreira, disponível em: https://diariodarepublica.pt/dr/detalhe/acordao/1-2016-99338175.

LISBOA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Lisboa de 14-09-2021, processo número 8777/21.3T8LSB.L1-7, Relator: Luís Filipe Pires de Sousa, disponível em: https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0e71bdbb89eaa24a8025876000400276.

LISBOA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Lisboa de 14-03-2018, processo 483/15.4IDLSB.L1-3, Relator: João Lee Ferreira, disponível em: https://www.dgsi.pt/jtrl.nsf/-/4F697801A7E4B393802582CC0050ACCF.

LISBOA, TRIBUNAL DA RELAÇÃO – Acórdão do Tribunal da Relação de Lisboa de 28-09-2017, processo 433/15.8PBSNT.L1-9, Relatora: Filipa Costa Lourenço, disponível em: https://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/b01d41186c611ba4802581aa007442c4.

PORTO, TRIBUNAL DA RELAÇÃO - Acórdão do Tribunal da Relação do Porto de 08-05-2023, processo 7251/22.5T8PRT.P1, Relatora: Fernanda Almeida, disponível em:https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/8c246bf5f321c363802589d4002ff5da?OpenDocument.

WEBGRAFIA:

Australian Government: Office of the Australian Information Commissioner (2024) - *Facial recognition technology: a guide to assessing the privacy risks*. Consultado a 28.01.2025, disponível em: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks

BARROS, Gabriel Osório de (2024) - *Regulamentação da Inteligência Artificial na União Europeia: Uma análise do AI Act*. Gabinete de Estratégia e Estudos do Ministério da Economia. Consultado a 21.11.2024, pp.4-5, disponível em: https://www.gee.gov.pt/pt/?option=com_fileman&view=file&routed=1&name=GEE_Em%20An%C3%A1lise_Regulamento%20da%20Intelig%C3%AAncia%20Artificial.pdf&folder=estudos-e-seminarios%2Fartigos&container=fileman-files.

BERIDZE, Irakli; BUTTERFIELD, Kay Firth; BIK, Marjolein Smit-Arnold; GOUT, Cyril (2022) - *A Policy Framework for Responsible Limits on Facial Recognition: Use Case: Law Enforcement Investigations*. World Economic Forum. Consultado entre 20.10.2024 e 21.10.2024, pp. 7-13, disponível em: https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf.

Biometrics Institute (2025) - *Physiological and Behavioural Biometrics*. Consultado a 3.10.2024, disponível em: https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/.

Biometrics Institute (2025) - *Types of Biometrics* – Eye: Iris. Consultado a 12.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-eyes-iris/.

Biometrics Institute (2025) - *Types of Biometrics – Eye: Retina*. Consultado a 14.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-eye-retina/.

Biometrics Institute (2025) – *Types of Biometrics – Fingerprint.* Consultado a 9.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-fingerprint/.

Biometrics Institute (2025) - *Types of biometrics – Gait*. Consultado a 4.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-gait/.

Biometrics Institute (2025) – *Types of Biometrics: Hand Geometry*. Consultado a 7.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-hand-geometry/.

Biometrics Institute (2025) - *Types of Biometrics – Voice*. Consultado a 8.10.2024, disponível em: https://www.biometricsinstitute.org/types-of-biometrics-voice/

Comissão Europeia: Direção-Geral de Redes de Comunicações, Conteúdos e Tecnologia (2019) - *Orientações éticas para uma IA de confiança* . Escritório de

Publicações. Consultado a 21.11.2024, pp.17-25, disponível em: **https://data.europa.eu/doi/10.2759/2686**.

Conselho da União Europeia (2025) - *A IA em síntese: utilização e impacto.* Consultado a 23.10.2024, disponível em: https://www.consilium.europa.eu/pt/policies/ai-explained/.

CURRAO, Elettra (2021) - *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio? Facial recognition and fundamental rights: setting the balance*. Diritto Penale e Uomo (DPU): Criminal Law and Human Condition. Consultado entre 14.11.2024 a 22.11.2024, pp. 11-13, disponível em: https://dirittopenaleuomo.org/wp-content/uploads/2021/05/Currao_DPU.pdf.

Council of Europe (2021) - *Guidelines on facial recognition: Convention 108*. Consultado entre 13.01.2025 a 24.01.2025, pp. 8-27, disponível em: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751

DUSHI, Desara (2020) - *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*. Global Campus, South East Europe. Consultado a 21.01.2025, pp. 6-10, disponível em: https://repository.gchumanrights.org/server/api/core/bitstreams/51d86ab3-1cb5-45f6-b141-64c06dcef5d8/content.

Edpb: European Data Protection Board (2023) - *Linee guida 05/2022 sull´uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto*. Consultado entre 13.10.2024 a 15.11.2024 e 12.022025, pp. 5-47, disponível em: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_it.pdf

FRA – European Union Agency For Fundamental Rights (2019) - *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. Consultado entre 17.10.2024 a 22.11.2024, pp. 9-30, disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

GARVIE, Clare (2022) - *A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations*. Center on Privacy & Technology at Georgetown Law. Consultado a 30.10.2024, pp.5-6, disponível em: https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf.

GONZÁLEZ; José A.R. Lorenzo (2022) - *Reconhecimento Facial (FRT) e direito à imagem*. Revista da Faculdade de Direito da Universidade de Lisboa. Vol. LXIII nºs 1 e 2. Consultado a 18.11.2024, pp.581-585, disponível em: https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Jose%CC%81-A.-R.-Lorenzo-Gonza%CC%81lez.pdf

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee (2019) - *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. National Institute of Standards and

Technology. Consultado entre 25.11.2024 a 13.01.2025, disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial (2018) – *Uma Definição de IA: Principais Capacidades e Disciplinas Científicas.* Consultado entre 24.10.2024 e 25.10.2024, pp. 1-3, disponível em: https://lms.nau.edu.pt/assets/courseware/v1/3e0b4d98484f187196e18fb8e2d7e6bf/asset-v1:DGE+IAESC+2020_T4+type@asset+block/ADEFINITIONOFAI-PTpdf.pdf.

HILL, Dallas; O'CONNOR, Christopher D; SLANE, Andrea (2022) - *Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making* in International Journal of Police Science & Management. Vol. 24(3). Consultado a 31.10.2024, pp.325-335, disponível em: https://journals.sagepub.com/doi/pdf/10.1177/14613557221089558.

IEEE: Public Safety Technology (2025) - *Ethical Considerations in the Use of Facial Recognition for Public Safety.* Consultado a 03.02.2025, disponível em: https://publicsafety.ieee.org/topics/ethical-considerations-in-the-use-of-facial-recognition-for-public-safety.

Information Commissioner's Office (2021) - *The use of live facial recognition technology in public places*. Consultado a 10.02.2025, pp. 36-39, disponível em: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf.

Innocence Project (2024) – *Eyewitness Misidentification*. Consultado a 19.09.2024, disponível em: https://innocenceproject.org/eyewitness-misidentification/

JAIN, Anil K.; ROSS, Arun; PRABHAKAR, Salil (2004) - *An Introduction to Biometric Recognition.* IEEE transacions on circuits and systems for video technology, Vol. 14, No. 1. Consultado entre 4.10.2024 a 8.10.2024, pp. 9-18, disponível em: https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf.

JR., Perritt Henry H. (2020) - *Defending Face-Recognition Technology (And Defending Against It)*. Vol. 25 : Iss. 1 , Article 2, journal of Technology law & police. Consultado entre 21.10.2024 a 22.10.2024, pp. 46-51, disponível em: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1003&context=jtlp.

LEE, Jyh-Na; ZHOU, Peng (2024) - *FRT Regulation in China*. Cambridge University Press. Consultado a 4.11.2024, pp.242-243, disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D0FA408D7A063C4E97E52558D90D03D0/9781009321198c18_242-252.pdf/frt-regulation-in-china.pdf.

LEWIS, James A.; CRUMPLER, William (2021) - *Facial Recognition Technology Responsible Use Principles and the Legislative Landscape*. Center for Strategic and International Studies. Consultado entre 14.01.2025 a 29.01.2025, pp. 2-15, disponível em: https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

LOFTUS, Elizabeth F.; PALMER, John C (1974) - *Reconstruction of Automobile Destruction: An Example of the Interaction Between Language and Memory.* Journal of Verbal Learning and Verbal Behavior 13. Consultado a 30.09.2024, pp. 585-189, disponível em: https://www.demenzemedicinagenerale.net/images/mens-sana/AutomobileDestruction.pdf

LYNCH, Nessa (2024) - *Facial Recognition Technology in Policing and Security - Case Studies in* Regulation*,* Laws 13, 35. Consultado entre 5.11.2024 a 6.11.2024, pp. 3-4, disponível em: file:///Users/sofiaramos/Downloads/laws-13-00035%20(6).pdf.

MAGALHÃES, Paulo Sérgio; SANTOS, Henrique Dinis (2003) - *Biometria e Autenticação.* Atas da 4ª Conferência da Associação Portuguesa de Sistemas de Informação" (edição em CD-ROM), Porto. Consultado a 12.09.2024, p.8, disponível em: https://core.ac.uk/reader/55603020.

MOBILIO, Giuseppe (2021) - *Tecnologie Di Riconoscimento Facciale. Rischi per i diritti dondamentali e sfide regolativa*, Editoriale Scientifica s.r.l. Consultado entre 12.10.2024 a 17.10.2024 e 11.02.2025, pp. 11-38, disponível em: https://flore.unifi.it/retrieve/e398c381-3a8a-179a-e053-3705fe0a4cff/Mobilio%2c%20Tecnologie%20di%20riconoscimento%20facciale%2c%202021.pdf.

MURRAY, Daragh (2024) - *Netherlands Quarterly of Human Rights: Facial recognition and the end of human rights as we know them?* Volume 42, Issue 2. SageJournals. Consultado a 22.11.2024, pp. 150-152, disponível em: https://journals.sagepub.com/doi/epub/10.1177/09240519241253061.

National Research Council (US) Whither Biometrics Committee (2010) - *Biometric Recognition: Challengs and opportunities*. National Library of Medicine: National Center for Biotechnology Information. Pato JN, Millett LI, editors. Consultado a 07.10.2024, disponível em: https://www.ncbi.nlm.nih.gov/books/NBK219892/.

Parlamento Europeu (2023) - *O que é a inteligência artificial e como funciona*? Consultado a 23.10.2024, pp. 1-7, disponível em: https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804/20200827STO85804_pt.pdf

PEREIRA, Diana Silva; ALVES, Catarina Paulino; FERREIRA, Teresa (2017)- *O direito à imagem: Toda a imagem tem o seu preço.* Carlos Pinto de Abreu e Associados. Consultado a 18.11.2024, p.2, disponível em: https://carlospintodeabreu.com/public/files/35_societario_direito_imagem.pdf.

PIKE, Graham (2019) - *Visual, identification: Unconscious transference.* Forensic psychology: Week 6: 1.4. OpenLearn - Open University. Consultado a 30.09.2024, disponível em: https://www.open.edu/openlearn/mod/oucontent/view.php?id=68097&section=1.4.

PINTO, Amâncio da Costa (1986) - *Uma análise experimental sobre a credibilidade das identificações efectuadas por testemunhas ocultares*. Revista de Investigação Criminal,

vol. 21. Consultado a 21.09.2024, pp. 67-72, disponível em: https://www.fpce.up.pt/docentes/acpinto/artigos/01_testemunho_ocular.pdf.

PRAIA, João de Matos-Cruz (2019) – *Proibições de prova em processo penal: algumas particularidades no âmbito da prova por reconhecimento e da reconstituição do facto.* Revista Julgar online. Consultado a 09.12.2024, p.4, disponível em: https://julgar.pt/wp-content/uploads/2019/12/20191209-ARTIGO-JULGAR-Proibi%C3%A7%C3%B5es-de-prova-em-processo-penal-Jo%C3%A3o-Praia.pdf.

SACCHETTO, Ernestina (2020) – *Face To Face: Il Complesso Rapporto Tra Automated Facial Recognition Tecnhnology e Processo Penale*. Consultado a 6.11.2024, pp. 1-3, disponível em: https://iris.unito.it/retrieve/handle/2318/1758754/668686/Sacchetto-finale.pdf.

SACCHETTO, Ernestina (2019) - Spunti per una riflessione sul rapporto fra biometria e processo penale: ideas para reflexionar sobre la relación entre biometría y proceso penal. Revista Trimestral De Derecho Penal. Consultado entre 4.10.2024 a 14.10.2024, pp. 467-472, disponível em: https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_sacchetto.pdf

SILVA, Sandra Oliveira e (2011) - *Legalidade da Prova e Provas Proibidas*. Revista Portuguesa de Ciência Criminal. Ano 21, n.º 4. Consultado entre 09.12.2024 a 11.12.2024, pp. 545-591, disponível em: https://repositorio-aberto.up.pt/bitstream/10216/133333/2/49978.pdf

SMITH, Marcus; MANN, Monique (2024) - *The Cambridge Handbook of Facial Recognition in the Modern State: Facial Recognition Technology and Potential for Bias and Discrimination*. Cambridge University Press. Consultado entre 14.11.2024 e 13.01.2025, pp. 89-91, disponível em: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B1C4A7F38AE00781EC8A559EFE48B3DF/9781009321198c7_87-95.pdf/facial-recognition-technology-and-potential-for-bias-and-discrimination.pdf.

STANFORD, Alyxaundria (2024) - *Artificial Intelligence Is Putting Innocent Peaple at Risk of Being Incarcerated*. Innocence Project. Consultado a 14.11.2024, disponível em: https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/.

SWARNS, Christina (2023) - *When Artificial Intelligence Gets It Wrong*. Innocence Project. Consultado a 25.11.2024, disponível em: https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/.

U.S: Commission on Civil Rights (2024) - *The Civil Rights Implications of the Federal Use of Facial Recognition Tecnology*. Consultado a 30.10.2024 e 21.11.2024, pp. 4-29, disponível em: https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

VINAGRE, João; MONIZ, Nuno (2020) – *Inteligência Artificial: Riscos e promessas*. Revista de Ciência Elementar, V8 (04):052. Consultado a 24.10.2024, pp. 2-4, disponível em: https://rce.casadasciencias.org/rceapp/pdf/2020/052/.