

Universidades Lusíada

Merkens, Melissa Stefanie Costa Cidade de
Carvalho, 1990-

Intimidade, imagem e reconhecimento facial

<http://hdl.handle.net/11067/7424>

Metadados

Data de Publicação

2023

Resumo

As tecnologias de informação vieram revolucionar as sociedades modernas. Esta revolução provocada pela utilização massiva dos computadores e da Internet alterou o modo e também o ritmo do processamento de informações, refletindo-se consequentemente na redefinição da própria sociedade de consumo. Na verdade, as informações passaram a ser partilhadas a uma velocidade veloz pondo em perigo o direito à privacidade. Desta forma, passou-se a viver num mundo virtual, sem fronteiras, onde tudo passa a e...

Information technologies have come to revolutionize modern societies. This revolution, brought about by the massive use of computers and the Internet, has not only changed the way information is processed but also its pace, consequently leading to the redefinition of consumer society. In fact, information is now shared at a rapid pace, endangering the right to privacy. As a result, we find ourselves living in a borderless virtual world where everything is easily accessible with just a small ges...

Palavras Chave

Direito à Privacidade, Proteção de dados - Direito e legislação, Retratos - Direito e legislação, Identificação biométrica - Direito e legislação

Tipo

masterThesis

Revisão de Pares

Não

Coleções

[ULL-FD] Dissertações

Esta página foi gerada automaticamente em 2026-10-29T22:12:22Z com
informação proveniente do Repositório



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

Intimidade, imagem e reconhecimento facial

Realizado por:

Melissa Stefanie Costa Cidade de Carvalho Merkens

Orientado por:

Prof. Doutor José Alberto Rodríguez Lorenzo González

Constituição do Júri:

Presidente:	Prof. Doutor José Artur Anes Duarte Nogueira
Orientador:	Prof. Doutor José Alberto Rodríguez Lorenzo González
Arguente:	Prof. Doutor Luís Manuel Barbosa Rodrigues

Dissertação aprovada em: 28 de fevereiro de 2024

Dissertação reformulada

Lisboa

2023



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Direito

Intimidade, imagem e reconhecimento facial

Melissa Stefanie Costa Cidade de Carvalho Merkens

Dissertação reformulada

Lisboa

Dezembro 2023



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Direito

Intimidade, imagem e reconhecimento facial

Melissa Stefanie Costa Cidade de Carvalho Merkens

Dissertação reformulada

Lisboa

Dezembro 2023

Melissa Stefanie Costa Cidade de Carvalho Merkens

Intimidade, imagem e reconhecimento facial

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

Área científica: Ciências Jurídico-Civilísticas

Orientador: Prof. Doutor José Alberto Rodriguez Lorenzo
Gonzalez

Dissertação reformulada

Lisboa

Dezembro 2023

FICHA TÉCNICA

Autora Melissa Stefanie Costa Cidade de Carvalho Merkens
Orientador Prof. Doutor José Alberto Rodriguez Lorenzo Gonzalez
Título Intimidade, imagem e reconhecimento facial
Local Lisboa
Ano 2023

MEDIATECA DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

MERKENS, Melissa Stefanie Costa Cidade de Carvalho, 1990-

Intimidade, imagem e reconhecimento facial / Melissa Stefanie Costa Cidade de Carvalho Merkens ; orientado por José Alberto Rodriguez Lorenzo Gonzalez. - Lisboa : [s.n.], 2023. - Dissertação de Mestrado em Direito, Faculdade de Direito da Universidade Lusíada.

I - GONZÁLEZ, José A.R.L., 1965-

LCSH

1. Direito à privacidade
2. Proteção de dados - Direito e legislação
3. Retratos - Direito e legislação
4. Identificação biométrica - Direito e legislação
5. Universidade Lusíada. Faculdade de Direito - Teses
6. Teses - Portugal - Lisboa

1. Privacy, right of
2. Data protection - Law and legislation
3. Portraits - Law and legislation
4. Biometric identification - Law and legislation
5. Universidade Lusíada. Faculdade de Direito - Dissertations
6. Dissertations, academic - Portugal - Lisbon

LCC

1. K3264.C65 M47 2023

“Suprimir os obstáculos não é dar liberdade,
mas sim permitir o desregramento, que
conduz à desestruturação, à monotonia, ao
nada”.

Pablo Picasso

APRESENTAÇÃO

Intimidade, imagem e reconhecimento facial

Melissa Stefanie Costa Cidade de Carvalho Merkens

As tecnologias de informação vieram revolucionar a sociedade, alterando a forma e o ritmo do processamento de informações e, conseqüentemente, a massiva utilização das comunicações à distância mudou a sociedade de consumo, com a partilha de informações em tempo real.

Porém, se esta verdadeira revolução trouxe inúmeras vantagens, também veio trazer novos perigos, designadamente no que respeita aos direitos fundamentais, criando novos mecanismos por via dos quais os mesmos podem ser violados, desde logo, colocando em risco o direito à privacidade.

É que, se é verdade que o mundo virtual sem fronteiras facilita tarefas do quotidiano, mas também traz desafios, especialmente na proteção de dados e privacidade.

Assim, a adaptação do Direito a essa realidade é crucial para se conseguir enfrentar desafios como a obtenção, armazenamento e uso dos dados pessoais e questões como consentimento informado, finalidade e limitação do uso dos dados, segurança da informação e direito ao esquecimento têm de ser alvo de regulamentação clara e, inerentemente, é necessário prever responsabilidades claras para empresas, fornecedores de serviços online e utilizadores, com a aplicação do instituto da responsabilidade civil e até mesmo criminal em caso de flagrantes violações de privacidade.

Neste enquadramento, o uso de dados biométricos, especialmente imagens faciais, levanta preocupações éticas, dado o risco de poder ser usado de forma discriminatória.

Palavras-chave: Reconhecimento Facial; Privacidade; Anonimato; Direito à Imagem; RGPD.

PRESENTATION

Intimacy, Image, and Facial Recognition

Melissa Stefanie Costa Cidade de Carvalho Merkens

Information technologies have revolutionized society, changing the way and pace of information processing and, consequently, the massive use of remote communications has changed the consumer society, with the sharing of information in real time.

However, if this true revolution has brought numerous advantages, it has also brought nine dangers, particularly regarding fundamental rights, creating new mechanisms through which they can be violated, thereby putting the right to privacy at risk.

It is true that the virtual world without borders facilitates everyday tasks, but it also brings challenges, especially in data protection and privacy.

Thus, the adaptation of the Law to this reality is crucial to be able to face challenges such as the collection, storage and use of personal data and issues such as informed consent, purpose and limitation of data use, information security and the right to be forgotten have to be clearly regulated and, inherently, it is necessary to provide clear responsibilities for companies, online service providers and users, with the application of the institute of civil and even criminal liability in case of flagrant violations of privacy.

In this context, the use of biometric data, especially facial images, raises ethical concerns, given the risk that it could be used in a discriminatory manner.

Keywords: Facial Recognition; Privacy; Anonymity; Right to Image; RGPD.

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

al.	-	Alínea
art.º	-	Artigo
CDFUE	-	Carta dos Direitos Fundamentais da União Europeia
CEDH	-	Convenção Europeia dos Direitos do Homem
cfr.	-	Confrontar
cit.	-	Citado
CNPD	-	Centro Nacional de Proteção de Dados
CRP	-	Constituição da República Portuguesa
disp.	-	Disponível em
ed.	-	Edição
ex.	-	Exemplo
FRT	-	Fontes de Reconhecimento Técnico
GNS	-	Gabinete Nacional de Segurança
IA	-	Inteligência Artificial
id.	-	Idem
n.º	-	Número
p.	-	Página
pp.	-	Páginas
RF	-	Reconhecimento Facial
RGPD	-	Regulamento Geral de Proteção de Dados
ss.	-	Seguintes
TC	-	Tribunal Constitucional
TEDH	-	Tribunal Europeu dos Direitos do Homem
v.	-	<i>Vide</i>
vol.	-	Volume

SUMÁRIO

Introdução	15
1. Enquadramento da questão.....	19
1.1. Direitos Fundamentais	21
1.2. Principais Direitos Fundamentais.....	23
1.3. Direito à Reserva da Intimidade da Vida Privada	26
1.4. Direito à imagem.....	27
1.4.1. O conceito de imagem	27
1.4.2. O consentimento da pessoa retratada.....	28
1.5. Distinção dos Direitos Fundamentais face aos Direitos de Personalidade....	34
Capítulo I- A Privacidade no Ordenamento Jurídico Português e Evolução da Proteção de Dados	37
2. Legislação Aplicável	37
2.1. A Evolução da Legislação em Portugal e no Mundo	37
2.2. Regulamento Geral de Proteção dos Dados	40
2.3. Princípios previstos no RGPD.....	42
3. O Direito à privacidade e à proteção da vida privada	47
3.1. Desafios atuais à privacidade dos cidadãos.....	47
3.2. Ameaças atuais a este direito	49
3.3. A tecnologia como ameaça à vida privada	52
3.4. Implementação de medidas minimizadoras.....	53
4. O Anonimato na Sociedade Digital	55
4.1. Consequências do anonimato na Internet.....	55
4.2. Os benefícios do anonimato na Internet.....	55
4.3. O anonimato na Internet em Portugal e no Mundo	56
4.4. Jurisprudência Internacional – O Anonimato na Internet.....	57
Capítulo II – A Revolução na Intimidade, no Direito à Imagem e no Reconhecimento Facial.....	61
5. A Tecnologia do Reconhecimento Facial.....	61
5.1. Capacidades técnicas envolvidas	61
5.2. Como funciona o procedimento.....	62
5.3. Como é realizada a captação de imagem pessoal	68
5.4. A constituição de uma base de dados e a regulamentação da inteligência artificial	69
5.5. Impacto da utilização de sistemas biométricos de identificação e tecnologias de reconhecimento facial	71

5.6. Vantagens do sistema.....	73
5.7. Aspectos diferenciadores e fragilidades.....	75
5.8. Ponderação de interesses.....	77
5.9. A estratégia da União Europeia para a Inteligência Artificial e para os Sistemas de Identificação Biométrica.....	81
Conclusão	85
Referências	89
Sítios da internet consultados.....	95
Jurisprudência consultada	99
Jurisprudência nacional	99
Jurisprudência internacional	99

INTRODUÇÃO

Num mundo cada vez mais complexo e em constante evolução, os direitos fundamentais emergem como a bússola moral que guia a humanidade através das encruzilhadas éticas.

Em Portugal, esta tradição de pensamento remonta a figuras como S. TOMÁS DE AQUINO ou IMMANUEL KANT, cuja filosofia política e moral ainda ressoa nos alicerces da nossa sociedade.

Por um lado, TOMÁS DE AQUINO, com a sua síntese magistral de razão e fé, delineou uma visão onde a dignidade humana se encontra intrinsecamente ligada à realização dos direitos fundamentais. Estes direitos, ancorados na natureza humana e na ordem divina, transcendem as vicissitudes temporais, erguendo-se como pilares inabaláveis da justiça¹ e, por outro lado, KANT desenvolveu uma teoria ética baseada na noção de dever e na universalidade das normas morais, enfatizando, no contexto dos direitos fundamentais, a importância da dignidade humana, dado que, para ele, os seres humanos têm um valor intrínseco e devem ser tratados como fins em si mesmos, nunca apenas como meios para atingir outros objetivos².

Ora, ambas as perspetivas fundamentam a ideia de que cada indivíduo possui direitos inalienáveis à sua existência, como a liberdade e a igualdade, os quais devem ser respeitados independentemente das circunstâncias.

Assim, a importância dos direitos fundamentais desdobra-se numa salvaguarda contra a tirania e a arbitrariedade.

Em Portugal, o entendimento de que cada pessoa possui inalienáveis direitos à vida, liberdade e propriedade encontra-se entrelaçada com a construção da identidade nacional, entendendo-se que estes direitos não são concessões benevolentes do poder político-legislativo, mas sim uma expressão direta da dignidade intrínseca que todos os seres humanos possuem.

Na era digital que vivemos, onde as fronteiras entre o público e o privado se diluem, a defesa dos direitos fundamentais ganha uma importância renovada, sendo essencial não esquecer a importância da liberdade e da justiça na organização da sociedade em

¹ Cfr.. AERTSEN, Jan (2012) – *A Medieval Philosophy as Transcendental Thought*. From Philip the Chancellor (ca. 1225) to Francisco Suárez, Leiden/ Boston, Brill, pp. 209 a 271.

² Cfr. SALGADO, Joaquim Carlos (2012) – *A ideia de justiça em Kant: seu fundamento na liberdade e na igualdade*. 3.ª Edição, Belo Horizonte, Del Rey.

que a liberdade de expressão, a privacidade e a igualdade perante a lei se tornam faróis que iluminam o caminho para uma comunidade justa e equitativa.

Ora, neste enquadramento, o reconhecimento facial emergiu como uma tecnologia promissora e de ampla aplicação no cenário contemporâneo. As suas capacidades de identificação e autenticação com base em características faciais têm revolucionado diversos setores, desde a segurança até o comércio. No entanto, essa tecnologia também levanta questões pertinentes em relação à privacidade e ao direito à imagem, bem como ao direito à intimidade no mundo cada vez mais digitalizado³.

A capacidade do reconhecimento facial de identificar indivíduos de forma automatizada e em tempo real suscita preocupações sobre o controlo e a utilização dos dados biométricos capturados.

Neste sentido, a coleta, armazenamento e compartilhamento de informações faciais levantam questões éticas e legais sobre a proteção dos direitos fundamentais dos cidadãos num contexto de constante vigilância tecnológica⁴.

Ora, no presente estudo, exploraremos as implicações do reconhecimento facial para a privacidade e para o direito à imagem dos indivíduos, investigaremos como essa tecnologia pode afetar o controlo que as pessoas têm sobre as suas informações pessoais, a preservação da sua identidade e o respeito à sua intimidade num ambiente cada vez mais conectado. Analisaremos a legislação e regulamentações existentes relacionadas ao uso do reconhecimento facial e como essas medidas buscam equilibrar a inovação tecnológica com a proteção dos direitos individuais e, além disso, examinaremos os desafios enfrentados pelas autoridades e pela sociedade em relação à implementação ética e justa do reconhecimento facial, evitando possíveis discriminações e concretas violações de privacidade.

Com vista conseguir um entendimento o mais aprofundado possíveis do tema, entendemos pertinente dividir o presente estudo em diversos capítulos.

Assim, primeiramente procuraremos explorar a intricada relação entre direitos fundamentais e direitos de personalidade, procurando-se delinear uma visão abrangente, destacando elementos distintos, como o direito à reserva da intimidade da

³ Cfr. <https://www.thalesgroup.com/pt-pt/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition>.

⁴ Cfr. <https://www.electronicid.eu/pt/blog/post/como-funciona-o-reconhecimento-facial-e-a-sua-seguranca/pt>.

vida privada, o direito à palavra e o direito à imagem, desdobrando este último em conceitos como o conceito de imagem e consentimento da pessoa retratada.

Seguidamente, mergulharemos na esfera jurídica portuguesa, analisando a evolução da proteção de dados, abordando a evolução da legislação em Portugal e no mundo até às nuances trazidas pelo Regulamento Geral de Proteção de Dados e os princípios implicitamente entrelaçados neste enquadramento legal. Neste âmbito, o direito à privacidade e à proteção da vida privada será um ponto fulcral, onde exploraremos os desafios contemporâneos que confrontam a privacidade dos cidadãos e abordaremos como a tecnologia, apesar dos seus avanços, se apresenta como uma ameaça à vida privada, motivo pelo qual discutiremos a implementação de medidas minimizadoras para salvaguardar estes direitos fundamentais.

Adentrando o mundo da sociedade digital, investigaremos ainda o anonimato, os seus benefícios na internet e como esta questão é abordada em Portugal e no mundo, inclusive com referência à jurisprudência internacional.

Por último, focaremos no reconhecimento facial, explorando a estratégia da União Europeia para a inteligência artificial e os sistemas de identificação biométrica, analisaremos os prós e contras do reconhecimento facial, bem como a captação de imagem pessoal para este fim, destacando os desafios éticos e legais que esta tecnologia enfrenta.

Desta forma, esperamos contribuir para o debate sobre o uso responsável do reconhecimento facial, promovendo uma reflexão crítica sobre como essa tecnologia pode ser adequadamente regulamentada para salvaguardar os valores essenciais da privacidade, da imagem e da intimidade dos indivíduos num mundo cada vez mais tecnológico e interconectado.

1. ENQUADRAMENTO DA QUESTÃO

Conforme nos refere LUDWIG WITTGENSTEIN, a noção de dignidade da pessoa humana é constantemente referida em textos legais, discursos jurídicos e constitucionais. No entanto, apesar de onnipresente, a complexidade do tema torna-o uma “terra incógnita”, suscitando desafios significativos para a investigação científica, dado que, a sua aplicabilidade abrange tanto o domínio jurídico como o ético e filosófico, contribuindo para uma diversidade de abordagens, sentidos e contextos⁵.

E, de acordo com INGO SARLET, apesar de a dignidade da pessoa humana ser percebida de forma intuitiva, mantém-se como um conceito vago e impreciso, caracterizado pela sua ambiguidade e polissemia, motivo pelo qual, apesar dos esforços da Filosofia do Direito, o seu significado ontológico permanece um dos mais indeterminados na ordem jurídica⁶. Na mesma linha interpretativa, MICHEL RENAUD, afirmam que, “não obstante todos tenhamos uma compreensão espontânea e implícita da dignidade da pessoa humana, ainda assim, em sendo o caso de explicar no que consiste esta dignidade, teríamos grandes dificuldades”⁷.

Sem prejuízo de todo o exposto, com vista a esclarecer o conceito em apreço, STEVEN LUKES afirma que a dignidade da pessoa humana pode ser entendida como “o axioma moral (ou religioso) que reconhece o valor supremo e intrínseco do indivíduo”⁸.

E, por seu turno, partindo da premissa de não coisificação, JORGE REIS NOVAIS afirma que ao “indivíduo (..), primacialmente, a configuração e densificação do conteúdo preciso de sua dignidade”, significando isto que a dignidade é algo inerente ao Ser Humano e que, o mesmo, dentro do seu livre arbítrio deve ter o poder de escolher o seu espaço de dignidade pessoal, sendo o mesmo dotado de liberdade para fixar e atingir as suas metas pessoais, independentemente de qualquer julgamento moral ou social.

Neste enquadramento, apreciado o conceito de dignidade da pessoa humana sob um ponto de vista liberal, JOHN STUART MILL afirma que o uso do poder com forma de

⁵ Cfr. WITTGENSTEIN, Ludwig (2001) – *Philosophical investigations*. 3. ed. Oxford: Blackwell, 2001, §11.

⁶ Cfr. SARLET, Ingo (2008) – *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 6. ed. Porto Alegre: Livraria do Advogado, 2008, pp. 41-42.

⁷ Cfr. RENAUD, Michel (1999) – *A dignidade do ser humano como fundamentação ética dos direitos do homem*. Brotéria. Cultura e Informação. - Vol. 148, nº. 2 (Fev. 1999), pp. 135 a 154.

⁸ Cfr. LUKES, Steven (2006) – *Individualism*, Colchester: University of Essex/ ECPR, p. 54.

restrição da liberdade individual apenas se justifica como forma de evitar prejudicar terceiros⁹.

Assim, o referido autor defende que uma pessoa não pode ser legitimamente obrigada a agir de determinada maneira ou abster-se de algo apenas porque tal seria abstratamente benéfico para ela, a tornaria mais feliz ou seria considerado sábio ou correto pelos outros¹⁰.

Ponderando os diversos aspetos em apreço, cumpre referir a magistral posição de SAMUEL PUFENDORF, o qual entende que é dever de todo ser humano promover e preservar a convivência social, sendo, para isso, essencial respeitar a igualdade e dignidade de cada indivíduo, evitando causar danos ao próximo. A base da sociedade, segundo PUFENDORF, deve ser o reconhecimento mútuo da igual dignidade de todos, promovendo a harmonia através da prevenção de ações destrutivas, comportamentos negativos e incentivando a benevolência¹¹.

Partindo de um conceito meramente teórico-filosófico, verificamos que, ao longo do tempo, se deu uma incorporação de princípios inerentes à dignidade da pessoa humana no domínio constitucional.

Este movimento teve origem principalmente na Carta das Nações Unidas de 1945¹² e na Declaração Universal dos Direitos Humanos, adotada pela Organização das Nações Unidas a partir de 1948¹³, documentos que introduziram a consagração normativa da dignidade da pessoa humana no âmbito do direito internacional e, a partir desse reconhecimento jurídico internacional, muitas das democracias ocidentais passaram a incluir constitucionalmente a dignidade da pessoa humana como um princípio fundamental de todo o ordenamento jurídico e um elemento de coesão axiológica da Constituição.

Ora, associado ao conceito jurídico-filosófico de dignidade da pessoa humana, neste enquadramento normativo de proteção do cidadão emergem os direitos fundamentais

⁹ Cfr. MILL, John Stuart (1991) – *Sobre a Liberdade*. 2. ed. Clássicos do Pensamento Político; v. 22. Petrópolis, RJ: Vozes, p. 53.

¹⁰ *Id.*

¹¹ Cfr. PUFENDORF, Samuel – *De jure naturae et gentium (Liber primus – Liber quartus)* apud SAHD, Luiz F. N. de A. e Silva. O contrato social em Samuel Pufendorf. Revista Aurora de Filosofia. Curitiba, v. 21, n. 28, jan./jun. 2009, p. 143-163.

¹² Cfr. <https://unric.org/pt/wp-content/uploads/sites/9/2009/10/Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf>.

¹³ Cfr. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf.

e os direitos de personalidade consagrados internamente na ordem jurídica dos Estados.

1.1. DIREITOS FUNDAMENTAIS

Os direitos fundamentais são os alicerces que sustentam a edificação da sociedade, conferindo-lhe solidez e justiça e estão intrinsecamente ligados ao conceito profundo de dignidade da pessoa humana.

A dignidade humana, como princípio basilar, permeia todas as facetas dos direitos fundamentais, guiando a sua interpretação e aplicação.

Em concreto, podemos referir que a dignidade da pessoa humana se revela como a essência que ilumina o caminho dos direitos fundamentais, não sendo apenas um conceito abstrato, mas sim uma força impulsionadora que molda as leis e as práticas sociais.

E, conforme nos salienta GOMES CANOTILHO, os direitos fundamentais, por sua vez, são as manifestações concretas desse respeito pela dignidade, garantindo que cada indivíduo seja tratado com justiça, igualdade e liberdade¹⁴.

Ora, a compreensão dos direitos fundamentais como uma ordem objetiva que reflete valores e metas estabelecidos democraticamente na comunidade indica que o sistema de direitos fundamentais está enraizado em um contexto económico e político-ideológico do Estado, pelo que, além da relação destacada entre a dignidade da pessoa humana e o poder estatal, observa-se que não apenas o sistema de direitos fundamentais impacta o Estado, através da subjetivação dos direitos individuais, mas o Estado também exerce uma influência direta sobre os direitos fundamentais. Tal ocorre porque a comunidade incorporada no Estado é responsável por eleger as circunstâncias, meios e limites para a consagração desses direitos no âmbito da sua constituição.

Neste sentido, JORGE MIRANDA afirma que “não basta, pois, para que haja ou para que sejam garantidos direitos fundamentais que exista Estado. É necessário que o regime ou o sistema político lhes seja adequado; é necessário que a estrutura do poder seja compatível com a sua salvaguarda. Se o que está em causa é a posição da pessoa perante o poder, torna-se ineliminável a conexão entre o sistema de poder e o

¹⁴ Cfr. CANOTILHO, Gomes (2018) – *Direito Constitucional e Teoria da Constituição*, 7.ª Ed., Almedina, Coimbra, p. 386.

dos direitos fundamentais e um e outro fazem parte de uma mesma Constituição, com a sua coerência própria. A concentração do poder não se compadece com as liberdades públicas e, no limite, até com as liberdades privadas. Apenas a divisão do poder as assegura ou assegura plenamente; e divisão do poder requer legitimação não autocrática e mecanismos de controlo”¹⁵.

E, conforme apontado por JORGE REIS NOVAIS, a proteção legal assegurada pelos direitos fundamentais evolui de acordo com o progresso e aperfeiçoamento das instituições do Estado de Direito. Inicialmente, no contexto do Estado liberal, essa proteção limitava-se a defender contra a atuação ilegal da Administração e, posteriormente, no início do Estado social de Direito, ampliou-se com a constitucionalização dos direitos sociais e a garantia, também contra o legislador, de um núcleo essencial dos direitos fundamentais como valores. Atualmente, essa evolução traduz-se numa proteção abrangente contra qualquer dano à liberdade causado pelo Estado¹⁶.

E, por seu turno, VIERA DA SILVA afirma que os direitos fundamentais podem ser interpretados de diferentes maneiras. Podem ser vistos como direitos naturais inerentes a todos os seres humanos, independentemente de tempo e lugar, uma perspectiva filosófica ou jusnaturalista e, alternativamente, podem ser entendidos como os direitos mais importantes das pessoas num determinado momento e lugar, ou seja, em um Estado específico ou numa comunidade de Estados, uma perspectiva estadual ou constitucional. Além disso, também podem ser considerados como direitos essenciais das pessoas num determinado período de tempo em qualquer lugar ou, pelo menos, em grandes regiões do mundo, numa perspectiva universalista ou internacionalista¹⁷.

Ora, JORGE MIRANDA qualifica os direitos fundamentais como posições ativas estabelecidas na Constituição (seja em termos formais ou materiais), inerentes ao nascimento de qualquer cidadão. Estas posições têm a finalidade de proteger os valores e posições jurídicas mais significativos tanto para pessoas individuais quanto para entidades coletivas¹⁸.

¹⁵ Cfr. MIRANDA, Jorge (1999) – *O Homem e o Estado - Direitos do Homem e Democracia*. Artigo publicado na Revista Interesse Público. São Paulo: Notadez, Ano I, n. 01, Janeiro/Março 1999, 1, pp. 79 e 80.

¹⁶ Cfr. NOVAIS Jorge Reis (2010) – *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2ª ed, Coimbra Editora, Coimbra, p. 295.

¹⁷ Cfr. ANDRADE José Carlos Vieira de (2012) – *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 5ª ed., Almedina, Coimbra, p. 15.

¹⁸ Cfr. MIRANDA, Jorge (1999) – *Direitos Fundamentais: Introdução Geral* (Lisboa, 1999), p. 11.

Esta ideia destaca que os direitos fundamentais são posições jurídicas conferidas pela Constituição da República Portuguesa.

Assim, a escolha do critério de atribuição baseia-se na fonte dessa atribuição, implicando uma relação direta e uma vinculação especial do Estado, dado que, os direitos fundamentais têm uma inclinação imediata para o caráter publicista, mesmo quando os efeitos se manifestam nas relações entre particulares.

Dentro desse contexto, os direitos fundamentais representam posições da pessoa em relação ao Estado, o que significa que esses direitos estabelecem uma espécie de escudo legal para proteger os cidadãos contra a atuação excessiva ou arbitrária do Estado.

Assim, ainda que os efeitos desses direitos se manifestem nas relações entre particulares, a origem e a finalidade primordial residem na relação especial e direta entre o cidadão e o Estado, refletindo uma dinâmica fundamental no ordenamento jurídico português, sendo este o aspeto fundamental para destrinçar entre direitos fundamentais e direitos de personalidade.

1.2. PRINCIPAIS DIREITOS FUNDAMENTAIS

Não sendo este o principal foco do presente estudo, ainda assim, cremos ser pertinente deixar uma breve nota quanto aos principais direitos fundamentais previstos na Constituição da República Portuguesa.

A CRP, aprovada no ano de 1976, é a lei fundamental que estabelece os princípios e regras que regem o Estado português e nela são reconhecidos e garantidos os direitos fundamentais dos cidadãos portugueses, que – como já vimos – são as posições jurídicas básicas que todos os indivíduos têm, independentemente da sua nacionalidade, raça, sexo, religião ou qualquer outra condição.

Em primeiro lugar, quando falamos sobre os direitos fundamentais em Portugal, é importante destacar que a Constituição da República Portuguesa organiza-os em duas categorias principais. Por um lado, temos os “direitos, liberdades e garantias”, que estão detalhados nos artigos 24.º e seguintes da CRP e, por outro lado, encontramos os “direitos e deveres económicos, sociais e culturais” definidos nos artigos 58.º e seguintes da referida Constituição¹⁹.

¹⁹ Cfr. <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

Estas duas grandes categorias abrangem uma variedade de direitos que visam garantir a dignidade, liberdade e igualdade de todos os cidadãos, bem como promover o desenvolvimento económico, social e cultural da sociedade.

Numa sociedade democrática, os direitos, liberdades e garantias assumem um papel fundamental, sendo verdadeiros pilares que sustentam a vivência dos cidadãos. Estes direitos não são meras abstrações legais; são, antes, a essência da liberdade individual e coletiva e a sua importância vai além da mera existência escrita em documentos legais, porquanto os mesmos representam a base da experiência democrática, conferindo aos cidadãos a segurança de que as suas liberdades estão protegidas, mesmo na ausência de leis específicas.

Assim, podemos afirmar que os direitos, liberdades e garantias, como o direito à liberdade e à segurança, à propriedade privada, à integridade física e moral (onde se inclui o direito à palavra ou o direito à imagem), à liberdade de expressão, à participação política e à participação na administração da justiça, são fundamentais para a experiência democrática, motivo pelo qual são amparados por um regime constitucional que torna difícil a sua restrição²⁰ ou suspensão²¹.

²⁰ V. Art.º 18.º CRP

Força jurídica

“1. Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são diretamente aplicáveis e vinculam as entidades públicas e privadas.

2. 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.

3. As leis restritivas de direitos, liberdades e garantias têm de revestir carácter geral e abstrato e não podem ter efeito retroativo nem diminuir a extensão e o alcance do conteúdo essencial dos preceitos constitucionais”, Cfr.

<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

²¹ Veja-se o art.º 19.º da CRP Suspensão do exercício de direitos

“1. Os órgãos de soberania não podem, conjunta ou separadamente, suspender o exercício dos direitos, liberdades e garantias, salvo em caso de estado de sítio ou de estado de emergência, declarados na forma prevista na Constituição.

2. O estado de sítio ou o estado de emergência só podem ser declarados, no todo ou em parte do território nacional, nos casos de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública.

3. O estado de emergência é declarado quando os pressupostos referidos no número anterior se revistam de menor gravidade e apenas pode determinar a suspensão de alguns dos direitos, liberdades e garantias suscetíveis de serem suspensos.

4. A opção pelo estado de sítio ou pelo estado de emergência, bem como as respetivas declaração e execução, devem respeitar o princípio da proporcionalidade e limitar-se, nomeadamente quanto às suas extensão e duração e aos meios utilizados, ao estritamente necessário ao pronto restabelecimento da normalidade constitucional.

5. A declaração do estado de sítio ou do estado de emergência é adequadamente fundamentada e contém a especificação dos direitos, liberdades e garantias cujo exercício fica suspenso, não podendo o estado declarado ter duração superior a quinze dias, ou à duração fixada por lei quando em consequência de declaração de guerra, sem prejuízo de eventuais renovações, com salvaguarda dos mesmos limites.

6. A declaração do estado de sítio ou do estado de emergência em nenhum caso pode afetar os direitos à vida, à integridade pessoal, à identidade pessoal, à capacidade civil e à cidadania, a não retroatividade da lei criminal, o direito de defesa dos arguidos e a liberdade de consciência e de religião.

Os direitos, liberdades e garantias são a espinha dorsal de uma sociedade democrática.

Por conseguinte, como nos refere CARLOS BLANCO DE MORAIS, a sua estrutura constitucional reforça a ideia de que esses direitos não são apenas concedidos, mas são inerentes à natureza da democracia e à própria cidadania²², formando a essência da convivência democrática, motivo pelo qual apenas em casos muito restritos podem tais direitos ser limitados²³.

Noutro âmbito, os direitos económicos, sociais e culturais, como o direito a uma habitação condigna, ao emprego, à segurança social, ao meio ambiente e à qualidade de vida, dependem das condições sociais e económicas conjunturais para serem efetivamente realizados. Nessas situações, a não realização desses direitos não concede automaticamente aos cidadãos o direito de requerer uma compensação financeira.

Isso significa que, embora esses direitos sejam direitos fundamentais, a sua concretização prática está muitas vezes condicionada à existência de um ambiente social e económico favorável.

Esta perspectiva destaca a interdependência entre os direitos e as condições sociais e económicas, reconhecendo-se que, em certas circunstâncias, a realização plena desses direitos pode ser desafiadora devido a fatores externos, estando tais direitos – nas palavras do TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÃO – sujeitos à reserva do possível²⁴.

7. A declaração do estado de sítio ou do estado de emergência só pode alterar a normalidade constitucional nos termos previstos na Constituição e na lei, não podendo nomeadamente afetar a aplicação das regras constitucionais relativas à competência e ao funcionamento dos órgãos de soberania e de governo próprio das regiões autónomas ou os direitos e imunidades dos respetivos titulares.

8. A declaração do estado de sítio ou do estado de emergência confere às autoridades competência para tomarem as providências necessárias e adequadas ao pronto restabelecimento da normalidade constitucional”, Cfr.

<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

²² Cfr. MORAIS, Carlos Blanco de – *Some new thoughts on the so called “dogmatic unity” between liberty rights and social rights in times of financial emergency*, disp. in <http://e-publica.pt/volumes/v1n3a05.html>

²³ Este aspeto foi frequentemente debatido aquando das sucessivas restrições à liberdade de reunião e deslocação durante o período mais conturbado da pandemia da COVID-19.

²⁴ A expressão “reserva do possível” foi introduzida pelo Tribunal Constitucional Federal Alemão em 18 de julho de 1972, no julgamento BVerfGE 33, 303 (*numerus clausus*). Essa decisão avaliou a constitucionalidade das normas estaduais que regulamentavam a admissão aos cursos de medicina em Hamburgo e na Baviera em 1969 e 1970. Devido à capacidade exaurida desses cursos, foram estabelecidas restrições absolutas de admissão, conhecidas como *numerus clausus*, Cfr. SCHWABE, Jürgen (2005) – *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*. Organização e introdução por Leonardo Martins. Montevidéu: Konrad-Adenauer-Stiftung, pp. 656 a 667.

1.3. DIREITO À RESERVA DA INTIMIDADE DA VIDA PRIVADA

O direito à reserva da intimidade da vida privada e familiar encontra-se previsto no art.º 26.º da Constituição da República Portuguesa, nos arts. 190.º a 194.º do Código Penal e ainda no art.º 80.º do Código Civil.

Trata-se de um direito ao respeito pela vida privada²⁵, englobando tanto “o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar”, assim como “o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem”²⁶.

Estamos, portanto, perante um bem jurídico pessoal que assegura e garante “ao indivíduo o domínio sobre a sua esfera privada e, por via disso, um espaço de isolamento e auto-determinação resguardado contra as intromissões e injunções da sociedade e do Estado”²⁷.

O direito à proteção da vida privada²⁸ é um direito fundamental reconhecido pela maioria das constituições e leis em todo o mundo e é considerado uma extensão do direito à intimidade e protege os indivíduos de interferências indevidas na sua vida privada, família, lar e correspondência. Neste sentido, a reserva da intimidade da vida privada prende-se, desde logo, com a restrição no acesso à informação. A pessoa deve ter direito à autodeterminação informativa (figura que já existe no direito alemão), ou seja, a pessoa deve poder opor-se à divulgação de factos da vida privada e de controlar as informações que lhe dizem respeito quer sejam verdadeiras ou falsas²⁹.

O direito à proteção da vida privada permite que as pessoas controlem as informações que compartilham sobre si mesmas e protejam a sua imagem e reputação. Por outro lado, também protege os indivíduos de vigilância ou monitoramento não autorizado, incluindo a coleta, armazenamento e uso indevido de informações pessoais por parte de empresas e governos, o que significa que as pessoas têm o direito de decidir que

²⁵ Cfr. MEDEIROS, Rui e CORTÊS, António, “Artigo 16.º”, p. 452.

²⁶ Cfr. CANOTILHO, J.J. Gomes e MOREIRA, Vital – “Artigo 26.º”, p. 467. Rui Medeiros e António Cortês definem este direito como “o direito de oposição à divulgação da vida privada”, assim como “o direito ao respeito da vida privada, ou seja, o direito de oposição à investigação sobre a vida privada”, cfr. MEDEIROS, Rui e CORTÊS, António, “Artigo 26.º”, p. 452.

²⁷ Cfr. ANDRADE, Manuel da Costa, “Artigo 192.º (Devassa da vida privada)”, p. 727

²⁸ Cfr. <http://fra.europa.eu/pt/eu-charter/article/7-respeito-pela-vida-privada-e-familiar>

²⁹ Cfr. MOTA PINTO, Paulo (1989) – *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*, in: Estudos em Memória do Professor Doutor Paulo Cunha, Lisboa, p. 532.

informações desejam compartilhar e com quem, seja em conversas pessoais ou por outros meios³⁰.

Embora o direito à proteção da vida privada não seja absoluto e possa ser limitado em certas circunstâncias, como para proteger a segurança nacional ou a prevenção de crimes, qualquer restrição deve ser proporcional e necessária para atingir um objetivo legítimo, o que significa que devem ser necessárias e adequadas para alcançar o objetivo legítimo que justifica a limitação.

Procurando agora estreitar o âmbito do presente estudo, do geral para o particular e, relativamente àquilo que mais nos importa aprofundar, verificamos que, como referido por COSTA ANDRADE, “a revolução científico-tecnológica trouxe consigo a massificação de meios sem precedentes de devassa”³¹.

Assim, se se pretende utilizar as tecnologias de reconhecimento facial – apesar das suas vantagens para a realização da justiça e para a descoberta da verdade material – tal consubstancia necessariamente uma restrição ao direito à reserva da intimidade da vida privada e familiar (art.º 18.º da CRP), pelo que, deverá ser utilizada de forma proporcional e com cautela.

1.4. DIREITO À IMAGEM

1.4.1. O CONCEITO DE IMAGEM

Estabelece o art.º 79.º, n.º 1 do Código Civil que não se pode expor, copiar ou vender a imagem de alguém sem a sua autorização, cabendo, após a morte da pessoa, cabendo o poder de autorizar permissão aos indivíduos mencionados no art.º 71.º, conforme a ordem indicada.

Sem prejuízo do exposto, o n.º 2 do referido artigo 79.º esclarece que não é necessário obter autorização se a exposição da imagem for justificada pela notoriedade da pessoa, cargo ocupado, razões policiais ou judiciais, objetivos científicos, educacionais ou culturais ou ainda quando a imagem estiver relacionada a locais públicos, eventos de interesse público ou ocorridos publicamente.

³⁰ Cfr. MOTA PINTO, Paulo (1993) – *O Direito à reserva sobre a Intimidade e sobre a vida privada*, Boletim da FDUC, LXIX.

³¹ Cfr. ANDRADE, Manuel da Costa (1999) – “Artigo 192.º (Devassa da vida privada)”, in: *Comentário Conimbricense do Código Penal*, Parte Especial, Tomo I, dirigido por Jorge de Figueiredo Dias, Coimbra Editora, p. 726.

No entanto, é importante notar que, mesmo nessas situações, a imagem não pode ser reproduzida, exposta ou comercializada se causar danos à honra, reputação ou decoro da pessoa retratada (art.º 79.º, n.º 3 do Código Civil).

Neste sentido, verificamos que o retrato da pessoa humana não pode ser obtido e difundido sem consentimento da mesma, de acordo com o disposto nos artigos 81.º e 340.º do Código Civil.

Porém, coloca-se a questão: o que é, na realidade, a imagem de uma pessoa? Será apenas o seu rosto? Será o seu corpo? Ou será mais do que isso?

Ora, de acordo com ADALBERTO COSTA, “A imagem pessoal é composta não apenas pelo corpo, por todo o corpo da pessoa humana, mas também, pela sua personalidade, pelo seu conhecimento, pela sua educação, pela sua vida enquanto ser humano, pela sua idade, pela sua profissão, pelos seus gostos, pela sua sabedoria, pela inteligência, pela família, pela sensibilidade humana, etc.”³².

A imagem incorpora assim muitos outros bens de personalidade, o direito ao bom nome, o direito à honra, a consideração social. É pois, mais acertada uma conceção mais restrita do direito à imagem que apenas abranja a forma externa do ser humano.

1.4.2. O CONSENTIMENTO DA PESSOA RETRATADA

Conforme já foi referido, a imagem da pessoa não pode ser exposta ou comercializada sem o consentimento.

Por outro lado, como refere JOSÉ ALBERTO GONZALEZ, “não pode ser esquecida a regra *dominus membrorum suorum nemo videtur*, significa que nem qualquer consentimento é válido, ou que é o mesmo, que nem todo o consentimento legitima a intervenção na esfera jurídica de quem em tal assentiu”. De acordo com o conteúdo que se extrai do art.º 81º do Código Civil, o consentimento daquele que autolimita algum direito de personalidade não valida a ingerência de terceiro na sua esfera jurídica se for contrário ao princípio de ordem pública³³.

O consentimento previsto no art.º 81.º do Código Civil distingue-se do artigo 340.º deste mesmo diploma, porquanto funciona como cláusula de exclusão da ilicitude,

³² Cfr. COSTA, Adalberto (2012) – *O direito à imagem*, Revista Ordem dos Advogados, Ano 72, volume IV.

³³ Cfr. GONZALEZ, José (2022) – número 1 e 2, *Revista da Faculdade de Direito*, Universidade de Lisboa.

justificando a conduta de quem *a priori* pratica um ato ilícito e por isso mesmo iria incorrer em responsabilidade civil aquiliana nos termos do art.º 483.º do CC.

Uma questão interessante nesta matéria prende-se com a existência de uma exceção à regra contida no art.º 406º CC, dado tratar-se de matéria que respeita a tutela da personalidade humana, motivo pelo qual o consentimento em causa é sempre revogável.

A falta de referência explícita, na lei, à necessidade de consentimento, para a captação e eventual posterior difusão da imagem individual, não significa que ela não se requeira. Como a aquisição da imagem de outrem é diferenciável do momento relativo à sua disseminação, cabe também entender que a anuência para a primeira não envolve necessariamente a permissão da segunda. O preceito contido no art.º 79.º CC tem utilidade porque é através dele que se manifesta a preocupação de produzir um inventário dos casos em que a captação e/ou a divulgação da imagem alheia não depende do assentimento do titular.

Quanto aos casos em que não é necessário o consentimento, JOSÉ ALBERTO GONZÁLEZ salienta três situações:

- Numa, as razões atinentes à própria pessoa retratada que justificam a desnecessidade de consentimento (cargo que a pessoa desempenha, notoriedade da pessoa);
- Quando estão em causa as razões ligadas à finalidade da captação/divulgação do retrato (exigências de justiça, fins didáticos, fins sociais);
- E, por fim, a própria natureza do contexto em que a pessoa é retratada que funda a superfluidade do consentimento (Imagem enquadrada em locais públicos, na de factos de interesse público)³⁴. A desnecessidade de consentimento do retratado fundada na publicidade do próprio local ou do evento em que a pessoa é colhida supõe pelo menos que ela não tenha sido especialmente visada, pelo que, a exceção estará verificada sempre que tal imagem seja captada por razões fortuitas ou apenas quando a imagem tenha sido intercetada pelo autor do retrato.

³⁴ Cfr. GONZALEZ, José (2022) – número 1 e 2, *Revista da Faculdade de Direito*, Universidade de Lisboa.

Assim, quando um espectador de um determinado espetáculo está a ser filmado diretamente por um cameraman terá de existir anuência (expressa ou tácita).

Quanto à notoriedade pessoal, o critério para a sua definição passa, hoje em dia, muito pela frequência com que certa pessoa surge nos meios de comunicação social. O mesmo se refere quanto a notoriedade resultante do desempenho de cargos públicos.

Por outro lado, as exigências “de justiça, de polícia” determinam igualmente a superfluidade do consentimento para a obtenção e difusão do retrato. A fórmula usada é claramente de alcance dúbio, não se admitindo uma difusão em todo o lado, de qualquer forma, do retrato de uma pessoa só porque a mesma terá, alegadamente, praticado um crime.

Quanto a este aspeto, cumpre não esquecer que, de acordo com o disposto no art.º 32.º, n.º 2 da CRP, qualquer cidadão é inocente até prova em contrário.

Neste sentido, GERMANO MARQUES DA SILVA salienta ainda que, paralelamente ao exposto, o princípio *in dubio pro reo* – o qual também vigora no nosso ordenamento – representa uma consagração prática do princípio da presunção de inocência³⁵ e, no mesmo sentido, ALEXANDRA VILELA considera que a presunção de inocência significa que o acusado tem o direito de ser tratado como inocente até que haja provas suficientes especificamente sobre a sua culpabilidade. É como se fosse um direito pessoal do acusado a ser considerado inocente até que se prove o contrário³⁶.

Isto posto, qualquer uma das exceções ao art.º 79.º n.º 2 do CC à necessidade de anuência por parte da pessoa retratada deixa de ter aplicação sempre que a captação ou a divulgação da imagem ofenda a honra a reputação ou o decoro da pessoa, remete-se assim para a indispensabilidade de proteção devida a um outro direito de personalidade: o do “bom nome” e reputação. (art.º n.º 484.º CC e 26, n.º 1 da CRP).

Segundo o TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, “o direito à proteção da imagem individual compõe um dos principais ingredientes da intimidade pessoal e envolve, forçosamente, o poder de supervisionar a sua utilização”³⁷.

³⁵ Cfr. SILVA, Germano Marques (2008) – *Curso de Processo Penal*, Vol. I, Edições Verbo, pp. 83 e 84.

³⁶ Cfr. VILELA, Alexandra (2000) – *Considerações acerca da presunção de inocência em direito processual penal*, Coimbra Editora, p. 80.

³⁷ Cfr. <https://hudoc.echr.coe.int/eng?i=001-90617>.

No entanto, há exceções, como quando um indivíduo – conscientemente ou não – permite que a sua fotografia seja captada num contexto público ou similar, a proteção da imagem pressupõe a obtenção do consentimento do visado no momento em que ela é obtida (como já vimos, pode ser expresso ou tácito).

No entanto, este princípio não é absoluto.

Neste sentido, vejamos alguns motivos de interesse público e casos em que a inserção do indivíduo na categoria de figura pública podem justificar o registo da imagem sem o seu consentimento.

No caso de pessoas detidas, presas, alvo de processo penal, a utilidade objetiva das imagens captadas pelas autoridades após a detenção do indivíduo suspeito de cometer um crime pode legitimar deste modo a retenção da imagem.

No caso MURRAY v. REINO UNIDO, 1994, a tomada e manutenção, sem o seu assentimento, da fotografia de uma pessoa suspeita da prática de um crime de terrorismo, não foi considerada desproporcionada considerando o objetivo pretendido: a prevenção de atos terroristas³⁸.

Porém, de maneira diferente já entendeu o TEDH ao afirmar constituir uma violação do artigo 8.º da Convenção Europeia dos Direitos do Homem o caso em que a polícia forneceu fotografias à imprensa, sem consentimento prévio dos visados, casos de fotografias de indivíduos presos ou acusados (SCIACCA v. ITALIA, 2005³⁹), ou mesmo em que convidou equipas de imprensa para filmarem suspeitos de um crime na esquadra com a subsequente transmissão das imagens assim obtidas (TOMA v. ROMENIA, 2009⁴⁰), ou ainda o caso em que a exibição da fotografia de um indivíduo resultou da sua obtenção a partir de uma lista de *most wanted persons* (GUIORGUI NIKOLAICHVILI v. GEÓRGIA, 2009⁴¹) elaborada por entidades policiais.

Já, porém, a retenção por tempo ilimitado da fotografia do indivíduo suspeito de cometer um crime de cuja comissão foi, a final, absolvido, apresentava maior risco de desonra do que a retenção de dados sobre indivíduos que foram condenados por um crime (S. AND MARPER v. REINO UNIDO, 2008⁴²).

³⁸ Cfr. <https://rm.coe.int/case-law-on-data-protection/1680766992>.

³⁹ Cfr. <https://www.5rb.com/case/sciaccia-v-italy/>.

⁴⁰ Cfr. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-123515%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-123515%22]}).

⁴¹ Cfr. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-90590%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90590%22]}).

⁴² Cfr. <https://rm.coe.int/168067d216>.

No que toca as técnicas de reconhecimento e mapeamento facial que atualmente se podem aplicar a fotografias contendo retratos pessoas, por serem cada vez mais complexas, obrigam os tribunais nacionais, no entender do Tribunal Europeu de Direitos Humanos, a examinar ao pormenor a necessidade de qualquer interferência sobre o direito à imagem.

Neste sentido, o TEDH considerou no caso *REKLOS e DAVOURLIS v. GRÉCIA*, 2009, ter havido violação do artigo 8.º a propósito da obtenção numa clínica, de uma fotografia de um recém-nascido contra a vontade dos pais, de uma forma que permitiria a sua identificação e a possibilidade de uso indevido⁴³. De um igual modo, considerou-se ter havido violação do artigo 8º da CEDH nos casos *HAJOVSKY v. ESLOVÁQUIA*, 2021⁴⁴, no que respeita à publicação na imprensa de imagens não convenientemente desfocadas do requerente e ainda o caso *VOLDINA v. RUSSIA*, 2021⁴⁵, no que tange à falha das autoridades em proteger uma mulher contra a reiterada ciberviolência do marido que criou perfil falso da mesma e publicou fotos íntimas.

Já no caso *VON HANNOVER v. ALEMANHA*, 2012⁴⁶, a recusa dos Tribunais nacionais em interditar a publicação de uma fotografia de um casal famoso tirada sem consentimento foi entendida como não constituindo infração ao art.º 8.º da CEDH.

Em processos relativos à tomada pelas autoridades, para fins de prevenção criminal, de impressões digitais, dados biológicos, e perfis de ADN de pessoas suspeitas de crimes, indicou o TRIBUNAL EUROPEU DE DIREITOS HUMANOS que o recurso a modernas tecnologias não pode ser autorizado, embora reconhecendo que é de antecipar, tendo em conta o ritmo acelerado dos desenvolvimentos no campo da genética e da tecnologia de informação, a possibilidade de que, no futuro, o direito à vida privada e o direito à informação genética se tornem fortes adversários. O desenvolvimento rápido de técnicas cada vez mais inteligentes que tem permitido, entre outras coisas, o desenvolvimento de instrumentos de reconhecimento facial, faz do armazenamento e divulgação de fotografias um tema bastante delicado.

⁴³ Cfr. <https://www.5rb.com/case/reklos-and-davourlis-v-greece/>.

⁴⁴ Cfr. [https://hudoc.echr.coe.int/fre#{%22tabview%22:\[%22document%22\],\[%22itemid%22:\[%22001-210766%22\]\]}](https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],[%22itemid%22:[%22001-210766%22]]}).

⁴⁵ Cfr. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-211794%22\]\]](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-211794%22]]).

⁴⁶ Cfr. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-109029%22\]\]](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109029%22]]).

Assim, os Tribunais nacionais não devem, apesar disso, deixar de levar em conta estas evoluções tecnológicas ao avaliar a necessidade de interferência na vida privada.

A jurisprudência acima referida do TEDH, em matéria do direito à imagem, autoriza de imediato uma clara lição: nela, a respetiva tutela encontra o seu fundamento na proteção devida à “vida privada e familiar”.

Contudo, existe uma exceção a essa regra, que ocorre nos casos em que um terceiro é autorizado a exercer o direito à imagem conforme estipulado na CONVENÇÃO EUROPEIA DOS DIREITOS DO HOMEM⁴⁷.

Ao mesmo tempo, essa perspetiva possibilita afirmar que os casos em que um terceiro tem autorização para interferir no direito à imagem de outra pessoa devem ser enquadrados no n.º 2 do art.º 8.º CEDH. As referências presentes nesse artigo à segurança nacional, segurança pública, defesa da ordem e prevenção de infrações penais podem, no contexto das FRT (Fontes de Reconhecimento Técnico), ser proveitosas.

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

E, analisando a jurisprudência portuguesa, podemos referir o ACÓRDÃO DO SUPREMO TRIBUNAL DE JUSTIÇA DE 14/06/2005, que esclarece:

“1 - O direito à imagem e direito à reserva sobre a intimidade da vida privada, enquanto direitos fundamentais de personalidade, são inatos, inalienáveis, irrenunciáveis e absolutos, no sentido de que se impõem, por definição, ao respeito de todas as pessoas.

2 - O que se passa no interior da residência de cada pessoa e na área, privada, que a circunda, integra o núcleo duro da reserva da intimidade da vida privada legalmente protegida.

3 - A publicação numa revista pertencente à ré de uma reportagem fotográfica legendada divulgando, sem consentimento do autor, uma visita por ele feita na companhia da mulher à residência familiar então em fase de construção na cidade de

⁴⁷ Cfr. https://www.echr.coe.int/documents/d/echr/convention_por.

Madrid, integra a violação simultânea dos seus direitos à imagem e à reserva da intimidade da vida privada”⁴⁸.

1.5. DISTINÇÃO DOS DIREITOS FUNDAMENTAIS FACE AOS DIREITOS DE PERSONALIDADE

A acrescentar a todo o exposto nos pontos anteriores, numa sociedade jurídica complexa e multifacetada, é imperativo compreender a distinção entre direitos fundamentais e direitos de personalidade.

É que, ambos, embora intrinsecamente ligados, possuem contornos distintos.

Os direitos fundamentais são a espinha dorsal das garantias individuais, sendo consagrado nas normas constitucionais. Conforme verificamos, tais direitos são inalienáveis, universais e protegem a dignidade e liberdade de cada ser humano face ao Estado. São, por isso, pedras basilares que sustentam a construção de uma sociedade justa e equitativa e, nas palavras de JORGE REIS NOVAIS, “trunfos contra a maioria”⁴⁹.

Por outro lado, os direitos de personalidade centram-se na esfera privada do indivíduo, abrangendo as facetas mais íntimas da sua existência.

Estes direitos são moldados pela singularidade de cada pessoa, englobando aspetos como a imagem, a palavra e a reserva da intimidade da vida privada. Ao contrário dos direitos fundamentais, os direitos de personalidade não são exclusivamente vertentes da relação indivíduo-Estado, mas também regulam as relações entre os próprios cidadãos e entidades privadas⁵⁰.

De acordo com OLIVEIRA ASCENSÃO, “o facto de os direitos de personalidade terem fundamento comum na proteção constitucional da personalidade não significa que a sua definição e regime estejam rigidamente constitucionalizados”⁵¹.

⁴⁸ Disp. in

<http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20>

⁴⁹ Cfr. NOVAIS, Jorge Reis (2006) – *Direitos Fundamentais: Trunfos contra a Maioria*. Coimbra: Editora Coimbra, p. 72.

⁵⁰ Cfr. MIRANDA, Jorge; MEDEIROS, Rui (2005) – *Constituição portuguesa anotada*. Tomo I. Coimbra: Coimbra Editora.

⁵¹ Cfr. ASCENSÃO, José de Oliveira (2000) – *Direito civil – Teoria Geral*. Vol. I. 2ª ed. Coimbra: Coimbra Editora, pp. 19 e ss.

O direito à reserva da intimidade da vida privada (art.º 80.º do Código Civil), por exemplo, consagra a proteção da esfera mais reservada do indivíduo, impedindo interferências externas injustificadas⁵². Já o direito à imagem (art.º 79.º do Código Civil) confere a cada pessoa o controlo sobre a reprodução e divulgação da sua representação visual, salvaguardando a autodeterminação da sua imagem pública⁵³.

Assim, enquanto os direitos fundamentais estabelecem o alicerce dos princípios que regem a relação Estado-indivíduo, os direitos de personalidade moldam-se em torno da singularidade de cada pessoa, protegendo aspetos intrínsecos à sua individualidade, sendo aplicados na relação horizontal, ou seja, face a outros particulares. Esta distinção é crucial para a compreensão da complexidade do tecido jurídico que regula a convivência em sociedade, garantindo um equilíbrio entre liberdade individual, a sociedade como um todo e o bem comum.

⁵² “Artigo 80.º

(Direito à reserva sobre a intimidade da vida privada)

1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.

2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas”.

⁵³ “Artigo 79.º(Direito à imagem)

1. 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 no n.º 2 do artigo 71.º, segundo a ordem nele indicada.

2. Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente.

3. O retrato não pode, porém, ser reproduzido, exposto ou lançado no comércio, se do facto resultar prejuízo para a honra, reputação ou simples decoro da pessoa retratada”.

CAPÍTULO I- A PRIVACIDADE NO ORDENAMENTO JURÍDICO PORTUGUÊS E EVOLUÇÃO DA PROTEÇÃO DE DADOS

2. LEGISLAÇÃO APLICÁVEL

2.1. A EVOLUÇÃO DA LEGISLAÇÃO EM PORTUGAL E NO MUNDO

A privacidade é um direito fundamental reconhecido no ordenamento jurídico português e protegido pela Constituição da República Portuguesa.

E, apesar de apenas recentemente terem sido estabelecidos mecanismos específicos de proteção, em termos históricos cumpre referir a DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HOMEM, aprovada pela Assembleia Geral das Nações Unidas no ano de 1948, a qual prevê no art.º 12º que “ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação”⁵⁴.

Neste sentido, a atual perspetiva do direito fundamental à proteção dos dados pessoais decorre essencialmente de uma evolução legislativa dos países europeus ao longo das últimas quatro gerações.

A primeira teve a sua origem na Alemanha, através da LEI LAND HESSE, inaugura em 1970 a proteção dos dados informatizados (proteção para os dados informatizados de titularidade pública)⁵⁵.

Paralelamente, em 1977, a lei Alemã passou a regular os arquivos de utilidade pública e também privada⁵⁶.

No mesmo período, a Suécia (1973)⁵⁷, a Dinamarca (1978)⁵⁸ e a Áustria (1978)⁵⁹, legislaram no mesmo sentido;

A segunda fase focou-se na tutela dos direitos fundamentais envolvidos nas relações das comunicações virtuais.

⁵⁴ Cf. <https://www.cig.gov.pt/wp-content/uploads/2018/01/Declaracao-Universal-dos-Direitos-Humanos.pdf>.

⁵⁵ Cfr. https://gdprhub.eu/Data_Protection_in_Germany.

⁵⁶ Cfr. <https://yourdata-yourrights.eu/glossary/federal-data-protection-act/>.

⁵⁷ Cfr. <https://www.dataguidance.com/notes/sweden-data-protection-overview>.

⁵⁸ Cfr. <https://www.civil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/denmark>.

⁵⁹ Cfr. <https://www.civil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/austria>

Neste sentido, temos a lei francesa de 1978⁶⁰, a lei do Luxemburgo de 1979⁶¹ e a lei da Islândia de 1981⁶², as quais visaram criar mecanismo de proteção de arquivos informatizados.

Em 1981, a CONVENÇÃO 108 DO CONSELHO DA EUROPA (Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal⁶³), resultante do fluxo crescente, através das fronteiras, de dados de carácter pessoal suscetíveis de tratamento automatizado, traduz o reconhecimento da necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os Estados.

Assume-se, assim, como o primeiro instrumento internacional vinculativo que trata esta matéria, com o objetivo de proteger as pessoas singulares em relação ao tratamento automatizado de dados pessoais, conforme previsto no art.º 1.º, o qual nos refere que «A presente Convenção destina-se a garantir, no território de cada parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito (“proteção dos dados”)⁶⁴».

Por seu turno, no que respeita em específico ao ordenamento jurídico português, o artigo 26.º da Constituição da República Portuguesa prevê a “proteção da vida privada e familiar, do domicílio e da correspondência”, sendo que a lei define as concretas garantias necessárias para a sua proteção.

Paralelamente ao exposto, cumpre referir a proteção de dados em Portugal evoluiu significativamente nos últimos anos, com a aprovação do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia em 2016 (o qual analisaremos em pormenor mais à frente).

Antes do RGPD, a proteção de dados pessoais em Portugal era regulamentada pela Lei de Proteção de Dados Pessoais, de 1998, que já estabelecia algumas normas sobre a recolha, tratamento e armazenamento de dados pessoais⁶⁵. No entanto, essa

⁶⁰ Cfr. https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf.

⁶¹ Cfr. <https://www.civil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/luxembourg>

⁶² Cfr. <https://www.civil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/iceland>

⁶³ Cfr. <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>

⁶⁴ Cfr. <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>

⁶⁵ Cfr. <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/1998-34450175-43475975>

lei foi considerada desatualizada e insuficiente para lidar com os novos desafios impostos pela evolução tecnológica e pela globalização.

Com a entrada em vigor do RGPD, as empresas que operam em Portugal passaram a ter obrigações mais rigorosas em relação à proteção de dados pessoais, incluindo a necessidade de obter consentimento explícito e informado dos titulares dos dados, de implementar medidas de segurança adequadas e de notificar as autoridades competentes em caso de violação de dados⁶⁶.

Em Portugal, a entidade responsável pela proteção de dados pessoais é a Comissão Nacional de Proteção de Dados (CNPd), a qual tem como missão garantir a proteção dos direitos e liberdades fundamentais das pessoas singulares em relação ao tratamento de dados pessoais⁶⁷.

Neste enquadramento, no ano de 2019 foi aprovada a Lei nº 58/2019, de 8 de agosto⁶⁸, a qual visa assegurar a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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.

Por último, cumpre ainda referir o Despacho n.º 2705/2021, de 11 de março do Gabinete Nacional de Segurança (GNS), o qual vem tratar da “Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial”⁶⁹.

Em concreto, o Programa do XXII Governo Constitucional identifica como um dos desafios estratégicos a promoção de incentivos da sociedade digital, da criatividade e da inovação, privilegiando a simplificação administrativa, o reforço e a melhoria dos serviços prestados digitalmente pelo Estado, o seu acesso e utilização, a par da desmaterialização de mais procedimentos administrativos⁷⁰.

⁶⁶ Cfr. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm.

⁶⁷ Cfr. <https://www.cnpd.pt/>.

⁶⁸ Cfr. <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>.

⁶⁹ Cfr. <https://dre.tretas.org/dre/4447141/despacho-2705-2021-de-11-de-marco>.

⁷⁰ *Id.*

2.2. REGULAMENTO GERAL DE PROTEÇÃO DOS DADOS

O Regulamento Geral de Proteção dos Dados visa garantir a proteção dos dados pessoais dos cidadãos da UE e aplica-se a todas as empresas e organizações que processam dados pessoais de cidadãos da UE⁷¹.

O RGPD estabelece uma série de direitos para os titulares de dados pessoais, como o direito de acesso aos seus dados, o direito de retificação e eliminação, o direito à portabilidade dos dados e o direito de oposição ao processamento de dados. Além disso, o regulamento impõe obrigações às empresas que processam dados pessoais, como a obrigação de obter o consentimento explícito dos titulares dos dados para o processamento, de garantir a segurança dos dados pessoais e de notificar as autoridades competentes em caso de violação de dados.

Em Portugal, o RGPD veio revogar a Diretiva 95/46/CE e o seu principal objetivo do RGPD é proteger os direitos e liberdades fundamentais dos indivíduos, garantindo a privacidade e a proteção dos seus dados pessoais. O regulamento define o conceito de dados pessoais, que se refere a qualquer informação que possa identificar uma pessoa direta ou indiretamente e também estabelece as obrigações dos responsáveis pelo processamento de dados e os direitos dos titulares desses dados.

Com efeito, o Regulamento Geral de Proteção de Dados “aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público”⁷².

O RGPD não se aplica apenas aos dados pessoais constituídos e mantidos dentro do espaço europeu. A sua aplicação alarga-se aos dados transfronteiriços, abrangendo todas as operações realizadas por empresas da União Europeia, ainda que com sede fora da União, ficando claro o seu âmbito de aplicação alargado.

Contrariamente à Diretiva 95/46, de 24 de outubro, o RGPD tem aplicação direta na ordem jurídica interna dos Estados-membros e apresenta como principais objetivos: a harmonização legislativa; a coerência no tratamento dos dados pessoais em todo o espaço europeu; e a segurança jurídica. Para tanto, vai harmonizar e assegurar a defesa dos direitos e liberdades fundamentais das pessoas singulares e garantir a livre

⁷¹ Cfr. <https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html>.

⁷² Cf. Regulamento Geral de Proteção de Dados (2016, artigo 2º.)

circulação de dados pessoais entre os Estados-membros, contribuindo para a realização de um espaço de liberdade, segurança e justiça. Portanto, este novo dispositivo normativo europeu terá uma aplicação uniforme em todos Estados da União Europeia, tendo em vista a proteção de pessoas singulares e seus dados pessoais, enquanto direitos fundamentais, não se importando a nacionalidade ou local de residência.

O RGPD vem clarificar o conceito de dados pessoais, tornando-o mais abrangente e ainda consagrar novos direitos para os titulares de dados, como o direito à portabilidade; o direito ao esquecimento; o direito de oposição; o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a transferir os dados (art.º 20.º do RGPD), bem como prever aplicação de sanções ou medidas corretivas (coimas, advertências ou ordens) às empresas responsáveis pelo tratamento de dados pessoais e subcontratantes, em caso de violações⁷³.

De acordo com NUNO SALDANHA, esta evolução legislativa exigiu, da parte da União Europeia, a “criação de um quadro legal de proteção de dados pessoais e de uma aplicação rigorosa dessas mesmas regras, de forma a gerar a confiança necessária quer aos cidadãos, para disponibilizarem os seus dados, já que poderão ter um controlo sobre os mesmos, quer às organizações, no que toca ao desenvolvimento da economia digital no mercado interno da União Europeia”⁷⁴.

O referido autor salienta ainda a necessidade de uma legislação inovadora em matéria de proteção de dados, perante um “aumento dos fluxos transfronteiriços, em consequência, uma cada vez maior integração económica [e] da criação do mercado único e (...) um intenso intercâmbio de dados entre setores público e privado, resultado da evolução tecnológica contínua e uma globalização já imparável, [permitindo] uma maior recolha e partilha de dados pessoais por parte das organizações e empresas, tanto públicas como privadas, em que os dados pessoais passaram a ter um valor económico muito real e mensurável”⁷⁵.

Por todo o exposto, podemos afirmar que o RGPD é o normativo que melhor responde aos desafios que os Estados-Membros têm pela frente em matéria de proteção dos direitos pessoais dos seus cidadãos, compatibilizando direitos de igual valor

⁷³ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679>.

⁷⁴ Cfr. SALDANHA, Nuno (2018) – *Novo Regulamento de Proteção de Dados*, p. 15.

⁷⁵ Cfr. SALDANHA, Nuno (2018) – *Novo Regulamento de Proteção de Dados*, p. 15.

constitucional, mas por vezes contraditórios, como direito a privacidade, a intimidade, a segurança e a liberdade de expressão.

2.3. PRINCÍPIOS PREVISTOS NO RGPD

De acordo com o previsto no art.º 5.º do Regulamento Geral de Proteção de Dados, o Responsável pelo Tratamento de Dados tem obrigação de respeitar os princípios a seguir enunciados⁷⁶.

Em primeiro lugar, temos a “licitude, lealdade e transparência”, o que significa que os dados têm de ser processados de forma legal, justa e transparente.

O princípio da licitude determina que apenas é possível o tratamento de dados pessoais se existir uma razão suficientemente legítima que o justifique. Nestas circunstâncias, um tratamento de dados pessoais só é lícito se e na medida em que se verifique o consentimento.

O princípio da lealdade está relacionado com o desenvolvimento do tratamento de dados pessoais de uma forma equilibrada tendo em conta os interesses dos responsáveis pelo tratamento e dos subcontratantes, por um lado e dos titulares dos dados, por outro. Assume particular importância quando está em causa o tratamento de dados pessoais de trabalhadores pelas respetivas entidades empregadoras, públicas ou privadas. Caso se verifique incumprimento deste princípio, o responsável pelo tratamento pratica uma contraordenação muito grave, prevista e sancionada nos termos do art.º 83.º/5/a do RGPD⁷⁷ e do art.º 37.º/1/a e n.º 2 da Lei n.º 58/2019, de 8 de agosto⁷⁸ (que, como vimos, assegura a execução, na ordem jurídica nacional, do RGPD). O princípio da lealdade está relacionado com o desenvolvimento do tratamento de dados pessoais de uma forma equilibrada tendo em conta os interesses dos responsáveis pelo tratamento e dos subcontratantes, por um lado, e dos titulares dos dados, por outro.

Por outro lado, o princípio da transparência significa que as informações ou comunicações relacionadas com o tratamento de dados pessoais devem ser de fácil acesso e compreensão e formuladas numa linguagem clara e simples, em particular as informações fornecidas aos titulares dos dados sobre a identidade do responsável

⁷⁶ <https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/principios-do-tratamento-dados/>.

⁷⁷ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679#d1e3713-1-1>.

⁷⁸ Cfr. <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>.

pelo tratamento, assim como os fins a que o tratamento se destina e a salvaguarda dos direitos a obter confirmação dos dados pessoais que estão a ser tratados (Considerandos 39 e 59 do RGPD⁷⁹).

Este princípio é desenvolvido no artigo 12.º do RGPD, o qual determina que as informações previstas nos artigos 13.º e 14.º, bem como as comunicações referidas nos artigos 15.º a 22.º e 34.º, que digam respeito ao tratamento de dados pessoais, devem ser prestadas de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Tais informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos.

Em segundo lugar, temos a “limitação da finalidade”, o que quer dizer que os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não serão tratados posteriormente de forma incompatível com essas finalidades.

O princípio da limitação da(s) finalidade(s) determina que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas e, não podem ser tratados posteriormente de uma forma incompatível com essas finalidades, embora se admita o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica, ou para fins estatísticos. Este princípio assume uma importância fundamental uma vez que só depois de conhecida a finalidade do tratamento é possível apurar se a informação pessoal recolhida é necessária e não excessiva.

As finalidades do tratamento devem ser determinadas, explícitas e legítimas, porquanto está em causa estabelecer os limites para o tratamento e articulá-los com os fundamentos de legitimidade invocados. Nesta medida, afigura-se que não podem ser recolhidos dados pessoais para finalidades futuras, ainda não determinadas no momento da recolha.

Em terceiro lugar, temos a chamada “minimização de dados”, a qual se reporta ao facto de os dados deverem ser adequados, pertinentes e limitados ao necessário em relação à finalidade para a qual são tratados.

O princípio da minimização significa que os dados a tratar devem ser adequados, pertinentes e limitados ao que é exigido pelas finalidades que determinam o tratamento. Segundo este princípio, os dados pessoais apenas devem ser tratados se

⁷⁹ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679#d1e3713-1-1>.

a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. Decorre deste mesmo princípio que só devem ser tratados os dados necessários para a finalidade pretendida e não quaisquer outros. Caso se verifique que foram solicitados dados excessivos, o tratamento passará a ser ilícito, o que constitui contraordenação muito grave prevista e sancionada nos termos da alínea a) do n.º 5 do artigo 83.º do RGPD e da alínea a) do n.º 1 e do n.º 2 do artigo 37.º da Lei n.º 58/2019, de 8 de agosto (que assegura a execução, na ordem jurídica nacional, do RGPD⁸⁰).

Em quarto lugar, temos o conceito de “exatidão”, o que significa que os dados devem ser exatos e, sempre que necessário, atualizados.

O princípio da exatidão exige que os dados pessoais sejam corretos e atualizados sempre que necessário, devendo ser tomadas medidas adequadas para que os dados inexatos sejam apagados ou retificados sem demora.

Em quinto lugar, temos a “limitação da conservação”, ou seja, os dados não devem ser conservados durante mais tempo do que o necessário para o efeito.

O princípio da limitação da conservação impõe que os dados pessoais sejam conservados, de uma forma que permita a identificação dos respetivos titulares, apenas durante o período necessário para as finalidades previstas para o tratamento. Admite-se, contudo, que os dados sejam conservados por períodos mais longos desde que sejam tratados exclusivamente para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou ainda para fins estatísticos, em conformidade com o art.º 89.º/1 do RGPD. Caso se verifique incumprimento deste princípio, o responsável pelo tratamento pratica uma contraordenação muito grave, prevista e sancionada nos termos do art.º 83.º/5/a do RGPD e do art.º 37.º/1/a da Lei n.º 58/2019, de 8 de agosto (que assegura a execução, na ordem jurídica nacional, do RGPD). O art.º 21.º da Lei n.º 58/2019 contém regras específicas sobre conservação de dados pessoais.

Em sexto e último lugar, temos os princípios de “integridade e confidencialidade”, o que quer dizer que os dados são tratados com segurança apropriada, usando medidas técnicas e organizativas apropriadas, incluindo proteção contra processamento não autorizado ou ilegal, contra perda, destruição ou dano accidental.

⁸⁰ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679#d1e3713-1-1>.

O princípio da integridade e confidencialidade impõe que os dados pessoais sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, devendo o responsável pelo tratamento adotar medidas técnicas e organizativas adequadas a evitar o acesso indevido e a utilização dos dados por pessoas não autorizadas. Caso se verifique incumprimento deste princípio, o responsável pelo tratamento pratica uma contraordenação muito grave, prevista e sancionada nos termos do artigo 83.º/5/a do RGPD e do art.º 37.º/1/a e n.º 2 da Lei n.º 58/2019, de 8 de agosto (que assegura a execução, na ordem jurídica nacional, do RGPD⁸¹).

⁸¹ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679#d1e3713-1-1>.

3. O DIREITO À PRIVACIDADE E À PROTEÇÃO DA VIDA PRIVADA

3.1. DESAFIOS ATUAIS À PRIVACIDADE DOS CIDADÃOS

Face aos critérios anteriormente explanados, a proteção dos dados pessoais e a garantia dos direitos pessoais, principalmente o direito à privacidade, afigura-se entre os maiores desafios das atuais sociedades políticas, uma vez que os ordenamentos jurídicos terão de encontrar fronteiras de equilíbrio e conciliar valores, na maioria dos casos, considerados antagónicos, como a liberdade, a segurança, a privacidade, entre outros⁸².

Com a chegada do mundo virtual, este desafio torna-se muito mais exigente, pois não encontramos barreiras físicas, delimitativas de cada Estado. As fronteiras físicas estão agora diluídas, o que requer respostas inovadoras, quer em termos normativos quer em termos institucionais. Veja-se que os direitos pessoais, particularmente o direito à privacidade, constam da DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, instituída a 10 de dezembro de 1948, pela Organização das Nações Unidas⁸³.

O desenvolvimento tecnológico, paradoxalmente, torna as pessoas mais vulneráveis a partir do momento em que sua exposição pública passa a ser constante, o que fez surgir a necessidade crescente de um maior fortalecimento da proteção jurídica da privacidade, sendo relevante refletir sobre as limitações de uma compreensão da privacidade como direito individual.

Numa conjuntura de crescentes avanços tecnológicos, os sistemas de vigilância que utilizam tecnologias de reconhecimento facial tornam-se cada vez mais presentes no quotidiano de diversas sociedades. Alimentados por tecnologias de inteligência artificial e *big data*, tais sistemas potencializam a ocorrência de violações ao direito à privacidade, bem como ao direito à proteção de dados.

Ora, estes sistemas de vigilância não significam apenas uma ameaça à privacidade e à proteção de dados, mas também ocasionam a violação ainda mais patente de tais direitos em se tratando de determinadas pessoas e grupos sociais. Contudo, como afirma STEFANO RODOTÀ, *surveillance is not a destin*: “Não se pode negar que o progresso tecnológico pode proporcionar benefícios sociais inimagináveis há até

⁸² Cfr. CASTRO, Catarina Sarmiento e (2005) – *Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Edições Almedina, p. 40.

⁸³ Cfr. <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>

pouquíssimo tempo. Também não se pode negar a irrefreabilidade de tal progresso, mesmo que este não se apresente com prognósticos somente positivos”⁸⁴.

Portanto, torna-se crucial uma ponderação acerca dos interesses em jogo, para que se assegurem tanto a garantia dos direitos individuais quanto a progressiva abertura da sociedade, sempre em consonância com a participação pública e com debates abertos sobre as garantias e limitações que se mostrarão necessárias para que novas tecnologias sejam implementadas. Reconhecida como uma exigência direta da pessoa, sendo mesmo uma necessidade humana básica, a privacidade apresenta-se como um conceito relevante em todas as áreas da atividade humana, sendo consagrada um direito fundamental expresso em inúmeros documentos de índole jurídica.

Ora, a invasão da privacidade implica a violação da individualidade, da liberdade e da dignidade da pessoa.

Numa perspetiva de defesa da vida privada e do reconhecimento do direito à privacidade, GOMES CANOTILHO e VITAL MOREIRA referem que é “o direito a impedir o acesso de estranhos a informação sobre a vida privada e familiar e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem”⁸⁵.

Por seu turno, PAULO MOTA PINTO afirma que “a defesa da privacidade visa evitar ou controlar a tomada de conhecimento ou a revelação de informação pessoal, dos factos, comunicação ou opinião relacionados com o individuo que é razoável esperar que ele encare como íntimo ou pelo menos confidencial e que, por isso, queira excluir ou pelo menos restringir a sua circulação”⁸⁶.

Ora, o termo privacidade encontra-se consagrado nos textos constitucionais como um direito fundamental, cuja proteção constitui responsabilidade do Estado e do próprio cidadão, com vista à salvaguarda da dignidade da própria pessoa. O direito à reserva sobre a intimidade da vida privada está consagrado no elenco de direitos, liberdades e garantias, previsto no n.º 1 do art.º 26.º da nossa Constituição da República Portuguesa, o qual estabelece que “A todos são reconhecidos os direitos à identidade

⁸⁴ Cfr. RODOTÀ, Stefano (2008) – *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar.

⁸⁵ Cfr. CANOTILHO, Gomes e MOREIRA, Vital (1993) – *Constituição da República Portuguesa anotada*, 3.ª ed., Coimbra, p. 181

⁸⁶ *Apud* GUERRA, Amadeu (1999) – *Informática e privacidade – Nova lei de proteção de dados e a lei de proteção de dados no sector de telecomunicações*. Lisboa: Vislis Editores Lda., p. 158.

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”⁸⁷, bem como em inúmeras cartas europeias e internacionais.

Este direito está diretamente ligado ao princípio norteador do ordenamento jurídico português da dignidade da pessoa humana baseado no pressuposto que a mesma beneficia de um espaço de privacidade sob dois “sub-direitos”, o direito de impedir o acesso de terceiros a informações sobre a vida privada e familiar e o direito a que ninguém divulgue as informações de que disponha sobre a vida privada de outrem, traduzindo-o numa verdadeira proibição de ingerência na vida particular por terceiros, quer por acesso, quer por divulgação de informação, como consagrado no n.º 1 do art.º 80.º do Código Civil, o qual estabelece que “Todos devem guardar reserva quanto à intimidade da vida privada de outrem”⁸⁸.

Neste sentido, advoga GOMES CANOTILHO que “o sigilo que a Constituição consagra sobre os direitos que compõem a esfera privada do indivíduo é posto em risco”, uma vez que “determinados direitos fundamentais colidem com outros direitos constitucionalmente protegidos que encontram limites constituídos pelo direito de outras pessoas e limites da própria ordem social, estando [portanto] a todo momento em conflito”⁸⁹.

Este conflito permanente entre os direitos fundamentais, como o direito a privacidade, a informação e de ser informado, a liberdade de expressão, tem-se mostrado complexo, uma vez que se trata de direitos fundamentais, algumas vezes conflitantes, mas revestidos da força jurídica, cuja restrição é proibida por lei, salvo condições muito específicas. Assim, a resolução dos conflitos tem implicado a aplicação concreta do princípio de proporcionalidade.

3.2. AMEAÇAS ATUAIS A ESTE DIREITO

A privacidade é um dos valores intrínsecos à natureza da pessoa humana, cuja proteção constitui uma das grandes responsabilidades dos Estados modernos, sendo um direito fortemente ameaçado na atual era digital, caracterizada por uma maior circulação e partilha de dados pessoais, podendo tais dados serem alvo de acesso

⁸⁷ Cfr. <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

⁸⁸ Cfr. <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1966-34509075>.

⁸⁹ Cfr. CANOTILHO, Gomes (2018) – *Direito Constitucional e Teoria da Constituição*, 7.ª Ed., Almedina, Coimbra, p. 644.

não autorizado e utilização indevida por terceiros, violando assim o direito à privacidade. O direito à privacidade e os dados pessoais encontra-se, cada vez mais, sujeito a maiores riscos de violação pela quantidade de informação e dados pessoais acumulados na Internet.

Efetivamente, são poucos serviços na Internet que dispensam a recolha, armazenamento, tratamento e difusão de dados pessoais e toda esta utilização deixa traços diversos sobre a vida do utilizador, como por exemplo a sua opinião, os seus gostos, os seus hábitos de consumo, os seus interesses, as suas pesquisas. Nas ruas, nos transportes públicos, nos espaços comerciais, nos serviços, nas lojas, nos aeroportos, encontramos-nos sob constante observação, muitas vezes, com o pretexto da salvaguarda da segurança. Ao ligar o GPS, ao pedir uma pizza, ao procurar um emprego as pessoas produzem informações que são coletadas e armazenadas em equipamentos eletrónicos, muitos dos quais os telemóveis permitindo a sua utilização de acordo com os seus próprios interesses.

Ora, conforme nos refere STEFANO RODOTÁ, este facto torna-se um gravíssimo problema para os titulares dos dados e para a sociedade quando essas informações são compartilhadas e mesmo disponibilizadas a terceiros, o que acaba por transformar a vida particular num grande *reality show*, tornando o indivíduo num objeto em vigilância constante⁹⁰.

Com isso, as pessoas podem ser manipuladas (a partir de publicidades personalizadas, por exemplo), tendo as suas fragilidades mais privadas exploradas de modo a colocar em risco a liberdade e a democracia. Existem casos em que os próprios pais revelam dados pessoais dos filhos menores nas redes sociais, como a fotografia, o nome da escola, a morada da família ou outras informações que permitam identificar os filhos, com relativa facilidade⁹¹.

Sobre esta problemática foi possível perceber que são os próprios titulares de dados que se expõem, muitas vezes de forma inconsciente, disponibilizando os seus dados pessoais e dos seus familiares a terceiros, sem se aperceberem de que estarão a contribuir para que sua privacidade seja agredida, com prejuízo para o seu direito a privacidade e da sua família.

⁹⁰ Cfr. RODOTÁ, Stefano (2013) – *Some Remarks on Surveillance today*, in European Journal of Law and Technology, Vol. 4., No. 2., p.19.

⁹¹ Cfr. Tribunal da Relação de Évora: Processo nº 789/13.7TMSTB-B.E1 (25/06/15), disponível em www.dgsi.pt.

Consegue entender-se que os dados pessoais se converteram na nova matéria-prima do mundo económico. Como afirma CLIVE HUMBY⁹² “os dados são o novo petróleo com a particularidade de que o petróleo um dia poderá acabar, enquanto os dados se multiplicam a cada segundo”⁹³. Afirma ainda o matemático inglês que, assim como o petróleo precisa ser refinado, os dados, quando analisados, são uma ferramenta poderosíssima, permitindo tomadas de decisões eficientes. Como afirma BELLEIL,⁹⁴ “Diz-me quem és, lucrarei o suficiente para te poder oferecer gratuitamente este serviço”⁹⁵.

Na verdade, na atualidade, os dados pessoais são o maior ativo e a matéria-prima mais valiosa, sendo por isso muito apetecida pelas empresas de diferentes áreas. Por isso, o seu tratamento deve respeitar, como anteriormente referido, os direitos dos titulares e os princípios do seu tratamento, como o consentimento, a limitação do fim para que foi originariamente recolhida, assim como o direito de oposição⁹⁶ como forma de colocar barreiras necessárias à comercialização deste tipo de informação.

Entretanto, numa economia com um mercado sem barreiras alfandegárias de qualquer espécie, em que os dados pessoais são a matéria-prima mais comercializável e rentável, os fornecedores de serviços procuram recolher esses dados de maneira ainda mais sistematizada, para melhor conhecer o perfil dos utilizadores e facilitarem a personalização dos serviços. As empresas tendo estas e outras informações vão poder elaborar os perfis dos titulares de dados, que são consumidores, podendo desta forma personalizar os seus serviços e poder praticar o marketing *one to one*.

Estas práticas, próprias da atual “economia de vigilância”, com os dados a serem transformados em matéria-prima para a criação de perfis de comportamento, de consumo e de opções culturais e políticas, evidenciam que nem toda a recolha e análise de dados são realizadas em respeito ao equilíbrio que deve existir “entre os interesses relativos ao processo económico e o desenvolvimento do comércio, que prejudicasse a defesa e respeito pelos direitos fundamentais das pessoas singulares”⁹⁷ como cita o autor AMADEU GUERRA na sua obra “Informática e Privacidade”.

⁹² CLIVE HUMBY é matemático e empresário na área de dados e estratégias. Autor de vários livros.

⁹³ Cfr. <https://medium.com/project-2030/data-is-new-oil-a-ludicrous-proposition-1d91bba4f294>.

⁹⁴ Cfr. 2001, p. 22.

⁹⁵ Cfr. BELLEIL, A. (2001) – *@-privacidade, o mercado dos dados pessoais: proteção da vida privada na internet*. Lisboa: Instituto Piaget, p. 27.

⁹⁶ Cfr. RGPD (2016, artigos 5º e ss; 12º e ss.).

⁹⁷ Cfr. GUERRA, Amadeu (1999) – *Informática e privacidade – Nova lei de proteção de dados e a lei de proteção de dados no sector de telecomunicações*. Lisboa: Vislis Editores, Lda.

Para isso, entidades com responsabilidades em matéria de proteção dos dados e defesa dos direitos fundamentais, em especial o direito à privacidade, devem atuar e fazer cumprir os normativos existentes sobre esta matéria. Além disso, se os dados podem ser transacionados ou comercializados “o direito à privacidade, [sendo um direito fundamental], não pode ser cedido por quem dele beneficia, nem mesmo mediante uma contrapartida”⁹⁸.

3.3. A TECNOLOGIA COMO AMEAÇA À VIDA PRIVADA

Conforme já se aflorou, a tecnologia pode ser uma grande ameaça à privacidade das pessoas, uma vez que cada vez mais informações pessoais são coletadas e armazenadas digitalmente. As empresas de tecnologia frequentemente coletam dados pessoais dos usuários dos seus serviços, o que pode levar a violações da privacidade se esses dados forem mal utilizados ou divulgados a terceiros sem consentimento⁹⁹.

A vigilância e monitoramento são cada vez mais comuns, seja pelos governos, pelas empresas ou por indivíduos, o que pode levar a uma sensação de invasão de privacidade e pode ter implicações sérias para a liberdade de expressão e associação¹⁰⁰. Muitas vezes, as pessoas não estão cientes de que suas informações estão a ser coletadas ou compartilhadas, o que pode dificultar o exercício do direito à privacidade. Além disso, o consentimento nem sempre é livre e informado, e pode haver pressão social ou económica para concordar com termos e condições que não são favoráveis. O crescente fluxo de informações e dados através de fronteiras internacionais pode levar a questões jurisdicionais e regulatórias complexas, bem como dificultar a aplicação de leis de privacidade em todo o mundo¹⁰¹.

Assim, a vigilância e monitoramento podem interferir nos direitos fundamentais, como a liberdade de expressão, a liberdade de associação e o direito à privacidade, sendo, pois, necessário garantir que qualquer medida adotada seja proporcional e justificada e esteja em conformidade com as leis internacionais dos direitos humanos. Assim, podem ser tomadas uma série de medidas fomentadoras da segurança pública e que ao mesmo tempo respeitem a privacidade e a liberdade individual.

⁹⁸ Cfr. BELLEIL, A. (2001) – *@- privacidade, o mercado dos dados pessoais: proteção da vida privada na internet*. Lisboa: Instituto Piaget, p. 27.

⁹⁹ Cfr. <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2021/08/privacy-technology.pdf>.

¹⁰⁰ Cfr. MARQUES e LOURENÇO (2006) – *Direito da Informática*. (2.^a ed. rev. e act.) Coimbra: Edições Almedina, SA.. pp. 271 a 275.

¹⁰¹ Cfr. MARQUES e LOURENÇO (2006) – *Direito da Informática*. (2.^a ed. rev. e act.) Coimbra: Edições Almedina, SA.. pp. 271 a 275.

É, pois, fundamental implementar medidas minimizadoras.

3.4. IMPLEMENTAÇÃO DE MEDIDAS MINIMIZADORAS

Conforme se referiu, as medidas minimizadoras dos efeitos nefastos advenientes do mundo tecnológico no qual vivemos são essenciais para o bom funcionamento da sociedade moderna.

Neste sentido, é essencial ter leis claras que estabeleçam os limites e os procedimentos adequados para a vigilância e o monitoramento. Essas leis devem ser proporcionais, isto é, devem equilibrar a necessidade de segurança com a proteção dos direitos individuais, evitando medidas excessivas e invasivas.

Por outro lado, estabelecer mecanismos de supervisão independentes, como por exemplo; comissões de controlo, órgãos judiciais especializados, que possam monitorar e avaliar as atividades de vigilância e garantir que sejam conduzidas de acordo com a lei e os direitos fundamentais.

As decisões relacionadas à vigilância e ao monitoramento devem ser analisadas pelos tribunais para garantir que estão em conformidade com a lei e os princípios constitucionais, o que envolve uma análise criteriosa dos pedidos de vigilância, assegurando que sejam necessários e proporcionais.

Noutro âmbito, permitir a coleta apenas das informações estritamente necessárias para fins de segurança pública, evitando a obtenção excessiva e indiscriminada de dados pessoais, promover o uso de criptografia robusta e a segurança de dados para proteger a privacidade das comunicações e ainda garantir que as informações coletadas estejam devidamente protegidas contra acesso não autorizado. Estabelecer também mecanismos de prestação de contas que responsabilizem as autoridades por quaisquer abusos ou violações dos direitos individuais¹⁰².

Por último, fomentar a conscientização e a educação sobre os direitos individuais, a importância da privacidade e a necessidade de equilibrar segurança e liberdade, são algumas soluções que podem ajudar a conciliar a segurança pública com a preservação da privacidade e da liberdade individual.

¹⁰² Cfr. CASTRO, Catarina Sarmento e (2005) – *Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Edições Almedina, p. 18.

4. O ANONIMATO NA SOCIEDADE DIGITAL

4.1. CONSEQUÊNCIAS DO ANONIMATO NA INTERNET

Paralelamente à legislação já referida e, bem assim, aos mecanismos de minimização dos efeitos da exposição excessiva dos cidadãos ao universo *online*, cumpre agora abordar a temática do anonimato.

Ora, de acordo com SAMUEL WARREN e LOUIS BRANDEIS, a privacidade refere-se ao direito de estar só, à privacidade da vida familiar e pessoal, ao anonimato e à manutenção de uma certa distância em relação a desconhecidos¹⁰³.

O anonimato na sociedade digital em Portugal é um assunto bastante complexo e que tem gerado muitos debates nos últimos anos, dado que pode ser uma forma de proteger a privacidade e a liberdade de expressão dos indivíduos, permitindo que estes se manifestem livremente sem medo de retaliação ou perseguição.

No entanto, o anonimato também pode ser utilizado para propagar discurso de ódio, difamação, intimidação e outros tipos de comportamentos abusivos, que podem ter graves consequências para a segurança e bem-estar das pessoas.

Uma das estratégias utilizadas para combater o anonimato na internet é a exigência de identificação dos utilizadores em determinadas situações, como ao criar uma conta em redes sociais ou ao realizar transações financeiras online. No entanto, essa medida pode gerar controvérsias, já que algumas pessoas podem considerar que viola a sua privacidade e liberdade de expressão.

Assim, o anonimato digital é uma questão complexa pois envolve tanto os direitos individuais à privacidade quanto a necessidade de proteger a segurança pública e prevenir crimes.

4.2. OS BENEFÍCIOS DO ANONIMATO NA INTERNET

Como pontos positivos deste anonimato digital, podemos enunciar vários aspetos.

Em primeiro lugar, temos a proteção da privacidade, porquanto o anonimato permite que as pessoas possam expressar-se livremente sem ter que revelar sua identidade ou informações pessoais, o que pode ser um ponto importante para proteger a

¹⁰³ *Apud* MARQUES e LOURENÇO (2006) – *Direito da Informática*. (2.^a ed. rev. e act.) Coimbra: Edições Almedina, SA, pp. 102 a 106.

privacidade e evitar possíveis consequências negativas, como perseguição, retaliação ou discriminação.

Por outro lado, podemos referir a liberdade de expressão, dado que o anonimato também pode promover a liberdade de expressão, uma vez que as pessoas se sentem mais livres para expressar as suas opiniões, ideias e pensamentos sem medo de serem julgadas ou censuradas.

Paralelamente, poderá potenciar a proteção contra ameaças online como assédio, *stalking* ou *cyberbullying*¹⁰⁴.

Por outro lado, o recurso ao anonimato na Internet poderá incentivar a criatividade e a inovação, uma vez que as pessoas se sentem mais livres para experimentar e arriscar sem medo de críticas ou julgamentos alheios.

4.3. O ANONIMATO NA INTERNET EM PORTUGAL E NO MUNDO

Em Portugal, o anonimato digital é uma questão que ainda está em debate e não existe uma legislação específica que o regule.

No entanto, embora não haja uma legislação específica sobre o anonimato digital em Portugal, existem outras leis que podem ser aplicadas a casos relacionados ao uso da internet, como a proteção de dados pessoais, a Lei do Cibercrime ou a proteção contra a difamação. Além disso, a jurisprudência e as decisões judiciais podem desempenhar um papel na definição dos limites e responsabilidades relacionados ao anonimato digital.

A liberdade de expressão é garantida pela Constituição portuguesa e o anonimato pode ser uma forma de proteger essa liberdade.

De acordo com a Constituição portuguesa, todos os cidadãos têm direito à liberdade de expressão e informação, bem como o direito de manifestar o seu pensamento de forma livre, sem censura e sem prejuízo de eventual responsabilidade civil ou criminal, isto é, os indivíduos têm o direito de se expressar livremente, mesmo anonimamente, desde que não violem os direitos de outras pessoas ou a legislação vigente.

¹⁰⁴ Cfr. MARTINS, L. M. (2017) – *A tutela jurídica da privacidade e do sigilo na era digital: Doutrina, Legislação e Jurisprudência*. In Revista de Investigações constitucionais. (Vol. IV), Curitiba, N.º 3, pp. 167-200.

No mundo, a legislação sobre o anonimato digital varia de país para país. Alguns países permitem o uso do anonimato na internet, enquanto outros impõem restrições e exigem que os usuários revelem a sua identidade.

Assim, algumas jurisdições proíbem explicitamente o anonimato na internet, como o caso da China, que exige que todos os utilizadores de redes sociais e fóruns de discussão revelem as suas identidades reais¹⁰⁵.

Por outro lado, outros países têm leis que regulam o uso do anonimato online em determinadas situações, como em transações financeiras ou em casos de assédio.

Nos Estados Unidos, por exemplo, o uso do anonimato é protegido pela Primeira Emenda da Constituição, a qual garante a liberdade de expressão¹⁰⁶. No entanto, as empresas de internet e os provedores de serviços online podem ser obrigados a fornecer informações de identificação dos utilizadores em casos de crimes cibernéticos ou violações de direitos autorais.

No que respeita à jurisprudência portuguesa, as decisões judiciais em Portugal têm reconhecido que o anonimato digital não é um direito absoluto e que os utilizadores da internet devem respeitar os direitos fundamentais de terceiros, como a reputação, a honra e a privacidade. Assim, as pessoas que cometem crimes na internet utilizando pseudónimos ou perfis falsos podem ser identificadas e responsabilizadas criminalmente pelos seus atos, quebrando-se o véu do anonimato.

4.4. JURISPRUDÊNCIA INTERNACIONAL – O ANONIMATO NA INTERNET

Existem diversas decisões judiciais em vários países que abordam o tema do anonimato digital e o seu impacto no Direito.

Em primeiro lugar, podemos referir o caso TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, VON HANNOVER v. GERMANY, de 24 de junho de 2004¹⁰⁷, no qual o tribunal decidiu que as celebridades não têm um direito absoluto à privacidade e que a liberdade de expressão da imprensa pode prevalecer em casos de interesse público.

Paralelamente, podemos referir o caso SUPREME COURT OF THE UNITED STATES, DOE v. REED, de 24 de junho de 2010. Neste caso concreto, da apreciação

¹⁰⁵ Cfr. <https://www.terra.com.br/byte/internet/china-decreta-fim-do-anonimato-dos-usuarios-de-redes-sociais,3c29fe32cdbda310VgnCLD200000bbcceb0aRCRD.html>.

¹⁰⁶ Cfr. <https://www.freedomforum.org/first-amendment-protects-anonymous-speech-online/>

¹⁰⁷ Cfr. <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/02/Von-Hannover-vs.-Alemanha-II.docx.pdf>.

de toda a prova produzida o tribunal decidiu que os signatários de uma petição para colocar uma lei em votação pública não tinham o direito de permanecer anónimos, pois a transparência do processo eleitoral era um interesse legítimo do Estado¹⁰⁸.

Mais tarde surgiu o caso SONY MUSIC ENTERTAINMENT v. DOES 1-40 (EUA, 2011), no qual a SONY MUSIC processou um grupo de indivíduos que, utilizando pseudónimos, fizeram o *download* ilegal de músicas da empresa e as compartilharam na internet. A empresa obteve uma ordem judicial que obrigou o provedor de internet a divulgar as identidades dos utilizadores, demonstrando que o anonimato não é um direito absoluto e pode ser superado em casos de violação de direitos autorais¹⁰⁹.

Por outro lado, podemos referir o caso GOOGLE SPAIN v. MARIO COSTEJA GONZÁLEZ (Espanha, 2014), no qual um cidadão espanhol processou o Google e o jornal La Vanguardia por publicar uma notícia sobre uma sua dívida de 30 anos atrás. O Tribunal de Justiça da União Europeia decidiu que os indivíduos têm o direito de solicitar a remoção de informações pessoais obsoletas ou irrelevantes dos resultados de pesquisa do Google, mesmo que publicadas anteriormente com consentimento¹¹⁰.

No ano seguinte, temos o caso TRIBUNAL EUROPEU DOS DIREITOS HUMANOS, DELFI AS v. ESTONIA, de 16 de junho de 2015, no qual o tribunal decidiu que um portal de notícias *online* era responsável pelos comentários difamatórios postados por utilizadores anónimos no seu site, dado que não havia tomado medidas razoáveis para prevenir ou remover o conteúdo ilegal¹¹¹.

Ainda no mesmo ano, temos o caso FACEBOOK IRELAND LTD v. MAX SCHREMS, no qual o ativista austríaco MAX SCHREMS processou o Facebook por violação de privacidade e transferência de dados pessoais para os Estados Unidos, onde não existem proteções adequadas. O Tribunal de Justiça da União Europeia decidiu que os utilizadores da UE têm o direito de exigir que os seus dados pessoais sejam removidos de plataformas digitais e que o anonimato é um direito fundamental para proteger a privacidade na internet¹¹².

Paralelamente, temos também o caso CORTE SUPREMA DA ÍNDIA, PUTTASWAMY v. UNION OF INDIA, de 24 de agosto de 2017, no qual o tribunal reconheceu o direito

¹⁰⁸ Cfr. <https://supreme.justia.com/cases/federal/us/561/186/>.

¹⁰⁹ Cfr. <https://casetext.com/case/sony-music-entertainment-inc-v-does-1-40>.

¹¹⁰ Cfr. <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>.

¹¹¹ Cfr. [https://hudoc.echr.coe.int/fre#%7B%22itemid%22:\[%22002-8960%22\]%7D](https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22002-8960%22]%7D).

¹¹² Cfr. <https://globalfreedomofexpression.columbia.edu/cases/maximilian-schrems-v-facebook-ireland-limited/>

fundamental à privacidade como um direito autónomo protegido pela Constituição da Índia, incluindo a privacidade na internet¹¹³.

Ora, da análise das diversas decisões jurisprudenciais enunciadas, verificamos que o direito ao anonimato na internet é reconhecido em muitos países como um direito fundamental, mas não é um direito absoluto. Assim, os tribunais geralmente avaliam a importância do interesse da privacidade em relação a outros interesses legítimos, como o interesse do Estado em investigar crimes ou a proteção de direitos autorais. Neste âmbito, os acórdãos analisados revelam a complexidade e a evolução das questões de anonimato, privacidade e proteção de dados na esfera legal e cada decisão enfatiza a importância de equilibrar os direitos individuais com o interesse público e a liberdade de expressão, ao mesmo tempo em que reconhece a crescente relevância da privacidade e do direito ao anonimato na Era digital.

¹¹³ Cfr. <https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/>.

CAPÍTULO II – A REVOLUÇÃO NA INTIMIDADE, NO DIREITO À IMAGEM E NO RECONHECIMENTO FACIAL

5. A TECNOLOGIA DO RECONHECIMENTO FACIAL

Conforme já fomos referindo, a evolução tecnológica tem sido exponencial nos últimos anos, atingindo patamares nunca antes sequer imaginados.

Ora, os sistemas de reconhecimento são um exemplo claro desta evolução.

Os sistemas de reconhecimento biométrico operam remotamente sem conhecimento prévio da presença da pessoa em causa e coletam informações biométricas (inclusive através da identificação da imagem do rosto), cotejam esses dados com uma amostra existente ou banco de informações sem demora substancial, sendo usados com o propósito específico de determinar a identidade de um indivíduo.

Através das tecnologias de identificação facial, é viável empregar uma base de dados contendo imagens e vídeos, tais como aquelas presentes em documentos de identidade, sistemas de vigilância e outras fontes de informação e essa abordagem permite a identificação de pessoas no mundo real, seja em situações reais ou em registos visuais, como filmes e imagens de segurança. Ora, o facto de os sistemas de identificação biométrica e de reconhecimento facial possuírem estas características torna-os ferramentas muito interessantes para agentes públicos e privados¹¹⁴.

5.1. CAPACIDADES TÉCNICAS ENVOLVIDAS

Devido à sua natureza voltada para supervisão e regulação, as técnicas de identificação por reconhecimento facial abrangem um vasto leque de aplicações, abrangendo áreas como centros de compras, aeroportos, estádios, espetáculos musicais e policiamento.

Assim, as capacidades da tecnologia de reconhecimento facial igualmente abarcam a capacidade de prevenir atividades criminosas, detetar infratores, localizar crianças desaparecidas e contribuir para metas de segurança nacional, pelo que, em virtude desses atributos, não é de se estranhar que as forças policiais também demonstrem um profundo interesse na adoção desses sistemas.

¹¹⁴ Cfr. RAPOSO, Vera Lúcia (2022) – *(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation*, in *Information & Communications Technology Law*, 2022, disponível em <https://doi.org/10.1080/13600834.2022.2054076>.

Os sistemas de identificação biométrica são habitualmente vistos como ferramentas importantes para a prevenção de crimes. O seu uso para fins policiais está assim relacionado com a atividade de segurança pública do estado (incluindo – uma outra das aplicações de inteligência artificial que podem ser usadas pelas autoridades policiais – o chamado “policiamento preditivo” ou “previsão policial”¹¹⁵) e não com a atividade estatal envolvendo a perseguição de crimes¹¹⁶.

Assim, é inegável que a aplicação de sistemas de reconhecimento biométrico e tecnologias de identificação facial para fins de combate ao crime por parte do Estado é uma perspectiva viável. Adicionalmente, é importante ressaltar que essas abordagens podem ser consideradas ferramentas investigativas valiosas, capazes de auxiliar na identificação de suspeitos por meio da comparação de suas imagens ou fotos com aquelas armazenadas em bancos de dados, principalmente os de acesso público. Contudo, é fundamental reconhecer que a viabilidade dessa abordagem precisa de ser analisada à luz dos princípios legais e garantias fundamentais estabelecidos pelo Direito Processual Penal. Nesse sentido, a discussão sobre a utilização de sistemas de identificação biométrica e tecnologias de reconhecimento facial deve ser primeiramente explorada no contexto da segurança pública, considerando cuidadosamente as implicações jurídicas e os direitos individuais.

Além disso, é importante destacar que a adoção dessas tecnologias para fins de investigação criminal também deve ser equilibrada com preocupações relacionadas à privacidade, proteção de dados e possíveis abusos. Portanto, o debate sobre o uso desses sistemas deve envolver não apenas as autoridades policiais, mas também especialistas em Direito, ética e tecnologia, bem como a sociedade como um todo.

5.2. COMO FUNCIONA O PROCEDIMENTO

Para proceder ao reconhecimento facial, conforme nos refere PENTLAND e CHOUDHURY, é essencial que o computador aprenda o que é um rosto, o qual, em geral, obtém-se treinado um algoritmo, normalmente uma rede neural profunda, através do fornecimento de um elevado número de fotografias contendo rostos de pessoas em situações típicas¹¹⁷.

¹¹⁵ Sobre o policiamento preditivo ou previsão policial, *vide* EGBERT, Simon e LESSE, Matthias *Criminal futures: predictive policing and everyday police work*, London, New York, Routledge, 2021

¹¹⁶ Cfr. Ponto 24 da Resolução do Parlamento europeu, aprovada em 6 de outubro de 2021 (disponível em <https://eur-lex.europa.eu/legal-content/PT/txt/Pdf/?uri=celeX:52021IP0405&from=Pt>)

¹¹⁷ Cfr. PENTLAND, A., & CHOUDHURY, T. (2000) – *Face Recognition for Smart Environments. Computer*, 33, pp. 50-55.

Assim, sempre que uma imagem é apresentada ao algoritmo, esta estima a localização do desse rosto e, com a repetição, o algoritmo vai melhorar a sua fineza, vai realizar um acerto, a vai acabar por dominar a arte de detetar um rosto humano¹¹⁸. Surge o reconhecimento humano que pode operar de diversas maneiras, mas é comum usar uma grande rede neural à qual se fornece uma multiplicidade de retratos. Antes disso, os algoritmos mapearão cada rosto, medindo distâncias entre os olhos, entre o nariz e a boca etc. A rede vai gerar um vetor para cada rosto, uma sequência de números que o identifica de forma única dos demais¹¹⁹.

O grande desempenho da máquina depende, no entanto de vários fatores: uma fotografia nítida e clara integrada num banco de dados que integra imensas fotografias de alta qualidade. Neste contexto, a tecnologia apresenta ainda grande dificuldade em lidar com pessoas com rostos com geometrias bastante idênticas.

Os dados biométricos que são utilizados com êxito e com eficácia na investigação científica são um elemento-chave da ciência forense e um elemento precioso dos sistemas de controlo de acessos. Podem contribuir para aumentar o nível de segurança e para que os procedimentos de identificação e autenticação sejam fáceis, rápidos e práticos.

No passado, a utilização desta tecnologia era cara e, devido a esta limitação de ordem económica, o impacto sobre a proteção dos dados pessoais era reduzido.

No entanto, a situação alterou-se drasticamente nos últimos anos.

Graças aos avanços tecnológicos, o espaço de armazenamento e a capacidade de processamento informático são acessíveis, possibilitando a existência de álbuns com milhões e milhões de fotografias em linha e em redes sociais. Os leitores de impressões digitais e os dispositivos de videovigilância são hoje aparelhos com preços acessíveis.

Por outro lado, o desenvolvimento destas tecnologias contribuiu para que muitas operações sejam mais práticas, para a resolução de muitos crimes e para que os sistemas de controlo de acessos sejam mais fiáveis. No entanto, a usurpação de identidade passou a ser um problema recorrente do dia-a-dia.

¹¹⁸ Cfr. SADIN, Eric (2015) – *La vie algorithmique: critique de la raison numérique*. Paris: L'Echappée.

¹¹⁹ Cfr. YANG, X., & LV, F. (2011) – *The design of a face recognition system based on skin color and geometrical characteristics*. 2011 International Conference on Image Analysis and Signal Processing, pp. 276-279.

A tecnologia de biometria facial é um tipo de autenticação biométrica, cujo nível de segurança e assertividade depende diretamente da qualidade da base de dados de imagens (fotos e impressões digitais) e da tecnologia que está a ser utilizada, o que envolve desde quantos pontos da face são verificados, luminosidade, quantidade de pixels entre os olhos e demais itens que possam ajudar a diminuir eventual “falso positivo”.

É importante destacar que, apesar de trazer benefícios, esse tipo de tecnologia traz a discussão sobre a exatidão dessa análise de imagem, pois as tecnologias de reconhecimento facial são tecnologias de inteligência artificial, cujos resultados, como todo modelo estatístico de probabilidade, não são exatamente precisos.

Destaca-se que o atual entusiasmo no que diz respeito à pesquisa e desenvolvimento de tecnologias de inteligência artificial teve início aproximadamente em 2010 e foi movido pelos seguintes fatores: criação de métodos estatísticos e probabilísticos cada vez mais sofisticados; a disponibilidade de ampla e crescente quantidade de dados; a acessibilidade a um enorme poder computacional; e a transformação cada vez maior dos ambientes com as novas tecnologias de informação, como a automação residencial e a criação de cidades inteligentes¹²⁰.

Tais fatores possibilitaram o crescimento exponencial da criação e aperfeiçoamento de sistemas de IA nos últimos anos, não aparentando ser uma tendência passageira.

À medida que a adoção de sistemas de reconhecimento facial continua a crescer em todo o mundo, há uma séria preocupação crescente de que essa tecnologia possa prejudicar os direitos fundamentais de privacidade e como ela pode ser mantida sob controle.

Ora, o reconhecimento facial é uma categoria de *software* biométrico que mapeia matematicamente as características faciais de um indivíduo e armazena os dados como uma impressão facial. O *software* usa algoritmos de aprendizagem profunda para comparar uma captura ao vivo ou imagem digital com a impressão facial armazenada para verificar a identidade de um indivíduo e identifica 80 pontos nodais num rosto humano¹²¹. Nesse contexto, os pontos nodais são pontos finais usados para medir variáveis do rosto de uma pessoa, como comprimento ou largura do nariz, profundidade das órbitas oculares e formato das maçãs do rosto. O sistema funciona

¹²⁰ Cfr. FLORIDI et al., 2017

¹²¹ Cfr. SADIN, Eric (2015) – *La vie algorithmique: critique de la raison numérique*. Paris: L'Echappée.

capturando dados de pontos nodais numa imagem digital do rosto de um indivíduo e armazenando os dados resultantes como uma impressão facial. A impressão facial é então usada como base para comparação com dados capturados de faces numa imagem ou vídeo¹²².

Desde o seu aparecimento, em 1960, a tecnologia de reconhecimento facial vem sendo lapidada para chegar à sua melhor forma e suportar uma maior aplicação prática.

Assim, podemos afirmar que a tecnologia de biometria facial é um tipo de autenticação biométrica, cujo nível de segurança e assertividade depende diretamente da qualidade da base de dados de imagens (fotografias e impressões digitais) e da tecnologia que está a ser utilizada.

De acordo com WELINDER, a tecnologia de reconhecimento facial visa combinar as desenvolvidas percepções humanas com a imensa capacidade de processamento e armazenamento dos computadores¹²³.

E, por seu turno, KIRILL LAVASHOV salienta que “A tecnologia de reconhecimento facial utiliza uma câmara fotográfica em conjunto com software de reconhecimento facial. Este software consegue detetar e isolar rostos humanos captados pela câmara e analisá-los através de um algoritmo que extrai características identificativas¹²⁴. O algoritmo identifica e mede “pontos nodais” no rosto, definidos pelos picos e vales que compõem as características faciais humanas. Utilizando estas medições, o algoritmo determina características identificativas individuais, como a distância entre os olhos, a largura do nariz, a forma das maçãs do rosto e o comprimento da linha da mandíbula”¹²⁵.

¹²² Cfr. <https://www.techtarget.com/searchenterpriseai/definition/facial-recognition>.

¹²³ Cfr. WELINDER, Yana (2012) – *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks* (July 16, 2012). Harvard Journal of Law and Technology, v. 26, n. 1, p. 170.

¹²⁴ Cfr. BERTOCCHI, Daniela (2012) - *O algoritmo curador: o papel do comunicador num cenário de curadoria algorítmica da informação*. XXI Encontro Anual da Compós.

¹²⁵ “A tecnologia de reconhecimento facial usa uma câmara fotográfica combinado com um software de reconhecimento facial. Este software é capaz de detetar e isolar rostos humanos capturados pela câmara e analisá-los usando um algoritmo que extrai e identifica características. O algoritmo identifica e mede ‘pontos nodais’ na face, que são definidos pelos picos e vales que compõem as características faciais humanas. Utilizando estas medições, o algoritmo determina as características de identificação de um indivíduo, tais como a distância entre os olhos, largura do nariz, de forma maçãs do rosto, e o comprimento da linha da mandíbula”. LEVASHOV, Kirill (2013) – *The Rise of a New Type of Surveillance for Which the Law Wasn’t Ready*. Columbia Science and Technology Law Review, v. 15, p. 164, Fall 2013, pp 167-168.

Ora, a face das pessoas constitui uma das biometrias mais aceitáveis, por causa da familiaridade e especialmente porque a aquisição das imagens não é fisicamente intrusiva e tem um grau de fiabilidade elevado.

Neste sentido, SARA SMYTH acrescenta que em 2014 “a precisão dos sistemas já superava a das pessoas, sendo então integrados em sistemas de documentos e sua verificação, como passaportes, cartões de identidade e circuito fechado de televisão.”¹²⁶

Ora, a coleta abrange o processo de planeamento, sendo endereçadas questões tais como a definição da finalidade, origem dos dados, quem irá fazer a coleta, que tipo de informação será necessária, onde serão armazenados, de que forma o titular será comunicado, qual o enquadramento legal para promover o tratamento, bem como os detalhes referentes à combinação com outros conjuntos de dados. Essa etapa também abrange a real transmissão e gravação dos dados¹²⁷.

Por conseguinte, dado que empresas e governos utilizam as informações derivadas da coleta para conduzir vigilância, muitas vezes sem que os titulares tenham sequer o conhecimento de que estão a ser observados e tais entidades também não revelam que tipo de informação é coletada ou compartilhada, verificamos que este desequilíbrio de poder conduz à falta de liberdade e de autonomia para exercer adequado controlo a respeito da coleta, seja porque o sujeito não tem conhecimento, alternativa, ou porque as políticas de privacidade são redigidas em linguagem inacessível¹²⁸.

Especificamente no momento da coleta, os riscos relacionam-se com a realização de vigilância, rastreamento e criação de perfis, com a falta de transparência exercida pelos controladores e da liberdade no exercício do consentimento por parte dos titulares, de acordo com o propósito fixado, comas tentativas de burlar o sistema (*spoofing*)¹²⁹.

O reconhecimento facial utiliza dados enquadrados na categoria de informações biométricas, conforme as definições do artigo 4.º/14 do RGPD e artigo 3º/13 da

¹²⁶ Cfr. Smyth, *Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control*, pp. 24 e 25.

¹²⁷ Cfr. TAMÒ-LARRIEUX, *Designing for Privacy and its Legal Framework*, pp. 149–5.

¹²⁸ Cfr. TAMÒ-LARRIEUX, *Designing for Privacy and its Legal Framework*, pp. 8.

¹²⁹ Cfr. Opinion 03/2012 on developments in biometric technologies”, 27 de abril de 2012, https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2012/wp193_en.pdf. E ainda GALBALLY, J., MARCEL, S., & FIERREZ, J. (2014) – *Biometric Antispoofing Methods: A Survey in Face Recognition*. IEEE Access, 2, 1530-1552.

Diretiva UE 2016/680, por abranger elementos resultantes de um tratamento técnico específico relativo a características físicas de uma pessoa singular e que permitem a sua identificação e, por seu turno, os dados biométricos permitem a identificação de um indivíduo com base em facto biológico específico, permanente, relativamente imutável e que dele não pode ser dissociado¹³⁰.

Neste âmbito, o art.º 9.º do RGPD incluiu expressamente a referência aos dados biométricos como categoria especial de dados pessoais. A razão dessa proteção especial vai além de se proibir tratamento discriminatório. De acordo com o Considerando 75 do RGPD, os riscos são vários, como danos físicos, materiais ou imateriais, quando possa haver discriminação, roubo de identidade, perdas financeiras, prejuízo para a reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional, inversão não autorizada de pseudonimização ou quaisquer outros prejuízos importantes de natureza económica e social¹³¹.

A caracterização dos dados biométricos como dados sensíveis atrai proteções específicas. Neste âmbito, o art.º 9º, n.º 1 do RGPD adota por princípio a proibição de tratamento desse tipo de dados pessoais, sendo a autorização vista de modo excecional, nas hipóteses do n.º 2, que inclui o consentimento explícito do titular, o cumprimento de obrigações legais em matéria de legislação laboral, segurança social e proteção social, interesses vitais do titular ou de outras pessoas, no âmbito de atividades legítimas de determinadas organizações, informações manifestamente publicadas pelo titular, defesa de direitos em processos judiciais na função jurisdicional dos tribunais, motivo público importante, medicina laboral, saúde pública ou arquivo público¹³².

Nas hipóteses em que o titular participa da inscrição dos seus dados nos sistemas biométricos, deve ser especificamente comunicado, na forma do artigo 13.º do RGPD, já nesse momento.

Todavia, uma das principais características dos sistemas de reconhecimento facial é sua possibilidade de ser obtido em qualquer lugar e sem contato, tornando tecnicamente possível a realização de identificação das pessoas sem qualquer ação da sua parte ou a localização de seu nome sem que o dono do dispositivo tenha tido

¹³⁰ Facial Recognition - for a debate living up to the challenges”, 15 de Novembro de 2019, <https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf>.

¹³¹ Cfr. Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados.

¹³² Cfr. Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados.

qualquer relacionamento com o titular. Já quando os dados não são recolhidos junto do titular, aplicam-se as regras e requisitos indicados no artigo 14º do RGPD, para a satisfação do princípio da transparência. Os mesmo usos legítimos e bem definidos podem ter sérias consequências em caso de erro ou ciberataques, o que torna fundamental garantir a segurança dos dados biométricos.

Nesse contexto, a Opinião 03/2012 do GT29 recomenda a observância das seguintes medidas técnicas: 1) a preferência pelos modelos biométricos ao invés dos dados armazenados em bruto, permitindo sua renovação e revogação em caso de quebra de segurança; 2) o armazenamento encriptado; e 3) preferencialmente descentralizado, admitindo-se o contrário quando presentes necessidades objetivas para propósitos específicos, com a adoção de medidas de segurança para evitar reutilização indevida da identidade; 4) adoção de medidas para evitar a fraude ao sistema; 5) métodos automáticos de apagamento¹³³.

5.3. COMO É REALIZADA A CAPTAÇÃO DE IMAGEM PESSOAL

Poderemos assumir que todas as fotografias que são colocadas na internet são suscetíveis de apropriação por quem controla o algoritmo?¹³⁴ Mesmo aquelas que são arquivadas? Mesmo aquelas que têm outros fins?

A resposta a esta questão é negativa, quando consideramos os moldes em que o Direito à Imagem se encontra reconhecido pelo preceito contido no art.º 79.º do CC., bem como atendendo à natureza dos direitos, liberdades e garantias pessoais que a CRP lhe reconhece.

O segundo – que desponta em relação a qualquer base de dados, mas que aqui adquire especial acuidade tendo em conta o modo geralmente descontrolado como surge, se constitui e se compõe, concerne ao seu destino, na sua essência a quem tem legitimidade para aceder e, mais, que uso está permitido ser lhe dado? Em especial quando se reconheça a existência de um *right to publicity*, justificar a utilização de imagens alheias sem o devido consentimento do seu titular não apenas infringirá um direito de personalidade como transgredirá também um monopólio de exploração económica de que ele juridicamente goza¹³⁵.

¹³³ Cfr. Opinion 03/2012 on developments in biometric Technologies.

¹³⁴ Cfr. SADIN, Eric (2015) – *La vie algorithmique: critique de la raison numérique*. Paris: L'Echappée.

¹³⁵ Imagem proporcionada pelo right to publicity, tendo em vista reservar vários benefícios económicos.

O terceiro, referente ao defeituoso funcionamento do sistema, o relativo à sua fiabilidade. Uma errada identificação pode contender profundamente com direitos fundamentais e com princípios jurídicos elementares, o risco da base de dados não se encontrar devidamente construída, por não ter suficientes amostras, por não ser representativa da realidade, deve correr por conta de quem?

Assim, tanto do ponto de vista jurisprudencial como legal, a questão não parece poder ser ultrapassada, para já, através por exemplo, do recurso ao *three data protection tests*, extraíveis a partir do n.º 2 do artigo 8.º da Convenção Europeia dos Direitos do Homem (ao enumerar as condições de que depende a legítima ingerência no gozo de um direito protegido através dele: *the purpose test*; *the necessity test*; *the balancing test* ou ainda mediante o manuseio dos princípios orientadores, contidos nos n.ºs 2 e 3 do art.18 da CRP), com especial atenção, na necessidade, na proporcionalidade e na adequação da restrição (ao direito à imagem).

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

5.4. A CONSTITUIÇÃO DE UMA BASE DE DADOS E A REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Como salienta HOERNES, a constituição de uma base de dados supõe que os seus titulares cedam à entidade que os gere para um determinado fim¹³⁶. No entanto, a construção de uma base de dados para uma fonte de reconhecimento técnico, não pode, pela sua própria natureza, dar-se do mesmo modo. Se, por outra razão não for, em virtude de tal se mostrar verdadeiramente impraticável ou mesmo inexecutável,

¹³⁶ Cfr. HOERNES, G. (1972) – *Generalized view of a Data Base*, pp. 147-154.

resta assim pretender que a lei, quando decidir intervir, o faça para fixar em termos precisos e rigorosos os fins a que as FRT se podem destinar.

Neste sentido, a proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento de IA¹³⁷) e altera determinados atos legislativos da União, proíbe explicitamente a “utilização de sistemas de identificação biométrica à distância em tempo real em espaços públicos para efeitos de manutenção da ordem pública”, salvo as seguintes exceções: “se a utilização for estritamente necessária para alcançar um dos seguintes objetivos:”1.) investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas; 2.) prevenção de uma ameaça específica, substancial e iminente à vida ou segurança física de pessoas singulares ou de ataque terrorista, 3.) a deteção, localização identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no n.º 2, n.º 2 da Decisão Quadro 2002/584/JAI do Conselho.

A proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento de IA), sendo uma iniciativa importante para enfrentar os desafios éticos e de privacidade associados ao uso crescente de tecnologias como o reconhecimento facial. A proibição explícita da utilização de sistemas de identificação biométrica à distância em tempo real em espaços públicos para efeitos de manutenção da ordem pública é uma medida significativa para proteger os direitos fundamentais dos cidadãos¹³⁸.

Essa proibição, no entanto, é equilibrada por exceções que permitem o uso de tais tecnologias em circunstâncias estritamente necessárias e bem definidas.

As exceções, como investigação de crianças desaparecidas, prevenção de ameaças iminentes à vida ou segurança física das pessoas e combate ao terrorismo, demonstram a importância de equilibrar a segurança pública com a proteção da privacidade e dos direitos individuais.

É louvável que a proposta de Regulamento de IA esteja alinhada com a preocupação de preservar os valores essenciais da democracia e dos direitos humanos na Era da tecnologia avançada. A implementação dessas regras harmonizadas será fundamental

¹³⁷ Cfr. <https://www.europarl.europa.eu/news/pt/headlines/society/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>.

¹³⁸ <https://www.europarl.europa.eu/news/pt/headlines/society/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>

para garantir que a inteligência artificial seja utilizada de forma responsável, transparente e justa, preservando a dignidade e a privacidade dos cidadãos.

No entanto, é essencial que a legislação seja acompanhada de um rigoroso controlo e fiscalização para garantir o cumprimento das normas e evitar abusos. Além disso, a pesquisa contínua e a atualização das regulamentações serão necessárias para acompanhar o rápido desenvolvimento tecnológico e os novos desafios que surgem na área de inteligência artificial. A proposta de Regulamento de IA é um passo importante em direção à regulamentação ética do uso de reconhecimento facial e outras tecnologias de inteligência artificial na União Europeia. Ao estabelecer restrições claras e exceções bem definidas, visa-se encontrar um equilíbrio entre a segurança pública e a preservação dos direitos e liberdades fundamentais dos cidadãos.

Espera-se, assim, que essa legislação sirva de exemplo para outras jurisdições enfrentarem os desafios éticos e de privacidade relacionados à IA, promovendo um futuro mais justo e responsável no campo da tecnologia avançada.

5.5. IMPACTO DA UTILIZAÇÃO DE SISTEMAS BIOMÉTRICOS DE IDENTIFICAÇÃO E TECNOLOGIAS DE RECONHECIMENTO FACIAL

As apreensões levantadas sobre a utilização de sistemas biométricos de identificação e tecnologias de reconhecimento facial geralmente decorrem da convergência de duas ideias distintas, ainda que intimamente relacionadas.

Primeiramente, temos as particularidades singulares desses tipos de sistemas tecnológicos.

Em segundo lugar, destacam-se os efeitos possíveis desses sistemas e tecnologias sobre os direitos fundamentais das pessoas.

Ora, uma primeira fonte de inquietação refere-se às características técnicas e níveis de precisão dos sistemas e tecnologias¹³⁹.

¹³⁹ Cfr. HADDAD, Gabrielle M. (2021) – *Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom*, in Vanderbilt Journal of Entertainment and Technology Law, 23, 4, pp. 891-918. Porém, fazendo menção a possíveis mecanismos para garantir a precisão das tecnologias de reconhecimento facial, v. RAPOSO, Vera Lúcia (2022) – *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, in European Journal on Criminal Policy and Research, Springer online, 01 June 2022, disponível em <https://link.springer.com/content/pdf/10.1007/s10610-022-09512-y.pdf>.

De um lado, pode-se abordar a proliferação da tecnologia de reconhecimento facial e os desafios relacionados à supervisão humana eficaz durante a implementação.

Por outro lado, é válido mencionar as preocupações de segurança associadas à coleta e retenção de dados de identificação facial, combinadas com o risco de violação e uso inadequado dessas informações.

Adicionalmente, destaca-se o perigo de ocorrência de falhas nas tecnologias de reconhecimento facial, seja por não serem capazes de identificar um rosto presente em uma imagem, seja por identificarem erroneamente uma estrutura não facial como sendo um rosto real.

Esta possibilidade de erro levou empresas de renome a saírem do mercado de tecnologias de reconhecimento facial¹⁴⁰.

Além disso, é importante acrescentar que a falta de regulamentação e padrões consistentes também contribui para as preocupações. A ausência de uma estrutura sólida de gestão e supervisão pode agravar os desafios relacionados à precisão, segurança e ética no uso dessas tecnologias de identificação biométrica.

Noutro âmbito, outras fontes de preocupações relacionam-se com os direitos fundamentais, como já referimos neste estudo.

Por um lado, é perceptível a tendência de coleta e análise contínua de dados, incluindo informações pessoais, por meio de dispositivos como câmaras de vigilância e veículos autônomos, aproveitando o avanço da tecnologia de inteligência artificial, como o reconhecimento facial, dado que, este cenário pode resultar em implicações mais intrusivas para a privacidade individual e a segurança dos dados.

Por outro lado, especialistas expressaram de maneira enfática a sua preocupação de que a tecnologia de reconhecimento facial possa apresentar índices significativos de falsos positivos/negativos, sendo suscetível que possa resultar em diversas formas de discriminação contra certos segmentos populacionais, por exemplo, mostrando menos precisão para mulheres e indivíduos não brancos do que para homens brancos.

Especificamente, no contexto da aplicação coercitiva da lei, existe um alto risco de ocorrência de tratamento discriminatório. Além disso, são identificados vários riscos relacionados ao uso potencialmente generalizado da tecnologia de reconhecimento

¹⁴⁰ Cfr. MADIEGA, Tambiama e MILDEBRATH, Hendrik, Regulating facial recognition in the EU.

facial. Existe uma considerável probabilidade de que esses sistemas sejam empregados para propósitos além daqueles inicialmente autorizados e supervisionados, o que pode resultar em: (i) comprometimento da capacidade de se movimentar no espaço público de maneira anônima; (ii) imposição de conformidade prejudicial ao livre-arbítrio; (iii) interferência nas liberdades religiosas e direitos das crianças; (iv) impacto negativo na liberdade de expressão e opinião, afetando o direito de reunião e associação; (v) influência substancial no comportamento social e psicológico dos cidadãos; e (vi) realce de questões éticas cruciais.

De acordo TAMBIA MA DIEGA HENDRIK MILDEBRATH¹⁴¹, considerando tais complexidades e implicações, torna-se necessário conduzir um debate aprofundado e abrangente sobre a implementação e regulação das tecnologias de reconhecimento facial, tendo em vista a salvaguarda dos direitos individuais e a promoção de uma sociedade justa e equitativa¹⁴².

5.6. VANTAGENS DO SISTEMA

A vantagem primordial destas tecnologias é a inegável contribuição para a realização da justiça e para a descoberta da verdade material ¹⁴³.

Neste sentido, CLIVE NORRIS considera que “esta forma de vigilância” torna-se mais democrática uma vez que todos ficam igualmente sujeitos à vigilância, livre de restrições temporais como no caso da presença humana¹⁴⁴.

Não podemos também esquecer o efeito preventivo que podem ter estas tecnologias, uma vez que, sabendo que estamos a ser “vigilados”, o número de crimes poderá diminuir, isto por receio que através deste sistema se venha a descobrir a identidade do autor¹⁴⁵.

Em termos práticos, acrescenta-se o facto de que com esta tecnologia existe uma desnecessidade de mobilização de um grande numero de agentes, sendo estes mesmos substituídos por câmaras e tecnologias capazes de proceder à identificação

¹⁴¹ Cfr. MADIEGA, Tambiama e MILDEBRATH, Hendrik, *Regulating facial recognition in the EU*, cit., pp. 6-9.

¹⁴² Cfr. MADIEGA, Tambiama e MILDEBRATH, Hendrik, *Regulating facial recognition in the EU*, cit., pp. 6-9.

¹⁴³ Cfr. FIDALGO, Sónia, “A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo” p. 130.

¹⁴⁴ Cfr. NORRIS, Clive (2003) – From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control, in “*Surveillance as Social Sorting. Privacy, risk, and digital discrimination*”, Routledge, David Lyon, pp. 263-266, disponível em https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf.

¹⁴⁵ Ibidem.

de pessoas¹⁴⁶, o que é positivo, uma vez que os agentes quando se encontram a patrulhar não conseguem constantemente vigiar o mesmo local¹⁴⁷.

Ademais, e sendo um fator a favor da utilização destas tecnologias, está o facto de os dados biométricos serem intransmissíveis de pessoa para pessoa, uma vez que assim é muito difícil que estes sejam imitados. Destarte, torna-se este um procedimento mais seguro do que o uso de palavras-passe e códigos de acesso, que podem ser perdidos, esquecidos e usados por outrem que não seja o seu titular¹⁴⁸.

Por outro lado, o reconhecimento facial tem indiscutivelmente muitos benefícios. Uns mais prosaicos, como eliminar filas nos aeroportos; outros muito relevantes, como encontrar pessoas desaparecidas ou vítimas de tráfico humano.

Neste sentido, o aeroporto do Changi, Singapura, está a introduzir Smart Gates com capacidade de RF para reduzir filas de espera e agilizar o controlo dos passageiros eliminando o passaporte. Os navios de cruzeiro também estão a adotar a tecnologia de RF para que os passageiros possam fazer compras sem ter de levar cartões de crédito. Nos Estados Unidos, a adoção do RF para verificação de cartas de condução permite identificar qualquer um, mesmo quando não apresenta documentos de identificação. Na Nova Zelândia o RF está a ser utilizado para controlar jogadores que se autoexcluem de entrar nos casinos. E na Índia, onde todos os anos desaparecem milhares de crianças é possível, através de sistemas de Reconhecimento Facial, encontrar essas crianças desaparecidas. Por todo o mundo, as forças policiais estão a trabalhar na adoção do sistema de RF em situações bastante concretas como a identificação de suspeitos de crimes ou em espetáculos ao vivo, permitindo o controlo de todos os presentes em tempo real, adeptos violentos de futebol incluídos. Mas isto é só o começo¹⁴⁹.

À medida em que crescem as aplicações baseadas em RF e o interesse em adoptá-las aumenta, a concorrência no setor da IA aplicada ao RF também aumenta tornando a sua disseminação irreversível como parte do nosso quotidiano.

¹⁴⁶ Cfr. NISSENBAUM, Helen e INTRONA, Lucas, “*Facial Recognition Technology. A survey of Policy and Implementation Issues*”, The Center for Catastrophe Preparedness and Response, pp.20-21, disponível em https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues.

¹⁴⁷ *Ibidem*.

¹⁴⁸ Cfr. RODRIGUES, Sara Raquel dos Santos, “*Desenvolvimento de um Sistema de Reconhecimento Facial*”, pp. 66-67.

¹⁴⁹ Cfr. <https://observador.pt/opiniaao/reconhecimento-facial-democracia-4-0-0/>.

Neste âmbito, a China não está apenas a introduzir o sistema em todo o território como já o está a exportar, nomeadamente para outros países asiáticos e africanos enquanto as grandes tecnológicas americanas, que também têm os seus próprios sistemas de RF, começam a disseminá-los nas sociedades ocidentais.

5.7. ASPETOS DIFERENCIADORES E FRAGILIDADES

A grande diferença dos sistemas de reconhecimento fácil com os primeiros sistemas biométricos está no facto de que o reconhecimento facial não requer permissão.

No que respeita às impressões digitais, dificilmente se obtém as mesmas de alguém sem a sua aceitação e no caso do reconhecimento de voz, conforme salientam ALEKSIC e KATSAGGELOS, só a gravação de centenas de horas permite dar alguma fiabilidade ao sistema¹⁵⁰. Por outro lado, as análises do ADN tornaram-se mais rápidas e economicamente acessíveis a quase todos¹⁵¹.

Ora, como salientam MAGDUM e KURHEBHAGWA, o reconhecimento facial torna tudo bastante mais simples. Qualquer fotografia identificada por nós nas redes sociais já o fez. Até mesmo aqueles que não utilizam as redes sociais são facilmente inseridos no sistema. Qualquer pessoa pode ser identificada por um colega ou por um amigo numa selfie ou numa fotografia de grupo. A partir desse momento, o sistema fica a saber quem somos e vai identificar-nos instantaneamente em todas as outras imagens já existentes nas bases de dados, permitindo reconstruir todos os nossos movimentos passados assim como em todas as imagens futuras, independentemente do nosso conhecimento, independentemente da nossa aceitação¹⁵².

Atualmente, as consequências do reconhecimento facial nas nossas vidas pessoais e sociedade como um todo ainda não estão plenamente compreendidas.

Por conseguinte, como desvantagens do sistema, temos o risco de perda de privacidade e a verdadeira ameaça é a possibilidade de alterar fundamentalmente a estrutura de uma sociedade como a conhecemos hoje. Além disso, a disseminação de sistemas baseados em inteligência artificial terá um impacto significativo na economia,

¹⁵⁰ Cfr. ALEKSIC, P., & KATSAGGELOS, A. (2006) – *Audio-Visual Biometrics. Proceedings of the IEEE*, 94, pp. 2025-2044.

¹⁵¹ Cfr. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf

¹⁵² Cfr. MAGDUM, N., & KURHEBHAGWAN, S. (2017) – *Face Recognition by GroupWise Registration Technique*. *International Journal of Advance Research and Innovative Ideas in Education*, 3, pp. 1076-1080.

principalmente na automação, o que não surpreende mais quanto à destruição de empregos.

Quando todos olham para as consequências ao nível da segurança e da privacidade, esquecemo-nos de projetar o impacto que poderá vir a ter noutras áreas como a política, por exemplo, em que as consequências poderão ser muito significativas. Nas democracias do futuro, em muitos casos já presente, vamos ter de lidar com um mundo inundado de dados, que nós próprios fornecemos e sobre os quais não temos qualquer controlo ou benefício, utilizados por sistemas de algoritmos cujos objetivos desconhecemos¹⁵³.

O princípio da presunção de inocência é a base do nosso sistema jurídico e está vertido na DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, mas num mundo hiper-monitorizado, onde todos os passos de todos os cidadãos serão registados e vigiados em tempo real o flagrante delito poderá passar a ser a norma, nesse caso, que papel fica para os tribunais? E se por um lado os sistemas de RF podem ter um impacto bastante positivo quando permitem reduzir o crime, como sucedeu com a introdução do sistema nos transportes públicos na cidade costeira de Xiamen, China¹⁵⁴, também causam enorme preocupação quando permitem identificar todos os participantes de uma manifestação contra determinada ação do governo.

O sistema de reconhecimento facial, ao monitorar constantemente os movimentos dos cidadãos, pode-se tornar uma ferramenta poderosa para o controlo das populações, resultando em violações de privacidade e restrição de liberdades individuais. Essa capacidade de prever possíveis situações de conflito por parte de indivíduos ou grupos pode levar os governos a adotarem medidas profiláticas, eliminando antecipadamente qualquer forma de contestação, mesmo que seja pacífica e legal¹⁵⁵. Essa perspetiva pode representar uma ameaça real à democracia, pois os sistemas de RF podem suprimir comportamentos alternativos, desviantes e divergentes, resultando numa sociedade funcional, mas também homogênea, onde não há espaço para contestação ou expressão livre da genialidade humana.

Além disso, o uso generalizado de sistemas baseados em IA, incluindo o reconhecimento facial, pode ter implicações significativas na economia e no mercado

¹⁵³ Cfr. GENTZEL, M. (2021) – *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*. Philosophy & Technology, pp. 1 - 25.

¹⁵⁴ Cfr. <https://www.nobleprog.cn/en/face-recognition/training/xiamen>.

¹⁵⁵ Cfr. MAGDUM, N., & KURHEBHAGWAN, S. (2017) – *Face Recognition by GroupWise Registration Technique*. International Journal of Advance Research and Innovative Ideas in Education, 3, pp. 1076-1080.

de trabalho. A automação impulsionada por IA pode levar à substituição de empregos tradicionais por máquinas inteligentes, levantando questões sobre a sustentabilidade do emprego e a necessidade de requalificação dos trabalhadores para se adaptarem a novas funções¹⁵⁶. Essa mudança pode tanto trazer benefícios em termos de eficiência e produtividade, como também desafios sociais, como a necessidade de políticas de proteção social e redistribuição de recursos para garantir uma transição justa e equitativa.

Além disso, a utilização do reconhecimento facial também levanta preocupações éticas.

Os algoritmos por trás desses sistemas podem ser tendenciosos e discriminatórios, levando a injustiças e discriminação sistemática contra certos grupos, como minorias étnicas ou pessoas de determinadas origens socioeconómicas, o que pode reforçar desigualdades já existentes na sociedade e ampliar a lacuna entre os mais privilegiados e os mais marginalizados.

Portanto, é crucial que a sociedade encontre um equilíbrio entre o avanço tecnológico e a proteção dos direitos e liberdades individuais. É necessário um debate amplo e inclusivo para definir políticas e regulamentações adequadas que garantam o uso ético, responsável e transparente da tecnologia de reconhecimento facial, bem como das demais aplicações de IA. Somente assim poderemos colher os benefícios da inovação tecnológica sem comprometer os valores fundamentais que sustentam uma sociedade democrática e inclusiva.

5.8. PONDERAÇÃO DE INTERESSES

A tentação de muitos governos na adoção de um modelo de controlo generalizado, facilmente acessível, sempre foi elevada. Poder controlar a circulação de todos os cidadãos, a toda a hora e em todo o lado nem será o mais óbvio.

É que, como vimos, a implementação de um sistema centralizado de reconhecimento facial poderá assim reduzir o poder judicial a verificar flagrantes delitos, empurrar o poder legislativo para a transposição de procedimentos e deixar ao poder executivo o domínio sobre todas as formas de contestação. A grande diferença em relação a fenómenos históricos já conhecidos reside no facto deste modelo se basear em

¹⁵⁶ Cfr. GENTZEL, M. (2021) – *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*. Philosophy & Technology, pp. 1 - 25.

sistemas de IA autônomos e supereficientes, imunes às fragilidades da natureza humana como a manipulação ou a corrupção, por exemplo.

É verdade que a evolução tecnológica é inevitável, assim como o próprio respirar de um organismo¹⁵⁷. Nesse contexto, o reconhecimento facial traz consigo uma série de benefícios que podem melhorar a vida dos cidadãos comuns de maneiras significativas.

Uma das vantagens mais evidentes para o cidadão comum é a possibilidade de eliminar filas e tempos de espera em repartições públicas. Com essa tecnologia, será possível obter documentos oficiais de forma instantânea, facilitando a vida de milhões de pessoas que precisam lidar com questões burocráticas. Além disso, o acesso direto a determinados locais sem a necessidade de burocracias adicionais também tornará a experiência do dia-a-dia mais prática e conveniente.

A aplicação do reconhecimento facial também tem o potencial de revolucionar processos eleitorais, permitindo que os cidadãos votem de maneira mais rápida e segura. Além disso, o uso dessa tecnologia pode facilitar a compra de uma casa ou outros bens, eliminando a necessidade de extensa documentação e processos burocráticos.

Outro ponto positivo é o uso do reconhecimento facial para fins de segurança. Os Governos poderão utilizar essa tecnologia para identificar e prender criminosos com mais eficiência. O controle de acessos em áreas sensíveis ou restritas também pode ser aprimorado, aumentando a segurança de instalações importantes¹⁵⁸.

Contudo, é importante reconhecer que, apesar dos pontos positivos, a implementação do reconhecimento facial deve ser cuidadosamente regulamentada. as preocupações sobre o abuso dessa tecnologia por parte dos governos para reprimir oposição política ou violar os direitos humanos são legítimas, pelo que, é crucial que a matriz democrática e os valores dos direitos humanos sejam preservados ao adotar essas tecnologias.

No entanto, os recursos às tecnologias de reconhecimento facial apresentam perigos com os quais não é fácil lidar. A possibilidade de o reconhecimento facial ser utilizado

¹⁵⁷ Cfr. MONTROLL, E., & SHULER, K. (1979) – *Dynamics of technological evolution: Random walk model for the research enterprise*. Proceedings of the National Academy of Sciences of the United States of America, 76 12.

¹⁵⁸ Cfr. MAGDUM, N., & KURHEBHAGWAN, S. (2017) – *Face Recognition by GroupWise Registration Technique*. International Journal of Advance Research and Innovative Ideas in Education, 3, pp. 1076-1080.

de forma capaz de afetar a imagem, a intimidade, o bom nome, a vida privada, a igualdade é um problema de enorme dimensão¹⁵⁹.

Quer o reconhecimento facial se dirija à identificação de pessoas, que seja “apenas” um método de autenticação. Basta que as redes neurais tenham sido alimentadas sobre desiguais qualidades e quantidades de dados¹⁶⁰, por exemplo, diferente número de faces de diversos grupos sociais.

Se, por um exemplo, sistema for treinado sobre milhões de rostos masculinos brancos e apenas milhares de rostos de mulheres ou de pessoas de outras raças, o mesmo será claramente menos preciso relativamente a estes dois últimos grupos, isto significa, que nestes últimos dois grupos poderá haver muitos mais erros de imprecisão na identificação destes dois últimos grupos.

Tem o nome de enviesamento algorítmico, ou seja, enviesamento inerente ao conjunto de dados subjacentes¹⁶¹.

Para mitigar, ao máximo estas inexactidões e as possíveis discriminações emergentes, estabelece a CARTA PORTUGUESA DE DIREITOS HUMANOS NA ERA DIGITAL, que “As decisões com impacto significativo na esfera dos destinatários que sejam tomadas mediante o uso de algoritmos devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis, nos termos previstos na lei”¹⁶².

Por seu turno, ADRIENNE YAPO e JOSEPH WEISS afirmam que o Facebook utiliza uma técnica de reconhecimento facial baseada em algoritmo que, assim que descarregamos uma fotografia no Facebook, esse reconhecimento facial vai automaticamente reconhecer as pessoas que estão presentes na fotografia e sugerir o nome das mesmas, o que permite facilmente, gerar em caso de errada identificação facial, ingerências ou associações não desejadas¹⁶³.

¹⁵⁹ Cfr. GENTZEL, M. (2021) – *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*. Philosophy & Technology, pp. 1 - 25.

¹⁶⁰ Como refere SUSAN LEAVY, Gender Bias in Artificial Intelligence, <https://aristotle.ucd.ie/files/talks-2019/Susan-Leavy-gender-bias-and-ai.pdf>.

¹⁶¹ N° 27 da proposta de resolução do parlamento europeu que contém recomendações à comissão sobre o quadro dos aspetos éticos da IA, da Robótica e das Tecnologias conexas.

¹⁶² Cfr. Artigo 9º, n°2, Lei n°27/2021 de 17/05, Cfr.

https://www.parlamento.pt/Legislacao/Paginas/Educacao_Carta-Portuguesa-de-Direitos-Humanos-na-Era-Digital.aspx

¹⁶³ Cfr. YAPO, Adriene; WEISS, Joseph (2018) – *Ethical Implications Of Bias In Machine Learning*. 51st Hawaii International Conference on System Sciences.

Os perigos de intromissão desnecessária e desproporcionada em “direitos, liberdades e garantias” e em direitos de personalidade, consequência de uma intromissão desregulada são, portanto mais que muitos.

Assim, “A utilização da IA deve ser orientada pelo respeito pelos direitos fundamentais, garantindo um justo equilíbrio entre os princípios da explicabilidade, da segurança, da transparência, da responsabilidade, que atenda às circunstâncias de cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação”¹⁶⁴. Neste sentido, veja-se o sucedido em 2015, quando a aplicação Google Photos etiquetou duas pessoas de raça negra como gorilas¹⁶⁵.

Efetivamente, um dos maiores problemas que pode surgir é a errada identificação de uma pessoa, isto porque se trata de uma tecnologia que não é perfeita e que está em constante desenvolvimento.¹⁶⁶

Assim, embora as tecnologias de reconhecimento facial tenham vindo para ficar, especialmente por razões ligadas à prevenção criminal, no entanto, o reconhecimento facial, ligado por algoritmos apresenta diversos perigos, para além dos que em geral se apresentam devido ao processamento de dados¹⁶⁷, havendo, inclusive, algumas formas de defraudar o resultado, como é o caso do uso de maquilhagem, óculos, cirurgias estéticas e, ainda, o caso de se tratarem de gémeos entre outros¹⁶⁸.

Pode acontecer ainda que a variação da luz e o ângulo das imagens possa interferir no resultado, podendo conduzir a um resultado erróneo¹⁶⁹, ou seja, se não se conseguir garantir a qualidade e fiabilidade das imagens, pode de facto comprometer-se a exatidão dos resultados alcançados¹⁷⁰. Assim, a qualidade de imagens retiradas de câmaras de vigilância está longe de ser de fácil controlo, podendo também constituir um sério risco para o rigor dos resultados que se pretende com o uso do

¹⁶⁴ Cfr. Art.º 9 da Carta Portuguesa de Direitos Humanos na Era Digital.

¹⁶⁵ Google apologises for photos app’s racist blunder.

¹⁶⁶ DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., “A Technological and Ethical Analysis of Facial Recognition ...”, pp. 13-15.

¹⁶⁷ Cfr. https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

¹⁶⁸ Cfr. RODRIGUES, Sara Raquel dos Santos, “Desenvolvimento de um Sistema de Reconhecimento Facial”, pp. 49-52.; ORVALHO, Verónica, Reconhecimento Facial, ob. cit.; GALBALLY, J.; FERRARA, P.; HARAKSIM, R.; PSYLLOS, A. e BESLAY, L., “Study on Face Identification Technology for its Implementation in the Schengen Information System”, EUR 29808 EN, Publication Office of the European Union, Luxemburg, 2019, ISBN 978-92-76-08843-1, doi:10.2760/661464, JRC116530, pp. 38-41 disponível em <https://op.europa.eu/en/publication-detail/-/publication/dd473249-adbf-11e9-9d01-01aa75ed71a1/language-en>.

¹⁶⁹ Cfr. SANTOS, Hugo Luz dos, “Inteligência Artificial e Processo Penal”, Braga: Nova Causa, Edições Jurídicas, 2022, ISBN 9789899026308, pp. 163-165.

¹⁷⁰ Cfr. Article 29 Data Protection Working Party, “Opinion 3/2012 on developments on biometric technologies”, 27 de abril de 2012, 00720/12/EN, WP193, p. 6, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf,

reconhecimento facial uma vez que a má qualidade pode conduzir a uma incorreta identificação de um indivíduo¹⁷¹. Nestes casos a “fidedignidade depende da exatidão dos meios tecnológicos usados”¹⁷².

Não obstante, com o avanço dos anos, tem havido um maior rigor nestas tecnologias, sendo que o risco de erro tem vindo a diminuir¹⁷³.

Na operação de reconhecimento facial são reunidos e armazenados dados biométricos, mas é preciso ter em conta que, com o passar dos anos, as características biométricas vão-se degradando, vão-se alterando, sendo que após cinco anos será mais difícil de obter resultados exatos diminuindo, portanto, a precisão destes¹⁷⁴.

5.9. A ESTRATÉGIA DA UNIÃO EUROPEIA PARA A INTELIGÊNCIA ARTIFICIAL E PARA OS SISTEMAS DE IDENTIFICAÇÃO BIOMÉTRICA

Tendo em consideração todas as vantagens e riscos atrás enunciados, no âmbito da União Europeia, os parâmetros essenciais para o desenvolvimento e utilização de sistemas de identificação biométrica e tecnologias de reconhecimento facial são delineados pelas normas de proteção de dados, privacidade e não discriminação, assim como pela Proposta de Regulamento sobre Inteligência Artificial datada de 21 de abril de 2021.

No entanto, a abordagem adotada pela União Europeia transcende esses enquadramentos jurídicos. Diversos outros requisitos da UE também devem ser considerados, tais como os direitos das crianças e dos idosos, a liberdade de expressão, a liberdade de reunião e associação, o direito a uma administração eficiente e o direito a um processo judicial efetivo. Adicionalmente, os sistemas de identificação biométrica levantam questões pertinentes à segurança dos produtos, à responsabilidade do fabricante e à proteção do consumidor. Por outro lado, as legislações relativas ao controlo das fronteiras devem ser abordadas no contexto da aplicação coerciva da lei.

¹⁷¹ FRA – European Union Agency For Fundamental Rights, “*Facial recognition technology: fundamental rights considerations...*”, ob. cit., p. 10.

¹⁷² Cfr. FIDALGO, Sónia, “*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais(ainda mais) em perigo*”, p. 142.

¹⁷³ FRA – European Union Agency for Fundamental Rights, “*Facial recognition technology: fundamental rights considerations in the context of law enforcement*”, pp. 33-34.

¹⁷⁴ Ibidem, pp. 28-29.

A abordagem da União Europeia abarca uma visão holística que se estende para além dos domínios jurídicos mencionados, buscando garantir a consideração de diversos fatores interconectados, com o objetivo de promover a proteção dos direitos individuais, a segurança pública e a equidade nos diversos aspetos relacionados à utilização dessas tecnologias.

A Proposta de Regulamento sobre a Inteligência artificial de 21 de abril de 2021, apresentada pela Comissão, deve ser entendida no contexto de vários outros (e anteriores) marcos e requisitos jurídicos europeus.

A este respeito, é possível dizer que existe um enquadramento multinível (*multi-level framework*) da União Europeia¹⁷⁵, que compreende vários enquadramentos jurídicos.

Os antecedentes da Proposta são o livro branco da Comissão Europeia sobre a Inteligência Artificial de 19 de fevereiro de 2020, bem como várias outras iniciativas do Parlamento europeu relativas à definição de limites quanto ao uso do reconhecimento facial na União Europeia¹⁷⁶.

Apesar da atualidade deste tema, existe um ACÓRDÃO DO SUPREMO TRIBUNAL DE JUSTIÇA DE 27-09-2017 que se refere ao reconhecimento facial, definindo este como o “emprego de técnicas de fotografia forense avançadas que incluem identificação de padrões faciais, elaboração de um perfil antropométrico único e comparação com os padrões que não oferecem dúvidas. Por meio de software de edição fotográfica determina-se a correcção a aplicar sobre a imagem para, deste modo, poder precisar a localização dos pontos de referência. Por meio de negatoscópio digital pode-se realizar sobreposições entre as imagens que oferecem

¹⁷⁵ É o caso da Resolução do Parlamento europeu, aprovada em 6 de outubro de 2021, iniciativa apresentada antes da Proposta da Comissão e que contém várias referências à utilização de dados biométricos e ao reconhecimento facial. Na exposição de motivos da Proposta já se reconhecia que a inteligência artificial oferece grandes oportunidades no domínio da aplicação coerciva da lei, permitindo nomeadamente melhorar os métodos de trabalho dos serviços policiais e das autoridades judiciais e combater mais eficazmente certos tipos de criminalidade, elencando um conjunto de aplicações, nas quais incluía as tecnologias de reconhecimento facial. Mas também se chamava a atenção para os riscos para os direitos fundamentais. A Resolução aprovada em 6 de outubro de 2021 reitera essas preocupações, em especial nos pontos 25, 26, 27, 30 e 31.

¹⁷⁶ É o caso da Resolução do Parlamento Europeu, aprovada em 6 de outubro de 2021, iniciativa apresentada antes da Proposta da Comissão e que contém várias referências à utilização de dados biométricos e ao reconhecimento facial. Na exposição de motivos da Proposta já se reconhecia que a inteligência artificial oferece grandes oportunidades no domínio da aplicação coerciva da lei, permitindo nomeadamente melhorar os métodos de trabalho dos serviços policiais e das autoridades judiciais e combater mais eficazmente certos tipos de criminalidade, elencando um conjunto de aplicações, nas quais incluía as tecnologias de reconhecimento facial. Mas também se chamava a atenção para os riscos para os direitos fundamentais. A Resolução aprovada em 6 de outubro de 2021, reitera essas preocupações, em especial nos pontos 25, 26, 27, 30 e 31.

dúvidas e as isentas de dúvidas, analisando a correspondência entre os pontos de referência”¹⁷⁷.

¹⁷⁷ Cfr. Ac. do STJ, Proc. n.o 427/14.0JACBR.C1, de 27-09-2017 disponível em <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/79760e66f0bf4ba4802581bb003b2bd8?OpenDocument>

CONCLUSÃO

Os conceitos de intimidade, imagem e o tema do reconhecimento fácil, conforme verificámos ao longo do presente estudo, são conceitos que se encontram plenamente interligados.

Em concreto, a tecnologia do reconhecimento facial, à medida que se torna uma presença cada vez mais intrínseca em diversas esferas da sociedade, coloca em questão os fundamentos dos direitos individuais. Enquanto a tecnologia avança, proporcionando inovações notáveis, as implicações para a privacidade e a autonomia dos cidadãos tornam-se cada vez mais evidentes. Ora, num mundo onde a conectividade digital é onipresente, a implementação generalizada do reconhecimento facial levanta preocupações substanciais.

Uma das principais inquietações reside na coleta maciça e no armazenamento de dados biométricos, que incluem características únicas de cada indivíduo, dado que, a amplitude dessas informações sensíveis suscita receios quanto à sua segurança e ao potencial uso indevido por parte de entidades governamentais ou corporativas. A privacidade, sendo um dos pilares dos direitos fundamentais, é diretamente impactada pelo reconhecimento facial. Assim, a capacidade de identificar e rastrear pessoas sem o seu conhecimento ou consentimento prévio levanta questões éticas e jurídicas. O direito à autodeterminação, no qual os indivíduos têm o controlo sobre as suas próprias informações pessoais, é desafiado quando a tecnologia facial é empregada de maneira indiscriminada.

Ademais, o risco de discriminação entra em cena, porquanto diversos estudos têm destacado que os sistemas de reconhecimento facial muitas vezes apresentam disparidades significativas em precisão dependendo de características como etnia e género.

Ora, este facto não só coloca em cheque a equidade do uso da tecnologia, mas também gera uma preocupação real sobre a possibilidade de aprofundar as desigualdades já existentes na sociedade.

Assim, para equilibrar o avanço tecnológico e a salvaguarda dos direitos individuais, é imperativo estabelecer regulamentações robustas. A transparência no desenvolvimento e aplicação desses sistemas é crucial, assegurando que os cidadãos compreendam como e quando o reconhecimento facial é utilizado. Além disso, a obtenção de consentimento informado deve ser uma prioridade, garantindo que as

peçoas tenham a oportunidade de decidir se desejam participar de ambientes ou serviços que empregam essa tecnologia. Por outro lado, a supervisão efetiva do uso do reconhecimento facial é uma responsabilidade que recai tanto sobre as entidades governamentais quanto sobre as empresas privadas. Neste sentido, devem ser implementados mecanismos de prestação de contas, permitindo avaliações regulares do impacto dessa tecnologia nos direitos fundamentais. Essa supervisão não apenas protege os cidadãos de possíveis abusos, mas também contribui para o desenvolvimento responsável de tecnologias que têm um impacto significativo na sociedade.

O potencial do reconhecimento facial para melhorar a eficiência e a conveniência em várias áreas é inegável. No entanto, também existem preocupações significativas em relação à privacidade, segurança e potenciais abusos. O uso indiscriminado do reconhecimento facial pode levar a violações de privacidade, coleta e uso indevido de dados pessoais, além de gerar perfis discriminatórios e étnicos ou raciais.

Assim, como vimos, é essencial que haja uma regulamentação adequada para proteger os cidadãos e garantir que a tecnologia seja utilizada da forma mais ética e responsável. As políticas devem abordar a transparência na coleta e uso de dados, o consentimento informado, a proteção contra o uso indevido e a salvaguarda contra a discriminação. Além disso, é fundamental incentivar pesquisas contínuas sobre o aprimoramento das técnicas de reconhecimento facial, especialmente no que diz respeito à melhoria da precisão. A sociedade também precisa ser educada sobre as implicações do uso dessa tecnologia, para que possam tomar decisões informadas e participar ativamente do debate público.

Como tivemos oportunidade de analisar, esta é uma tecnologia promissora, mas deve ser abordada com cautela e responsabilidade para equilibrar os benefícios com os riscos associados e somente por meio de uma abordagem ética, regulamentação apropriada e participação ativa da sociedade poderemos garantir que o uso do reconhecimento facial seja benéfico para todos sem comprometer a privacidade e os direitos individuais.

Ao longo deste estudo foi possível analisar as implicações e desafios éticos relacionados com o crescente uso do reconhecimento facial em diversas áreas, desde a segurança até o atendimento ao cliente e verificámos que o reconhecimento facial, apesar das suas inúmeras aplicações benéficas, pode representar uma séria ameaça à privacidade individual e coletiva, porquanto, a capacidade de monitorar, rastrear e

identificar indivíduos de forma automatizada levanta questões profundas sobre a proteção dos direitos fundamentais das pessoas, especialmente no contexto de um mundo cada vez mais conectado.

Constatamos também que o potencial de uso inadequado ou abusivo dessa tecnologia é real, podendo levar a discriminação, violações de privacidade e danos sociais. A necessidade de desenvolver regulamentações sólidas e transparentes torna-se imperativa para proteger os indivíduos e preservar os princípios democráticos.

Contudo, é importante reconhecer que o reconhecimento facial também tem potencial para impulsionar avanços significativos em áreas como segurança, medicina, atendimento ao cliente e outras. Se utilizado de forma responsável, pode trazer benefícios muito importantes à sociedade, melhorando eficiência e oferecendo soluções bastante inovadoras.

Assim, para alcançar um equilíbrio adequado entre o progresso tecnológico e a preservação da privacidade, é fundamental aprofundar a discussão e o diálogo entre governos, empresas, especialistas em ética, tecnologia e a sociedade como um todo, sendo necessário investir em pesquisas contínuas para entender melhor as implicações e os limites éticos do reconhecimento facial, bem como para desenvolver algoritmos mais justos, transparentes e responsáveis.

REFERÊNCIAS

AERTSEN, Jan (2012) – *A medieval philosophy as transcendental thought : from Philip the Chancellor (ca. 1225) to Francisco Suárez*. Leiden : Brill.

ALEKSIC, Petar S. ; KATSAGGELOS, Aggelos K. (2006) – Audio-Visual Biometrics. *Proceedings of the IEEE* [Em linha]. V. 94, n. 11 (Nov. 2006) p. 2025-2044. Disponível em WWW:<URL: 10.1109/JPROC.2006.886017>.

ANDRADE José Carlos Vieira de (2012) – *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. 5.^a ed. Coimbra : Almedina

ANDRADE, Manuel da Costa (1999) – Artigo 192.º (Devassa da vida privada). In DIAS, Jorge de Figueiredo, dir. - *Comentário Conimbricense do Código Penal, Parte Especial*. Coimbra : Coimbra Editora. T. 1.

ASCENSÃO, José de Oliveira (2000) – *Direito civil – Teoria Geral*. 2.^a ed. Coimbra : Coimbra Editora. V. 1.

BELLEIL, A. (2001) – *@-privacidade, o mercado dos dados pessoais: proteção da vida privada na internet*. Lisboa: Instituto Piaget

BERTOCCHI, Daniela (2012) - *O algoritmo curador: o papel do comunicador num cenário de curadoria algorítmica da informação*. XXI Encontro Anual da Compós

CANOTILHO, Gomes e MOREIRA, Vital (1993) – *Constituição da República Portuguesa anotada*, 3.^a ed., Coimbra

CANOTILHO, Gomes (2018) – *Direito Constitucional e Teoria da Constituição*, 7.^a Ed., Almedina, Coimbra

CANOTILHO, J.J. Gomes e MOREIRA, Vital – “Artigo 26.º”, p. 467. Rui Medeiros e António Cortês definem este direito como “o direito de oposição à divulgação da vida privada”, assim como “o direito ao respeito da vida privada, ou seja, o direito de oposição à investigação sobre a vida privada”, cfr.

CASTRO, Catarina Sarmiento e (2005) – *Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Edições Almedina

COSTA, Adalberto (2012) – O direito à imagem. *Revista Ordem dos Advogados*. A. 72, n. 4 (out.-dez. 2012) p. 1323-1978.

DUONG, J. HURTADO, J. KUNTJORO, N. MAK, N. MAXWELL, N. & VU, B., “A *Technological and Ethical Analysis of Facial Recognition ...*”

EGBERT, Simon e LESSE, Matthias *Criminal futures: predictive policing and everyday police work*, London, New York, Routledge, 2021

FIDALGO, Sónia, “*A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*”

FRA – European Union Agency For Fundamental Rights, “Facial recognition technology: fundamental rights considerations...”

GALBALLY, J. [et al.] (2019) - *Study on Face Identification Technology for its Implementation in the Schengen Information System* [Em linha]. Luxemburg : Publication Office of the European Union. ISBN 978-92-76-08843-1. EUR 29808 EN. Disponível em WWW:<URL:<https://op.europa.eu/en/publication-detail/-/publication/dd473249-adbf-11e9-9d01-01aa75ed71a1/language-en>>.

GALBALLY, J., MARCEL, S., & FIERREZ, J. (2014) – *Biometric Antispoofing Methods: A Survey in Face Recognition*. IEEE Access, 2.

GENTZEL, M. (2021) – *Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy*. Philosophy & Technology

GONZALEZ, José (2022) – *Reconhecimento facial (FRT) e direito à imagem*. Revista da Faculdade de Direito da Universidade de Lisboa. V. 63, n 1-2 (2022).

GUERRA, Amadeu (1999) – *Informática e privacidade – Nova lei de proteção de dados e a lei de proteção de dados no sector de telecomunicações*. Lisboa: Vislis Editores, Lda.

HADDAD, Gabrielle M. (2021) – *Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom*, in Vanderbilt Journal of Entertainment and Technology Law, 23, 4

HOERNES, G. (1972) – *Generalized view of a Data Base*

LEVASHOV, Kirill (2013) – *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*. Columbia Science and Technology Law Review, v. 15, p. 164, Fall 2013

LUKES, Steven (2006) – *Individualism*, Colchester: University of Essex/ ECPR

MADIEGA, Tambiama e MILDEBRATH, Hendrik, *Regulating facial recognition in the EU*.

MAGDUM, N., & KURHEBHAGWAN, S. (2017) – *Face Recognition by GroupWise Registration Technique*. International Journal of Advance Research and Innovative Ideas in Education, 3

MAGDUM, N., & KURHEBHAGWAN, S. (2017) – *Face Recognition by GroupWise Registration Technique*. International Journal of Advance Research and Innovative Ideas in Education, 3

MARQUES e LOURENÇO (2006) – *Direito da Informática*. (2.^a ed. rev. e act.) Coimbra

MARTINS, L. M. (2017) – *A tutela jurídica da privacidade e do sigilo na era digital: Doutrina, Legislação e Jurisprudência*. In Revista de Investigações constitucionais. (Vol. IV), Curitiba, N.º 3

MILL, John Stuart (1991) – *Sobre a Liberdade*. 2. ed. Clássicos do Pensamento Político; v. 22. Petrópolis, RJ: Vozes.

MIRANDA, Jorge (1999) – *Direitos Fundamentais: Introdução Geral* (Lisboa, 1999)

MIRANDA, Jorge (1999) – *O Homem e o Estado - Direitos do Homem e Democracia*. Artigo publicado na Revista Interesse Público. São Paulo: Notadez, Ano I, n. 01, Janeiro/Março 1999, 1

MIRANDA, Jorge; MEDEIROS, Rui (2005) – *Constituição portuguesa anotada*. Tomo I. Coimbra: Coimbra Editora.

MONTROLL, E., & SHULER, K. (1979) – *Dynamics of technological evolution: Random walk model for the research enterprise*. Proceedings of the National Academy of Sciences of the United States of America, 76 12.

MORAIS, Carlos Blanco de – *Some new thoughts on the so called “dogmatic unity” between liberty rights and social rights in times of financial emergency*, disp. in <http://e-publica.pt/volumes/v1n3a05.html>

MOTA PINTO, Paulo (1989) – *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*, in: Estudos em Memória do Professor Doutor Paulo Cunha, Lisboa

MOTA PINTO, Paulo (1993) – *O Direito à reserva sobre a Intimidade e sobre a vida privada*, Boletim da FDUC, LXIX.

NISSENBAUM, Helen e INTRONA, Lucas, “*Facial Recognition Technology. A survey of Policy and Implementation Issues*”, The Center for Catastrophe Preparedness and Response, pp.20-21, disponível em https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy_and_Implementation_Issues.

NORRIS, Clive (2003) – From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control, in “*Surveillance as Social Sorting. Privacy, risk, and digital discrimination*”, Routledge, David Lyon, pp. 263-266, disponível em https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf.

NOVAIS Jorge Reis (2010) – “*As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*”, 2ª ed, Coimbra Editora, Coimbra

NOVAIS, Jorge Reis (2006) – “*Direitos Fundamentais: Trunfos contra a Maioria.*” Coimbra: Editora Coimbra

PENTLAND, A., & CHOUDHURY, T. (2000) – *Face Recognition for Smart Environments. Computer*, 33

PUFENDOR, Samuel – *De jure naturae et gentium (Liber primus – Liber quartus)* apud SAHD, Luiz F. N. de A. e Silva. O contrato social em Samuel Pufendorf. Revista Aurora de Filosofia. Curitiba, v. 21, n. 28, jan./jun. 2009

RAPOSO, Vera Lúcia (2022) – *(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation*, in *Information & Communications Technology Law*, 2022, disponível em <https://doi.org/10.1080/13600834.2022.2054076>.

RAPOSO, Vera Lúcia (2022) – *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, in *European Journal on Criminal Policy and Research*, Springer online, 01 June 2022, disponível em <https://link.springer.com/content/pdf/10.1007/s10610-022-09512-y.pdf>.

RENAUD, Michel (1999) – *A dignidade do ser humano como fundamentação ética dos direitos do homem*. Brotéria. Cultura e Informação. - Vol. 148, nº. 2 (Fev. 1999)

RODOTÀ, Stefano (2008) – *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar.

RODOTÁ, Stefano (2013) – *Some Remarks on Surveillance today*, in European Journal of Law and Technology, Vol. 4., No. 2

RODRIGUES, Sara Raquel dos Santos, “*Desenvolvimento de um Sistema de Reconhecimento Facial*”

SADIN, Eric (2015) – *La vie algorithmique: critique de la raison numérique*. Paris

SALDANHA, Nuno (2018) – *Novo Regulamento de Proteção de Dados*

SALGADO, Joaquim Carlos (2012) – *A ideia de justiça em Kant: seu fundamento na liberdade e na igualdade*. 3.^a Edição, Belo Horizonte, Del Rey.

SANTOS, Hugo Luz dos, “*Inteligência Artificial e Processo Penal*”, Braga: Nova Causa, Edições Jurídicas, 2022

SARLET, Ingo (2008) – *Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988*. 6. ed. Porto Alegre: Livraria do Advogado

SCHWABE, Jürgen (2005) – *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Alemão*. Organização e introdução por Leonardo Martins. Montevideu: Konrad-Adenauer-Stiftung, pp. 656 a 667.

SILVA, Germano Marques (2008) – *Curso de Processo Penal*, Vol. I, Edições Verbo

TAMÒ-LARRIEUX, *Designing for Privacy and its Legal Framework*

VILELA, Alexandra (2000) – *Considerações acerca da presunção de inocência em direito processual penal*, Coimbra Editora

WELINDER, Yana (2012) – *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks* (July 16, 2012). Harvard Journal of Law and Technology, v. 26, n. 1

WITTGENSTEIN, Ludwig (2001) – *Philosophical investigations*. 3. ed. Oxford: Blackwell, 2001, §11.

YANG, X., & LV, F. (2011) – *The design of a face recognition system based on skin color and geometrical characteristics*, 2011 International Conference on Image Analysis and Signal Processing.

YAPO, Adriene; WEISS, Joseph (2018) – *Ethical Implications Of Bias In Machine Learning*. 51st Hawaii International Conference on System Sciences.

SÍTIOS DA INTERNET CONSULTADOS

- <http://fra.europa.eu/pt/eu-charter/article/7-respeito-pela-vida-privada-e-familiar>
- <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20>
- <https://assets.kpmg.com/content/dam/kpmg/br/pdf/2021/08/privacy-technology.pdf>.
- <https://casetext.com/case/sony-music-entertainment-inc-v-does-1-40>.
- <https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982>.
- <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1966-34509075>.
- <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/1998-34450175-43475975>
- <https://dre.tretas.org/dre/4447141/despacho-2705-2021-de-11-de-marco>.
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf,
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf
- https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2012/wp193_en.pdf.
- https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
- <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>.
- <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679>.
- <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679#d1e3713-1-1>.
- [https://eur-lex.europa.eu/legal-content/Pt/tXt/PdF/?uri=celeX:52021iP0405&from=Pt\)](https://eur-lex.europa.eu/legal-content/Pt/tXt/PdF/?uri=celeX:52021iP0405&from=Pt)

- <https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html>.
- https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm.
- https://gdprhub.eu/Data_Protection_in_Germany.
- <https://globalfreedomofexpression.columbia.edu/cases/maximilian-schrems-v-facebook-ireland-limited/>
- <https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/>.
- <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/02/Von-Hannover-vs.-Alemanha-II.docx.pdf>.
- [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-123515%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-123515%22]}).
- <https://hudoc.echr.coe.int/eng?i=001-90617>.
- [https://hudoc.echr.coe.int/fre#%7B%22itemid%22:\[%22002-8960%22\]%7D](https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22002-8960%22]%7D).
- [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-109029%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109029%22]}).
- [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-211794%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-211794%22]}).
- [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-90590%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-90590%22]}).
- [https://hudoc.echr.coe.int/fre#{%22tabview%22:\[%22document%22\],%22itemid%22:\[%22001-210766%22\]}](https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-210766%22]}).
- <https://medium.com/project-2030/data-is-new-oil-a-ludicrous-proposition-1d91bba4f294>.
- <https://observador.pt/opiniao/reconhecimento-facial-democracia-4-0-0/>.
- <https://rm.coe.int/168067d216>.
- <https://rm.coe.int/case-law-on-data-protection/1680766992>.
- <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>
- <https://supreme.justia.com/cases/federal/us/561/186/>.
- <https://unric.org/pt/wp-content/uploads/sites/9/2009/10/Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf>.
- <https://www.5rb.com/case/reklos-and-davourlis-v-greece/>.

- <https://www.5rb.com/case/sciacca-v-italy/>.
- <https://www.cig.gov.pt/wp-content/uploads/2018/01/Declaracao-Universal-dos-Direitos-Humanos.pdf>.
- <https://www.civil.law.cam.ac.uk/projectseuropean-data-protection-laws-and-freedom-expression/denmark>.
- <https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf>.
- <https://www.cnpd.pt/>.
- <https://www.dataguidance.com/notes/sweden-data-protection-overview>.
- https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf
- https://www.echr.coe.int/documents/d/echr/convention_por.
- <https://www.electronicid.eu/pt/blog/post/como-funciona-o-reconhecimento-facial-e-a-sua-seguranca/pt>.
- <https://www.europarl.europa.eu/news/pt/headlines/society/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>.
- <https://www.freedomforum.org/first-amendment-protects-anonymous-speech-online/>
- <https://www.nobleprog.cn/en/face-recognition/training/xiamen>.
- https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/por.pdf.
- <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.
- https://www.parlamento.pt/Legislacao/Paginas/Educacao_Carta-Portuguesa-de-Direitos-Humanos-na-Era-Digital.aspx
- <https://www.techtarget.com/searchenterpriseai/definition/facial-recognition>.
- <https://www.terra.com.br/byte/internet/china-decreta-fim-do-anonimato-dos-usuarios-de-redes-sociais,3c29fe32c8bda310VgnCLD200000bbcceb0aRCRD.html>.
- <https://www.thalesgroup.com/pt-pt/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition>.

- <https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/principios-do-tratamento-dados/>.
- <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>
- <https://yourdata-yourrights.eu/glossary/federal-data-protection-act/>

JURISPRUDÊNCIA CONSULTADA

JURISPRUDÊNCIA NACIONAL

- Ac. do STJ, Proc. n.o 427/14.0JACBR.C1, de 27-09-2017 disponível em <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/79760e66f0bf4ba4802581bb003b2bd8?OpenDocument>
- ACÓRDÃO DO SUPREMO TRIBUNAL DE JUSTIÇA DE 14/06/2005, Disp. in <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e4428a4a669f03088025705a0052bf9f?OpenDocument&Highlight=0,05A945%20>
- Cfr. Tribunal da Relação de Évora: Processo nº 789/13.7TMSTB-B.E1 (25/06/15), disponível em www.dgsi.pt.
- Cfr. Ac. do STJ, Proc. n.o 427/14.0JACBR.C1, de 27-09-2017 disponível em <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/79760e66f0bf4ba4802581bb003b2bd8?OpenDocument>

JURISPRUDÊNCIA INTERNACIONAL

- Corte Suprema Da Índia, Puttaswamy V. Union Of India, de 24 de Agosto de 2017
- Estonia, de 16 de Junho de 2015
- Facebook Ireland Ltd V. Max Schrems
- Google Spain V. Mario Costeja González (Espanha, 2014)
- Sony Music Entertainment V. Does 1-40 (Eua, 2011)
- Supreme Court Of The United States, Doe V. Reed, de 24 de Junho de 2010
- Von Hannover V. Germany, De 24 De Junho De 2004