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

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

Lisboa

2023

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

Intimidade, imagem e reconhecimento facial

Melissa Stefanie Costa Cidade de Carvalho Merkens

Lisboa

Agosto 2023

UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Direito

Intimidade, imagem e reconhecimento facial

Melissa Stefanie Costa Cidade de Carvalho Merkens

Lisboa

Agosto 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

Lisboa

Agosto 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

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 estar ao alcance de todos, para isto basta um pequeno gesto, um pequeno clique, e com a facilidade em termos de comodidade e rapidez, em que certas tarefas do quotidiano, outrora complexas e morosas, passaram a ser realizadas de forma rápida e cómoda.

Porém seria de uma enorme irresponsabilidade da nossa parte não reconhecer consequências negativas que as tecnologias de informação e comunicação têm trazido para as pessoas, especialmente no que diz respeito à proteção dos seus dados e, em consequência, ao direito à privacidade e à intimidade da vida privada.

Deste modo resulta o permanente apelo ao direito à privacidade e à necessidade de se controlar a difusão das informações que dizem respeito às pessoas. Neste sentido, há que fazer uma adaptação do Direito a esta nova realidade de modo a fazer face a estes novos desafios, de forma a impedir que o mundo digital seja visto ou se transforme num lugar sem regras, em que a transgressão, não dá lugar a responsabilidade civil e/ou criminal. À medida que a tecnologia digital avança, surgem novos desafios que exigem uma adaptação do Direito para lidar com eles de maneira adequada. É essencial garantir que o mundo digital não se torne uma área sem regras. No contexto da proteção da privacidade, é necessário que as leis sejam atualizadas para abordar as preocupações específicas relacionadas à coleta, armazenamento e uso de dados pessoais no ambiente digital. Questões como consentimento informado, finalidade e limitação do uso dos dados, segurança da informação e direito ao esquecimento são alguns dos aspetos que precisam ser considerados. Além disso, é importante estabelecer responsabilidades claras para os atores envolvidos no mundo digital.

Isso inclui empresas que coletam e processam dados pessoais, provedores de serviços online, redes sociais e até mesmo os próprios usuários. A responsabilidade civil e criminal deve ser aplicada quando ocorrerem violações da privacidade ou divulgação não autorizada de informações pessoais.

É muito tênue o limite entre uma utilização adequada às finalidades e uma possível situação abusiva, já que os dados biométricos, sobretudo as imagens faciais, podem ser usados com propósitos obscuros, muito pouco éticos ou até mesmo ilícitos, como por exemplo para fins discriminatórios ou de perseguição, de forma direta ou mesmo indireta. A partir da face, torna-se possível extrair não apenas informações como a idade, género, mas também origem étnica, os seus ideais políticos, desta forma o uso do reconhecimento facial pode gerar também discriminação contra determinados grupos de pessoas.

Diz-nos o atual regulamento que o tratamento dos dados pessoais deverá ser concebido para servir as pessoas. Isso significa que o foco principal deve estar na proteção dos direitos individuais e no benefício dos titulares dos dados. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

O atual regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação.

O crescente desenvolvimento económico e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio destes dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia e mesmo em todo o mundo. As autoridades nacionais dos Estados-Membros foram desta forma chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro.

Os objetivos da Diretiva 95/46/CE continuam a ser válidos, no entanto, não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.
A Diretiva 95/46/CE foi a legislação anterior à implementação do Regulamento Geral de Proteção de Dados na União Europeia. Embora os objetivos da Diretiva 95/46/CE ainda sejam considerados válidos, ela enfrentou desafios significativos na sua aplicação, o que resultou em fragmentação e insegurança jurídica no âmbito da proteção de dados.

Um dos principais problemas da Diretiva 95/46/CE foi a sua transposição inconsistente para a legislação nacional dos Estados membros. Cada país tinha a responsabilidade de implementar a diretiva na sua própria legislação, o que resultou em diferenças nas abordagens e requisitos de proteção de dados em toda a União Europeia. Isso criou uma fragmentação na aplicação das leis de proteção de dados e dificultou a coerência e a harmonização no mercado único digital. A Diretiva não foi capaz de fornecer orientações claras e abrangentes sobre como lidar com essas questões emergentes. A falta de uma estrutura legal e regulatória unificada levou a uma perceção de que os direitos individuais não estavam adequadamente protegidos.

Essas preocupações e desafios foram abordados com a introdução do Regulamento Geral de Proteção de Dados em 2018. O GDPR é um regulamento diretamente aplicável em todos os Estados membros da União Europeia e tem como objetivo harmonizar as leis de proteção de dados e fornecer um nível mais elevado de proteção aos dados pessoais. Ele aborda as lacunas e deficiências da Diretiva 95/46/CE, introduzindo regras mais rigorosas, transparência aprimorada, maior responsabilidade para as organizações e direitos mais fortes para os indivíduos. Com o GDPR, a União Europeia busca promover a segurança e a confiança no ambiente digital, garantindo a proteção efetiva dos dados pessoais. O regulamento aborda especificamente as atividades por meio

eletrônico, fornecendo orientações claras e requisitos específicos para o tratamento de dados pessoais nesse contexto.

Palavras chave: Reconhecimento Facial, Privacidade, Anonimato, direito à Imagem, RGPD

Abstrat

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 gesture, a simple click, and the convenience and speed with which certain daily tasks, once complex and time-consuming, are now performed quickly and comfortably.

However, it would be naive of us not to recognize the negative consequences that information and communication technologies have brought to individuals, particularly concerning the protection of their data and, consequently, their right to privacy and the privacy of their personal lives.

Hence, there is an ongoing appeal for the right to privacy and the need to control the dissemination of information concerning individuals. In this sense, it is essential to adapt the Law to this new reality to face these new challenges, preventing the digital world from becoming a place without rules, where transgressions do not entail civil and/or criminal responsibility.

As digital technology advances, new challenges arise that demand an adaptation of the Law to address them appropriately. Ensuring that the digital world does not become a lawless area is crucial. Regarding privacy protection, laws need to be updated to address specific concerns related to the collection, storage, and use of personal data in the digital environment. Aspects such as informed consent, purpose and limitation of data usage, information security, and the right to be forgotten are among the factors that need to be considered. Furthermore, it is essential to establish clear responsibilities for the entities involved in the digital world, including companies that collect and process personal data, online service providers, social networks, and even the users themselves. Civil and criminal liability should be applied when privacy violations or unauthorized disclosure of personal information occur.

The line between appropriate usage and potential abuse is very thin, especially concerning biometric data, particularly facial images, which can be employed for obscure, unethical, or even illegal purposes, such as discrimination or persecution, either directly or indirectly. From facial data, not only age and gender can be extracted but also ethnic origin and political ideals, making facial recognition susceptible to generating discrimination against certain groups of people.

According to current regulations, the processing of personal data should serve individuals. This means that the main focus should be on protecting individual rights and benefiting data subjects. The right to personal data protection is not absolute; it should be considered in relation to its function in society and balanced with other fundamental rights, following the principle of proportionality.

The current regulation respects all fundamental rights and observes the liberties and principles recognized in the Charter and enshrined in the Treaties, particularly regarding the respect for private and family life, communications, personal data protection, freedom of thought, conscience and religion, freedom of expression, and information.

The increasing economic and social development resulting from the functioning of the internal market has caused a significant rise in cross-border flows of personal data. The exchange of such data between public and private actors, including individuals, associations, and companies, has intensified both within the European Union and worldwide.

As a result of EU law, the national authorities of the Member States have been called to cooperate and exchange personal data among themselves to fulfill their functions or perform tasks on behalf of an authority from another Member State.

The objectives of Directive 95/46/CE remain valid; however, they have not prevented the fragmentation of data protection application at the EU level, nor the legal uncertainty or the widespread belief that significant risks to the protection of individuals persist, particularly concerning electronic activities. The differences in the level of protection of rights and individuals, especially the right to the protection of personal data in the context of data processing in the Member States, may hinder the free movement of personal data within the Union. Such differences can, therefore, constitute an obstacle to the exercise of economic activities within the Union, distort competition, and prevent authorities from fulfilling their obligations under EU law. These disparities in protection levels stem from differences in the implementation and application of Directive 95/46/CE.

Directive 95/46/CE was the legislation preceding the General Data Protection Regulation (GDPR) implementation in the European Union. While the objectives of Directive 95/46/EC remain valid, it faced significant challenges in its application, resulting in fragmentation and legal uncertainty regarding data protection.

One of the main issues with Directive 95/46/CE was its inconsistent transposition into the national legislation of Member States. Each country had the responsibility to implement the directive in its own legislation, leading to differences in approaches and data protection requirements throughout the European Union. This created fragmentation in the application of data protection laws and made it difficult to achieve coherence and harmonization in the digital single market. The Directive was unable to provide clear and comprehensive guidelines on how to address these emerging issues. The lack of a unified legal and regulatory framework led to a perception that individual rights were not adequately protected.

These concerns and challenges were addressed with the introduction of the General Data Protection Regulation (GDPR) in 2018. The GDPR is directly applicable in all UE Member States and aims to harmonize data protection laws and provide a higher level of protection for personal data. It addresses the gaps and deficiencies of Directive 95/46/CE by introducing stricter rules, enhanced transparency, greater accountability for organizations, and stronger rights for individuals. With the GDPR, the European Union seeks to promote security and trust in the digital environment, ensuring effective protection of personal data. The regulation specifically addresses activities carried out electronically, providing clear guidance and specific requirements for the processing of personal data in this context.

Keywords: Facial Recognition, Privacy, Anonymity, Right to Image, RGPD

Lista de Abreviaturas:

- ART. – Artigo

- CNPD - Centro Nacional de Proteção de Dados

- CC - Código Civil

- CRP - Constituição da República Portuguesa

- FRT – Fontes de Reconhecimento Técnico

- GNS - Gabinete Nacional de Segurança

- IA - Inteligência Artificial

- I.E – Isto é

- RF - Reconhecimento Facial

- RGPD - Regulamento Geral de Proteção de Dados

- TEDH - Tribunal Europeu de Direitos Humanos

- V.G - Por exemplo

Sumário

1. Introdução

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 ao 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 digitalizado.[1]

A capacidade do reconhecimento facial de identificar indivíduos de forma automatizada e em tempo real suscita preocupações sobre o controle e a utilização dos dados biométricos capturados. 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 tecnológica[2].

Neste 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 controle que as pessoas têm sobre suas informações pessoais, a preservação da sua identidade e o respeito à sua intimidade num ambiente cada vez mais conectado.

Ao longo desta pesquisa, analisaremos a legislação e regulamentações existentes relacionadas ao uso do reconhecimento facial e como essas medidas pretendem equilibrar a inovação tecnológica com a proteção dos direitos individuais. 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 violações de privacidade.

Desta forma, espero 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.

A presente dissertação tem por objetivo questionar o uso do reconhecimento facial, investigar as possíveis repercussões jurídicas com especial atenção ao direito à

[1] https://www.thalesgroup.com/pt-pt/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition.
[2] https://www.electronicid.eu/pt/blog/post/como-funciona-o-reconhecimento-facial-e-a-sua-seguranca/pt.

privacidade, identificar os riscos sobre os indivíduos e sobre a sociedade, e apontar medidas que devem ser tomadas para reduzir estes tais riscos, em observância aos princípios definidos na legislação de proteção de dados.

Visto que a imagem facial pode ser considerada como dado pessoal, investiga-se sobre o direito à privacidade, a sua origem e evolução jurisprudencial e legislativa na Europa. O estudo procura aprofundar a análise sobre a privacidade, na qualidade de direito fundamental da personalidade. Delineiam-se os seus contornos e o seu núcleo essencial, para relacionar a natureza sensível desses dados biométricos com as tecnologias de reconhecimento facial nas várias etapas do ciclo de vida da informação, e descrever de que maneira a privacidade e outros direitos fundamentais são afetados. À luz do RGPD e de interpretações provenientes de autoridades de proteção de dados, indicam-se medidas consideradas necessárias para minimizar os possíveis efeitos negativos decorrentes do uso dessas tecnologias. O uso das técnicas de reconhecimento facial impacta no atual contexto social, entra em conflito com as estruturas tradicionais da privacidade e da reserva da vida íntima do Ser Humano.

Nos últimos anos, existiu um aumento significativo do desenvolvimento de tecnologias de reconhecimento facial de modo que não é incomum encontrarmos câmaras de vigilância nas mais diversas situações do nosso dia a dia. A proliferação da internet, das novas tecnologias disruptivas apenas exacerbou os desafios para a proteção dos dados pessoais, com uma aceleração de tecnologias de vigilância e de monitorização dos indivíduos.

Atualmente, muitos dados pessoais são registados informaticamente e circulam pelos sistemas virtualmente sem limites temporais ou espaciais.

O atual uso dos meios tecnológicos fornece constantemente ao sistema informações sobre a vida dos indivíduos. Ao se realizarem compras na internet, ao se efetuarem pesquisas, são deixados dados de natureza pessoal (nomes, moradas, números de telefone, cartões bancários) que ficam à disposição do público em geral, podendo ser feito um uso ilícito dos mesmos, deste modo violando o nosso direito à privacidade e a nossa intimidade.

Esta escolha deste tema justifica-se essencialmente pela proteção da personalidade humana na atual sociedade de informação em que a proteção dos dados pessoais mediante essencialmente a técnica do RF e, em consequência, o direito à privacidade face o avanço tecnológico e suas consequências.

A natureza destes direitos, inerentes a própria existência da pessoa, obriga a que sejam tomadas medidas tanto normativas como outras que permitam a conjugação da convivência social no atual mundo virtual com a necessidade da proteção de dados pessoais, do direito à vida privada ou à intimidade.

No segundo capítulo, abordaremos o tema do Anonimato na Sociedade Digital em Portugal, uma matéria de considerável complexidade que tem suscitado intensos debates nos últimos anos. Serão discutidas as estratégias para mitigar tal anonimato, bem como as perceções de certos indivíduos de que a impossibilidade de manter o anonimato pode resultar na transgressão da esfera da privacidade. Abordar-se-ão os prós e contras subjacentes, além de se analisar a evolução desta problemática tanto em Portugal como a nível global.

No terceiro capítulo, explorar-se-á o vital e inalienável direito à proteção da vida privada. Emerge a preocupante perspetiva de que a aplicação do reconhecimento facial e da Inteligência Artificial poderá constituir uma franca violação deste direito fundamental. A Tecnologia será debatida como um potencial detrator da vida privada, dado que um volume crescente de informações de caráter pessoal é recolhido e arquivado sem o consentimento explícito dos próprios indivíduos. A atual economia de vigilância será examinada em profundidade, com uma análise equilibrada das suas vantagens e desvantagens, bem como das suas repercussões atuais e futuras. Serão delineadas medidas cabíveis, destinadas a restringir a coleta de informações apenas ao escopo estritamente necessário.

No terceiro capítulo, discutimos o preeminente direito à proteção da vida privada. Abordamos de maneira crucial a utilização do reconhecimento facial e da inteligência artificial, identificando a possibilidade de infringir diretamente esse direito fundamental. Aprofundamos a abordagem sobre a Tecnologia enquanto ameaça à esfera da vida privada. Isso decorre do aumento constante na coleta e armazenamento de informações pessoais, muitas vezes sem o devido consentimento do indivíduo em questão. Exploramos minuciosamente a atual economia de vigilância, analisando com rigor os prós e contras inerentes a esse cenário. Examina-se, com igual dedicação, as implicações imediatas e futuras, bem como as medidas apropriadas que podem e devem ser adotadas.

Nesse contexto, urge a implementação de ações para assegurar a coleta seletiva apenas das informações estritamente necessárias. O comprometimento com a

salvaguarda da privacidade requer a formulação e adoção de estratégias eficazes que mitiguem os potenciais impactos negativos dessa crescente tendência tecnológica.

O quarto capítulo do presente trabalho discorre sobre a temática da Privacidade no âmbito do Ordenamento Jurídico Português, bem como aborda a Evolução da Proteção de Dados. Este capítulo oferece uma análise detalhada da legislação que antecedeu o Regulamento Geral de Proteção de Dados (RGPD), identificando as suas lacunas que foram suplantadas pela atual legislação vigente. Além disso, explora as preocupações contemporâneas relacionadas com a privacidade e examina como os profissionais do direito em nosso país estão inclinados a abordá-las.

No contexto desta seção, são discutidos igualmente os princípios basilares estabelecidos pelo RGPD, sendo destacadas as implicações decorrentes do não cumprimento destes princípios. A análise minuciosa presente neste capítulo visa proporcionar uma compreensão ampla das implicações legais e éticas que envolvem a proteção da privacidade no contexto jurídico português.

O quinto capítulo da presente dissertação dedica-se à análise do direito à privacidade, bem como à exploração dos principais e atuais desafios políticos e económicos que emergem em face do desenvolvimento da Inteligência Artificial (IA). Especificamente, este capítulo aborda a ameaça contemporânea que paira sobre este direito fundamental, considerando a crescente vulnerabilidade das pessoas diante deste desafio recente.

Nesta secção, é realizada uma análise aprofundada das implicações trazidas pelo avanço da IA para o exercício do direito à privacidade. Destaca-se a delicada interseção entre os avanços tecnológicos, as políticas públicas e as considerações éticas, tudo isso em relação ao direito fundamental em questão. O propósito deste capítulo é promover uma compreensão esclarecedora das complexas dinâmicas que envolvem a privacidade no contexto contemporâneo, particularmente no que diz respeito ao impacto da IA.

No Capítulo 6, foram discutidos os aspectos referentes ao direito à imagem e à necessidade de consentimento por parte de indivíduos diante da proliferação de câmeras presentes em nosso cotidiano. Foram abordadas situações em que a obtenção desse consentimento não se mostra indispensável devido à concepção de "desnecessidade de consentimento". Adicionalmente, neste capítulo, foram examinadas

decisões de âmbito internacional que versam sobre essa matéria amplamente debatida a nível global.

Por fim, no sétimo capitulo, dedicamo-nos ao cerne da nossa investigação, o Reconhecimento Facial (RF), explorando a sua evolução tanto em Portugal quanto no cenário mundial. Além disso, foram tratadas as políticas e estratégias da União Europeia (UE) relativas à Inteligência Artificial (IA) e ao Reconhecimento Facial. Discutimos os inegáveis benefícios proporcionados por essa tecnologia recente que impacta nossas vidas diariamente. Não obstante, também efetuamos uma análise crítica das possíveis desvantagens associadas.

Destacamos, também, a questão da captação de imagens pessoais para fins de Reconhecimento Facial. Levantamos a indagação quanto à possibilidade de todas as imagens disponibilizadas na internet serem passíveis de apropriação por essa tecnologia.

2. O Anonimato na Sociedade Digital

Em termos conceituais o anonimato *"tem a ver com autonomia, nomeadamente a escolha individual de não divulgar o nome ao se comunicar por meio da Internet"*[3].

Este é o sentido amplo. Sob um ângulo de vista mais estrito, o anonimato na internet requer a observância de dois requisitos: (i) tornar uma ação não vinculável à identidade do agente, e (ii) fazer com que duas (ou mais) condutas realizadas pela mesma pessoa não tenham ponto de conexão entre si[4].

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

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

Uma das estratégias utilizadas para combater o anonimato na internet é a exigência de identificação dos usuários 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 a consideram uma violação da sua privacidade e liberdade de expressão.

---

[3] WEBER, Rolf H.; HEINRICH, Ulrike I. *Anonymisation*. London-Heidelberg-New York: Springer, 2012, p.35-36.

[4] CLARK, J.; GAUVIN, P.; ADAMS, C. Exit node repudiation for anonymity networks. In: KERR, Ian; STEEVES, Valerie; LUCOCK, Carole (Orgs.). *Lessons from the identity trail*: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009, p. 400.

2.1. Benefícios do Anonimato na Internet

Como pontos positivos deste anonimato digital podemos reter[5]:

Proteção da privacidade; o anonimato permite que as pessoas possam expressar-se livremente sem ter que revelar sua identidade ou informações pessoais. Isso pode ser um ponto importante para proteger a privacidade e evitar possíveis consequências negativas, como perseguição, retaliação ou discriminação.

Liberdade de expressão; 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.

Criação de comunidades; a possibilidade de interagir com outras pessoas anonimamente pode facilitar a criação de comunidades online, permitindo que indivíduos com interesses comuns se conectem e compartilhem informações.

Proteção contra ameaças online; em algumas situações, o anonimato pode ser importante para proteger as pessoas contra ameaças online, como assédio, stalking ou cyberbullying.

Incentivo à criatividade; o anonimato também pode 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.

Maior segurança em transações financeiras; o anonimato pode ser útil em transações financeiras online, garantindo que as informações pessoais e financeiras do usuário fiquem protegidas e não sejam expostas a possíveis fraudes ou roubos de identidade.
O anonimato na sociedade digital pode ter uma série de benefícios, desde a proteção da privacidade e da liberdade de expressão até a criação de comunidades online e maior segurança em transações financeiras. No entanto, é importante considerar os possíveis

[5] https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pt.htm

riscos e desvantagens do anonimato, como o potencial para o discurso de ódio e a propagação de informações falsas e prejudiciais.

2.2. O Anonimato 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 regule este uso do anonimato na internet. 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, crimes cibernéticos e difamação. Além disso, a jurisprudência e as decisões judiciais podem desempenhar um papel na definição dos limites e responsabilidades relacionados ao anonimato digital.

No entanto, é importante considerar que 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 livremente, 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.

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 sua identidade. Algumas jurisdições proíbem explicitamente o anonimato na internet, como a China, que exige que todos os usuários de redes sociais e fóruns de discussão revelem suas identidades reais. 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, que garante a liberdade de expressão. No entanto, as empresas de internet e os provedores de

serviços online podem ser obrigados a fornecer informações de identificação dos usuários em casos de crimes cibernéticos ou violações de direitos autorais.

A exigência de dano impede significativamente a execução de lei de privacidade. Na maioria dos casos de responsabilidade civil e contratual, deve-se estabelecer que os autores sofreram danos. A jurisprudência é uma confusão inconsistente e incoerente, sem princípios orientadores. Inúmeras violações de privacidade não são revolucionadas ou tratadas sob o argumento de que não houve nenhum dano percetível.

Em geral, 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. As pessoas que cometem crimes na internet utilizando pseudônimos ou perfis falsos podem ser identificadas e responsabilizadas criminalmente pelos seus atos.

2.3. Jurisprudência Internacional – O Anonimato na Internet

Existem diversas decisões judiciais em vários países que abordam o tema do anonimato digital e seu impacto no direito. Abaixo estão alguns exemplos de jurisprudência internacional:

Supreme Court of the United States, Doe v. Reed, de 24 de junho de 2010: neste caso, o tribunal decidiu que os signatários de uma petição para colocar uma lei em votação pública não tinham o direito de permanecer anônimos, pois a transparência do processo eleitoral era um interesse legítimo do Estado.

Tribunal Europeu dos Direitos Humanos, Von Hannover v. Germany, de 24 de junho de 2004: neste caso, 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.

Corte Suprema da Índia, Puttaswamy v. Union of India, de 24 de agosto de 2017: neste caso, o tribunal reconheceu o direito fundamental à privacidade como um direito autônomo protegido pela Constituição da Índia, incluindo a privacidade na internet.

Tribunal Europeu dos Direitos Humanos, Delfi AS v. Estonia, de 16 de junho de 2015: neste caso, o tribunal decidiu que um portal de notícias online era responsável pelos

comentários difamatórios postados por utilizadores anônimos em seu site, pois não havia tomado medidas razoáveis para prevenir ou remover o conteúdo ilegal.

Caso Sony Music Entertainment v. Does 1-40 (EUA, 2011): neste caso, a Sony Music processou um grupo de indivíduos que, utilizando pseudônimos, 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 autorais.

Caso Google Spain v. Mario Costeja González (Espanha, 2014): neste caso, um cidadão espanhol processou o Google e o jornal La Vanguardia por publicar uma notícia sobre 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 consentimento.

Caso Facebook Ireland Ltd v. Max Schrems (Europa, 2015): neste caso, 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 usuários da UE têm o direito de exigir que seus dados pessoais sejam removidos de plataformas digitais e que o anonimato é um direito fundamental para proteger a privacidade na internet.

Através destes Acórdãos podemos retirar algumas conclusões:

O direito ao anonimato na internet é reconhecido em muitos países como um direito fundamental, mas não é um direito absoluto. 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. os acórdãos analisados revelam a complexidade e a evolução das questões de anonimato, privacidade e proteção de dados na esfera legal. 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

3. O Direito à proteção da vida privada

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, está em causa, uma restrição ao direito à reserva da intimidade da vida privada e familiar, assim como, como referido por *Costa Andrade "a revolução científico-tecnológica trouxe consigo a massificação de meios sem precedentes de devassa"*[6].O direito em questão está previsto no art. 26.º da CRP e nos arts. 190.º a 194.º do CP, e ainda, com consagração no art. 80.º CC.

Trata-se, de um direito ao respeito pela vida privada[7], 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*".[8]

Estamos, portanto, perante um bem jurídico pessoal que assegura *"ao indivíduo o domínio sobre a sua esfera privada e, por vias disso, um espaço de isolamento e auto-determinação resguardado contra as intromissões e injunções da sociedade e do Estado".*[9]

O direito à proteção da vida privada[10] é um direito fundamental reconhecido pela maioria das constituições e leis em todo o mundo. Este direito é considerado uma extensão do direito à intimidade e protege os indivíduos de interferências indevidas na sua vida privada, família, lar e correspondência.

A reserva da intimidade da vida privada prende-se, maioritariamente, na 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

---

[6] 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.

[7] MEDEIROS, Rui e Cortês, António, "Artigo 16.º", p. 452.

[8] 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.

[9] ANDRADE, Manuel da Costa, "Artigo 192.º (Devassa da vida privada)", p.727

[10] http://fra.europa.eu/pt/eu-charter/article/7-respeito-pela-vida-privada-e-familiar

da vida privada e de controlar as informações que lhe dizem respeito quer sejam verdadeiras ou falsas[11].

O direito à proteção da vida privada permite que as pessoas controlem as informações que compartilham sobre si mesmas e protejam sua imagem e reputação. Protege também os indivíduos de vigilância ou monitoramento não autorizado, incluindo a coleta, armazenamento e uso indevido de informações pessoais por parte de empresas e governos. Esse direito garante às pessoas o controle sobre as informações que compartilham sobre si mesmas, bem como a proteção da sua imagem e reputação. Isso significa que as pessoas têm o direito de decidir quais informações desejam compartilhar e com quem, seja em conversas pessoais, ou por outros meios.

Além disso, o direito à proteção da vida privada protege os indivíduos de vigilância ou monitoramento não autorizado[12]. Isso inclui a coleta, armazenamento e uso indevido de informações pessoais por parte de empresas e governos. As pessoas têm o direito de saber se as suas informações pessoais estão a ser armazenadas e usadas, e têm o direito de consentir ou não com esta prática. No entanto, é importante observar que o direito à proteção da vida privada não é absoluto e pode ser limitado em certas circunstâncias, como quando há um interesse legítimo para proteger a segurança nacional, a ordem pública ou os direitos e liberdades de terceiros. Essas restrições devem ser proporcionais e estar de acordo com a legislação aplicável.

Essas restrições devem ser proporcionais, o que significa que devem ser necessárias e adequadas para alcançar o objetivo legítimo que justifica a limitação. Além disso, essas restrições devem estar em conformidade com a legislação aplicável, o que geralmente significa que devem ser estabelecidas por meio de leis específicas e claras. No entanto, mesmo quando existem restrições legítimas ao direito à proteção da vida privada, é importante garantir que tais restrições sejam necessárias e proporcionais.

Os governos e outras autoridades devem equilibrar cuidadosamente a proteção da segurança e dos direitos de terceiros com o respeito ao direito à privacidade individual. 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

---

[11] 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.

[12] MOTA PINTO, Paulo, (1993), "O Direito à reserva sobre a Intimidade e sobre a vida privada", Boletim da FDUC, LXIX.

prevenção de crimes, qualquer restrição deve ser proporcional e necessária para atingir um objetivo legítimo.

3.1. A tecnologia como uma ameaça à vida privada

A tecnologia pode ser uma 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 consentimento[13].
A vigilância e monitoramento são cada vez mais comuns, seja pelos governos, pelas empresas ou por indivíduos. Isso pode levar a uma sensação de invasão de privacidade e pode ter implicações sérias para a liberdade de expressão e associação.

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 econômica 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 mundo.

A vigilância e monitoramento podem interferir nos direitos fundamentais, como a liberdade de expressão, a liberdade de associação e o direito à privacidade, é, pois, necessário garantir que qualquer medida adotada seja proporcional e justificada e esteja em conformidade com as leis internacionais dos direitos humanos.

Podem ser tomadas uma série de medidas fomentadoras da segurança pública e que ao mesmo tempo respeitem a privacidade e a liberdade individual.
É fundamental 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

[13] https://assets.kpmg.com/content/dam/kpmg/br/pdf/2021/08/privacy-technology.pdf

equilibrar a necessidade de segurança com a proteção dos direitos individuais, evitando medidas excessivas e invasivas.

3.2. Implementação de medidas minimizadoras

Estabelecer mecanismos de supervisão independentes, como por exemplo; comissões de controle, 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. Isso envolve uma análise criteriosa dos pedidos de vigilância, assegurando que sejam necessários e proporcionais.

Implementar medidas de minimização de dados, ou seja, coletar apenas as informações estritamente necessárias para fins de segurança pública, evitando a coleta excessiva e indiscriminada de dados pessoais. Promover o uso de criptografia robusta e segurança de dados para proteger a privacidade das comunicações e 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 individuais.

Fomentar a conscientização e a educação sobre os direitos individuais, a importância da privacidade e a necessidade de equilibrar segurança e liberdade. Isso inclui informar os cidadãos sobre seus direitos e as medidas de proteção disponíveis.

Essas são algumas soluções que podem ajudar a conciliar a segurança pública com a preservação da privacidade e da liberdade individual.

4. Privacidade no Ordenamento Jurídico Português e Evolução da Proteção de Dados

4.1. 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. O artigo 26.º da Constituição prevê a *"proteção da vida privada e familiar, do domicílio e da correspondência"*, sendo que a lei define as garantias necessárias para a sua proteção.

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 RGPD é uma legislação abrangente que visa garantir a proteção dos dados pessoais dos cidadãos da UE e que se aplica a todas as empresas e organizações que processam dados pessoais de cidadãos da UE.

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 pessoais. No entanto, essa 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 dados[14].

[14] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm.

O RGPD estabeleceu normas mais rigorosas para a proteção de dados pessoais, incluindo o consentimento explícito dos titulares dos dados para o processamento dos seus dados, a obrigação de notificação de violações de dados e multas mais elevadas para organizações que não cumprem com as regras.
Em Portugal, a entidade responsável pela proteção de dados pessoais é a Comissão Nacional de Proteção de Dados (CNPD), que tem como missão garantir a proteção dos direitos e liberdades fundamentais das pessoas singulares em relação ao tratamento de dados pessoais.

Em 2019 foi aprovada a Lei nº 58/2019, que transpôs para o ordenamento jurídico português a Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.

A Declaração Universal dos Direitos do Homem, aprovada pela Assembleia Geral das Nações Unidas no ano de 1948 prevê no Art.º. 12º: *"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."* [15] .
Prevê que caso isto aconteça, a pessoa tem direito a ser protegida por este mesmo artigo referenciado. Este mesmo demonstra a importância do direito à privacidade alertando para a necessidade de garantia através da lei.

A nível interno, no Ordenamento Jurídico português, o direito à privacidade e de proteção de dados, bem como os mecanismos da sua garantia, estão consagrados em diversos instrumentos nos quais podemos referir a Constituição da República Portuguesa; a Diretiva 95/46/CE, de 24 de outubro; a Lei nº 67/98, de 26 de outubro, Lei de Proteção de Dados Pessoais; e, também, o Regulamento Geral de Proteção dos Dados.

A CRP no seu texto consagra vários Direitos pessoais, o direito à identidade pessoal, garantindo inclusive *"a identidade genética do ser humano (…) na criação, desenvolvimento e utilização das tecnologias e na experimentação científica"*, o direito ao livre desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom

[15] Cf. Declaração Universal dos Direitos do Homem, aprovada pela Assembleia-Geral das Nações Unidas, no dia 10 de dezembro de 1948, Artigo 12º.

nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar, e o direito a proteção contra quaisquer formas de discriminação. [16]

A CRP trouxe uma inovação oportuna em matéria de proteção de dados, ao prever sua utilização transfronteiriça, isto é, fora do país de residência do titular dos dados. Pois, face o direito de *"livre acesso às redes informáticas de uso público",* um direito constitucionalmente consagrado e os riscos associados a uma tal utilização de redes públicas de acesso, a CRP determinou que fosse definido por lei *"o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional."*[17] .

Nota-se uma verdadeira preocupação com a proteção dos dados. Assim, a CRP no artigo 35º, nº 7, estabelece que *"Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei."* Fica, pois, evidente a preocupação do legislador em considerar *"novas realidades, nomeadamente a utilização das Novas Tecnologias de informação e comunicação, criando as condições para que a circulação, partilha e tratamento de dados se façam também fora do espaço geográfico nacional."*

A Constituição de 1997, no artigo 35º, nº 4, proibia o acesso de terceiros [18] a dados pessoais.

Ainda sobre esta proteção constitucional de dados pessoais, defendem Canotilho & Moreira [19] *"nada mais é que a consequência lógica do alargamento do âmbito de proteção, regulando a proteção de todos e quaisquer dados pessoais, merecendo, por isso, os ficheiros manuais uma proteção idêntica à prevista no texto constitucional para os ficheiros automáticos."*

Os juristas portugueses *Canotilho e Vital Moreira* defendem que a proteção constitucional de dados pessoais em Portugal deve ser vista como um direito fundamental autónomo, que se fundamenta na dignidade da pessoa humana e no direito à reserva da vida privada.

Para estes autores, a proteção de dados pessoais é uma componente essencial do direito à privacidade, na medida em que a utilização abusiva ou excessiva de dados pessoais pode comprometer seriamente a autonomia individual e a dignidade da pessoa. Assim, a proteção de dados pessoais deve ser vista como um elemento fundamental da proteção da privacidade e da vida privada.

---

[16] Cf. Constituição da República Portuguesa (2010, artigo 26º, nºs 1, 2 e 3).
[17] Cf. Constituição da República Portuguesa (2010, artigo 35º, nº 6).
[18] Segundo CANOTILHO & MOREIRA (2014), "a noção de terceiros deve abranger todas as pessoas, (…) o pessoal informático que a lei ou os códigos deontológicos considerem responsável pelo ficheiro deve estar sujeito a um dever de sigilo profissional, já previsto na Lei."
[19] (2014, p. 185).

O reconhecimento de novos direitos, como é exemplo o direito a autodeterminação informacional, com igual valor constitucional tem gerado algum conflito entre direitos fundamentais, desafiando os Estados e seus poderes a introduzirem nos dispositivos normativos, como é o caso da Diretiva 95/46/CE, de 24 de outubro, e a atualizarem os já existentes, introduzindo novos princípios, com especial destaque para o princípio da proporcionalidade e da razoabilidade, como forma de garantir direitos opostos, de que são exemplos, o direito a informação ou mesmo a liberdade de expressão com o direito a privacidade.

O direito à privacidade, por exemplo, é fundamental para proteger os indivíduos contra a invasão nas suas vidas pessoais e garantir sua liberdade individual. Ao mesmo tempo, o direito à liberdade de expressão é essencial para a promoção da democracia e para permitir que as pessoas expressem suas opiniões e ideias livremente.
Portanto, os Estados e seus poderes devem tentar encontrar um equilíbrio adequado entre esses direitos fundamentais, introduzindo novos princípios e atualizando as leis existentes para garantir a proteção adequada dos direitos opostos.

O princípio da proporcionalidade e da razoabilidade é essencial nesse contexto, pois permite que os tribunais avaliem se a restrição de um direito fundamental é necessária e proporcional ao objetivo pretendido.
No entanto, é importante lembrar que a proteção dos direitos fundamentais não é absoluta e pode ser limitada em certas circunstâncias, como em casos de segurança nacional ou prevenção de crimes. É, portanto, fundamental encontrar um equilíbrio adequado entre a proteção dos direitos fundamentais e as necessidades legítimas do Estado em casos específicos.

A Diretiva 95/46/CE, de 24 de outubro, é o primeiro instrumento jurídico do Parlamento Europeu direcionado à proteção de dados pessoais singulares, ao seu tratamento e à livre circulação desses dados. A diretiva proporcionou a cada Estado-membros a possibilidade de transcrever, com alguma liberdade, o seu conteúdo, o que acabou por se traduzir numa produção avulsa de legislação sobre a proteção de dados, originando uma aplicação não uniforme pelos países da União Europeia (EU), gerando assim, uma insegurança jurídica que, para alguns, não favoreceu o desenvolvimento da economia.

A Diretiva 95/46/CE, de 24 de outubro, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, veio procurar conciliar o direito à informação com o direito à circulação de informação. Na verdade, influenciou decisivamente o panorama do direito interno de todos os países da União Europeia, obrigando-os a adoção de normas jurídicas de proteção de dados pessoais, onde não as havia, e uniformizando o nível de proteção em todos os Estados membros. Estabelecido esse nível comum de proteção de dados pessoais, a circulação da informação e pessoa passou a ser livre entre Estados-membros, obedecendo, porém, especiais requisitos, quando exportados para países terceiros.

No que se refere ao requisito do *"consentimento informado",* a diretiva não definiu uma tramitação rígida para o efeito, nem para a prestação da informação, nem para a recolha do consentimento. Todavia, entende-se ser indispensável, em qualquer caso, que a informação seja suficiente para que o consentimento seja considerado esclarecido. Pois, a informação quer oral ou escrita tem de exprimir em linguagem corrente e conter elementos iguais àqueles que um cidadão de padrão médio, no caso concreto, julgaria necessário para tomar qualquer decisão, e prestado para cada ato de tratamento de dados. Assim, conseguiu-se, portanto, inferir que a informação suficiente é um dos requisitos bastante para a validade do consentimento. Pelo contrário, se a informação não for suficiente o processamento efetuado para o tratamento dos dados passa a ser considerado não autorizado, tendo as correspondentes consequências civis e penais.

4.2. Regulamento Geral de Proteção dos Dados

A atual perspetiva do direito fundamental à proteção dos dados pessoais decorre essencialmente de uma evolução legislativa dos países europeus, nas 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). Em 1977, a lei Alemã passou a regular os arquivos de utilidade

pública e também privada. No mesmo período, a Suécia (1973), a Dinamarca (1978) e a Áustria (1978), legislaram no mesmo sentido;

- A segunda focou-se na tutela dos direitos fundamentais envolvidos nas relações das comunicações virtuais. A lei francesa de 1978, a lei do Luxemburgo de 1979 e as leis da Suíça da Islândia de 1981 e, foram no sentido da 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 Pessoal), 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, *"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")".*

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 foi transposto para a legislação nacional pela Lei de Proteção de Dados Pessoais (Lei n.º 58/2019), que estabelece as regras específicas para a proteção de dados pessoais no país e define as competências da Autoridade Nacional de Proteção de Dados (CNPD) na aplicação da lei.

O 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. Também estabelece as

obrigações dos responsáveis pelo processamento de dados e os direitos dos titulares desses dados.

O Regulamento Geral de Proteção de Dados, aprovado pela Lei nº 58/2019, de 8 de agosto, trata-se de um documento que veio permitir a transposição para a ordem jurídica nacional o Regulamento (UE) n.º 2016/679 do Parlamento e do Conselho Europeu, 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."*[20]

Com efeito, o Regulamento Geral de Proteção de Dados (2016), doravante designado RGPD, vem revogar a Diretiva 95/46/CE e criar um quadro legal mais claro e também mais coerente para a nova realidade. Este regulamento *"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 pública"*[21]

Já aqui, nota-se que o presente regulamento alarga o seu âmbito de aplicação para além do território nacional, não se aplicando apenas *"aos ficheiros de dados pessoais constituídos e mantidos sob a responsabilidade do Sistema de Informação da República Portuguesa",* sendo este regulado por disposições legais próprias, previstas na lei.

O RGPD não se aplica apenas aos dados pessoais constituídos e mantidos dentro do espaço europeu. A sua aplicação alarga-se aos dados transfronteiriços, abarcando todas as operações realizadas por empresas da União Europeia, ainda que com sede fora da união. Fica, desde logo, claro que o presente regulamento apresenta um âmbito de aplicação ainda mais alargado. Pois, a Lei nº 67/98, de 26 de outubro, aplicava-se também às operações de tratamentos ou recolhas de dados feitos fora do território nacional, mas, contrariamente ao RGPD, as entidades responsáveis tinham de ter a sua sede no território nacional.

Contrariamente à Diretiva 95/46, de 24 de outubro, com aplicação direta na ordem jurídica interna dos Estados-membros, o RGPD tem com 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

[20] Cf. RGPD (2016, artigos 15º e ss)
[21] Cf. RGPD (2016, artigo 2º.)

circulação de dados pessoais entre os Estados-membros, contribuindo para a realização de um espaço de liberdade, segurança e justiça. Pontanto, 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 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."* 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 violações.

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*."[22]

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"*[23] .

O RGPD vem esclarecer e atualizar várias questões em matéria de proteção de dados e contribuir para acabar com a insegurança jurídica criada pela Diretiva 95/46, de 24 de outubro ,que, como já se referiu anteriormente, permitia a que cada país transcrevesse, com relativa liberdade, para o seu conteúdo, para o seu ordenamento jurídico interno, traduzindo desta forma numa produção avulsa de legislação e sua aplicação pouco uniforme pelos Estados-membros, com impacto negativo no

[22] SALDANHA, (2018) "Novo Regulamento de Proteção de Dados", p. 15.
[23] SALDANHA, (2018), "Novo regulamento de Proteção de Dados", p. 15.

desenvolvimento económico, uma vez que vai gerar uma concorrência perversa entre os Estados, e deixa as autoridades nacionais sem capacidade de controlo.

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

O Despacho n.º 2705/2021, de 11 de março do Gabinete Nacional de Segurança (GNS) vem tratar da *"Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial.",* 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 usabilidade, a par da desmaterialização de mais procedimentos administrativos.

4.3 Princípios implícitos no RGPD

O Responsável pelo Tratamento de Dados tem obrigação de respeitar os seguintes princípios[24]:

1. *"licitude, lealdade e transparência*" - Os dados têm de ser processados de forma legal, justa e transparente;
2. *"limitação da finalidade"* - Os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não serão tratados posteriormente de forma incompatível com essas finalidades;
3. *"minimização de dados"* - Os dados são adequados, pertinentes e limitados ao necessário em relação à finalidade para a qual são tratados;
4. *"exatidão"* - Os dados são exatos e, sempre que necessário, atualizados;
5. *"limitação da conservação"* - Os dados não serão conservados durante mais tempo do que o necessário para o efeito;

[24] https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/principios-do-tratamento-dados/

6. *"integridade e confidencialidade"* - 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 acidental.

O princípio da licitude determina que só 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 pelo menos um Consentimento;

1. Execução de um Contrato;
2. Cumprimento de uma Obrigação Jurídica;
3. Defesa de Interesses Vitais;
4. Exercício de Funções de Interesse Público ou Exercício da Autoridade Pública;
5. Interesses Legítimos prosseguidos pelo Responsável pelo tratamento ou por Terceiro.

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 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 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.

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 pelo tratamento, 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 RGPD).

Este princípio é desenvolvido no artigo 12.º do RGPD, que 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.

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: 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.

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 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 RGPD).

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. 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 artigo 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 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.

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 acidental, 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 RGPD).

O princípio da responsabilidade consagrado no art.º 5.º/2, em conjugação com o art.º 24.º do RGPD exige, ainda, do Responsável pelo Tratamento de Dados, a aplicação de medidas adequadas e eficazes e de políticas de proteção de dados com base num critério de risco e de adaptabilidade e proporcionalidade das medidas que garantam o respeito pelos princípios e obrigações do RGPD e, quando solicitado, a sua demonstração às autoridades de controlo.

O princípio da proporcionalidade faz parte dos princípios gerais do direito da União e exige que os meios postos em prática por um ato da União sejam aptos a realizar o

objetivo prosseguido e não vão além do que é necessário para o alcançar, i.e., sejam utilizadas formas alternativas menos suscetíveis de afetar a privacidade das pessoas em causa.

5. O Direito à privacidade

5.1. Desafios atuais da Privacidade

Face aos desafios anteriormente explanados, a proteção dos dados pessoais bem como 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 outros[25].

Com a chegada deste 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 Unidas.

O desenvolvimento tecnológico, paradoxalmente, torna as pessoas mais vulneráveis a partir do momento em que sua exposição pública passa a ser constante. Isto 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. 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 Rodotà, s*urveillance is not a destin:. "Não se pode negar que o progresso tecnológico pode proporcionar benefícios sociais inimagináveis há até pouquíssimo tempo. Também não se pode negar*

[25] https://repositorium.sdum.uminho.pt/bitstream/1822/67115/1/ArtigoDtoPrivBD.pdf

a irrefreabilidade de tal progresso, mesmo que este não se apresente com prognósticos somente positivos."

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.
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, *Canotilho & 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."*

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".*

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 (CRP), "*A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação",* bem como em inúmeras cartas europeias e internacionais.

Este direito de personalidade está diretamente ligado ao princípio norteador do ordenamento jurídico português ,o da dignidade da pessoa humana baseado pressuposto que ela 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: "*Todos devem guardar reserva quanto à intimidade da vida privada de outrem*".

Advoga Canotilho,[26] *"o sigilo que a Constituição consagra sobre os direitos que compõem a esfera privada do indivíduo é posto em risco"*, uma vez que, acrescenta o professor, *"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".*

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 conflituantes, mas revestidos da força jurídica, cuja restrição é proibida por lei. A sua resolução tem implicado, não poucas vezes, como que a restrição, ainda que proibida por lei, de um direito de forma a garantir outro direito e vice-versa, pautando pelo princípio de proporcionalidade.

A privacidade é um dos valores intrínsecos à natureza da pessoa humana, cuja proteção constitui uma das grandes responsabilidades dos Estados modernos e seus poderes. 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 não autorizado e utilização indevida por terceiros, violando assim o direito à privacidade. O direito a privacidade e os dados pessoais encontra-se, cada vez mais, sujeitos a maiores riscos de violação pela quantidade de informação e dados pessoais acumulados na Internet.

5.2. A Atual ameaça deste Direito

São poucos serviços na Internet que dispensam a recolha, armazenamento, tratamento e difusão de dados pessoais. Toda esta utilização deixa traços diversos

[26] 1997, p. 644.

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, encontramo-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 eletrônicos, muitos dos quais os telemóveis permitindo a quem as coletou usá-las de acordo com os seus próprios interesses. Isso 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 um objeto em vigilância constante.[27]

Com isso, as pessoas podem ser manipuladas (a partir de propagandas personalizadas, por exemplo), tendo as suas fragilidades mais privadas exploradas de modo a colocar em risco a liberdade e a democracia.
O problema estará no facto do computador facilitar a acumulação e a interconexão de informação sobre pessoas, criando condições para violação do direito à privacidade.

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 facilidade.[28]

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.

Consegue entender-se que os dados pessoais se converteram na nova matéria-prima do mundo económico. Como afirma *Clive Humby*[29] *"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."* Afirma ainda o matemático inglês, que assim como o

[27] RODOTÁ, (2008), p.19.
[28] Tribunal da Relação de Évora: Processo nº 789/13.7TMSTB-B.E1 (25/06/15), disponível em www.dgci.pt)
[29] Clive Humby é matemático e empresário na área de dados e estratégias. Autor de vários livros.

petróleo precisa ser refinado, os dados, quando analisados, são uma ferramenta poderosíssima, permitindo tomadas de decisões eficientes. Como afirma *Belleil,*[30] "*Diz-me quem és, lucrarei o suficiente para te poder oferecer gratuitamente este serviço".*

Na verdade, 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 referidos, 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 oposição[31] 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"*[32] como cita o autor *Guerra A.* na sua obra *"Informática e Privacidade"*.

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

[30] 2001, p. 22.
[31] Cf. RGPD (2016, artigos 5º e ss; 12º e ss.)
[31] GUERRA, A., (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.

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"*[33] .

[33] BELLEIL, (2001), p. 27.

6. O Direito à Imagem

6.1 O conceito de Imagem

"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"[34].

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. O retrato da pessoa humana não pode ser obtido e difundido sem consentimento da mesma, sendo estabelecido pelos artigos 81º e 340 º do C.C.

6.2. O consentimento da Pessoa retratada

Por outro lado, como refere o Professor José Gonzalez, "*não pode ser esquecida regra, dominus membrorum suorum nemo videtur, significa que nem qualquer consentimento é valido, ou que é o mesmo, que nem todo o consentimento legitima a intervenção na esfera jurídica de quem em tal assentiu."* De acordo, com o conteúdo que se extrai do preceito encerrado no artigo 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 publica[35].

Tratando-se deste modo de um limite de difícil materialização, outra solução não resta senão a não ser aquela que passa pelo recurso, como sempre sucede no preenchimento de conceitos em aberto ou indeterminado a casos concretos, refere o *Professor José Gonzalez.*

[34] COSTA, Adalberto, 1375, o direito à Imagem, Revista Ordem dos Advogados, 2012, Ano 72, volume IV.
[35] GONZALEZ, J. A., 2022, número 1 e 2, Revista da Faculdade de Direito, Universidade de Lisboa.

O consentimento previsto no art.º 81º do Código Civil, distingue-se do artigo 340º deste mesmo diploma, neste funciona como clausula de exclusão da ilicitude, 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 483º do CC, aquele que produz a lesão não tem o direito de a provocar apenas beneficia da tolerância daquele outro que a sofre.

Na hipótese do art.º 81º CC, decorre que a parte que beneficia do consentimento tem o direito de exigir que o outro suporte os efeitos jurídicos e factuais associados à sua execução. Abre-se uma exceção à regra contida no art.º 406º CC, dado tratar se de matéria que respeita a tutela da personalidade humana; o consentimento em causa é sempre revogável.

A falta de referência explicita, 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 79º CC tem utilidade porque através dele 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.

Não necessitando de consentimento as seguintes situações[36];

- Numa, as razões atinentes à própria pessoa retratada que justificam a desnecessidade de consentimento (cargo que a pessoa desempenha, notoriedade da pessoa);

- Estão em causa as razões ligadas à finalidade da captação/divulgação do retrato (exigências de justiça, fins didáticos, fins sociais);

- 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 publico).

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

[36] Gonzalez, J. A., 2022, número 1 e 2, Revista da Faculdade de Direito, Universidade de Lisboa.

As exigências *"de justiça, de policia*" determinam igualmente, a superfluidade do consentimento para a obtenção e difusão do retrato. A fórmula usada é claramente de alcance dúbio.

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.

Assim quando um espectador de um determinado espetáculo esta a ser filmado por um camara men apenas o pode fotografar se este anuir (expressa e tacitamente).

Qualquer uma das exceções ao art.º 79º nº 2, 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 nº 484 CC e 26, nº1 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."* No entanto, há exceções, quando um individuo, conscientemente ou não, permite que a sua fotografia seja captada num contexto publico ou similar, a proteção da imagem pressupõe, a obtenção do consentimento do visado no momento em que ela é obtida. No entanto, este princípio não é absoluto.

Vejamos, motivos de interesse publico e a inserção do individuo na categoria de figura publica 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 individuo suspeito de cometer um crime legitima deste modo a retenção da imagem.

No caso *Murray v. Reino Unido, 1944,* 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 terroristas.

De maneira diferente, já entendeu o TEDH, no entanto, constituir uma violação do artigo 8º da Convenção Europeia dos Direitos do Homem o caso em que a policia forneceu fotografias à imprensa, sem consentimento prévio dos visados, fotografias de indivíduos presos, ou acusados *(Sciacca v . Italia, 2005)*, 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 , 2009*), ou ainda o caso em que a exibição da fotografia de um individuo resultou da sua obtenção a partir de uma lista de most wanted persons *(Guiorgui Nikolaichvili v. Geórgia, 2009*) elaborada por entidades policiais.

Já, porém, a retenção por tempo ilimitado da fotografia do individuo 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, 2020).*

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.

O TEDH, considerou no caso *Reklos e Davourlis v. Grécia , 2009*, ter havido violação do artigo 8º a propósito da obtenção numa clinica , 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 indevido. De um igual modo, considerou-se ter havido violação do artigo 8º da CEDH nos casos *Hajovsky v. Eslovaquia , 2021,* no que respeita à publicação na imprensa de imagens não convenientemente desfocadas do requerente, e *Voldina v. Russia , 2021*, no que tange à falha das autoridades em proteger uma mulher contra a reiterada cyber violência do marido que criou perfil falso da mesma e publicou fotos intimas.

Já o caso, *Von Hannover v. Alemanha, 2012*, 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 art. 8º CEDH.

Em processos relativos à tomada pelas autoridades, para fins de prevenção criminal, de impressões digitais, dados biológicos, e perfis de DNA 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.

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 Homem.

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 parágrafo 2 do artigo 8º CEDH. As referências presentes nesse parágrafo 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.

7. Reconhecimento Facial

Os sistemas de reconhecimento biométrico operam remotamente sem conhecimento prévio da presença da pessoa relevante em determinada área. Eles 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. Essa abordagem permite a identificação de pessoas no mundo real, seja em situações reais ou em registros visuais, como filmes e imagens de segurança.

O facto de os sistemas de identificação biométrica e de reconhecimento facial possuírem estas características torna-os ferramentas muito interessantes para agentes públicos e privados[37].

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. 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. Em virtude desses atributos, não é de se estranhar que as forças policiais também demonstrem um profundo interesse na adoção desses sistemas.

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 –

[37] 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*, disponível em https://doi.org/10.1080/13600834.2022.2054076.

o chamado *"policiamento preditivo"* ou *"previsão policial"*[38]) e não com a atividade estatal envolvendo a perseguição de crimes[39].

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 perspetiva 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 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.

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.

---

[38] Sobre o policiamento preditivo ou previsão policial, cfr. : Simon Egbert/ Matthias Lesse Criminal futures: predictive policing and everyday police work, london, new York, Routledge, 2021

[39] 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)

Uma primeira fonte de inquietação refere-se às características técnicas e níveis de precisão dos sistemas e tecnologias[40].

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. Essa possibilidade de erro levou empresas de renome a saírem do mercado de tecnologias de reconhecimento facial.[41]

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 governança e supervisão pode agravar os desafios relacionados à precisão, segurança e ética no uso dessas tecnologias de identificação biométrica.

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

Por um lado, é percetível 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. Esse cenário pode resultar em implicações mais intrusivas para a privacidade individual e a segurança dos dados. Por outro lado, especialistas expressaram de maneira enfática 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

---

[40] Gabrielle M. Haddad , “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, 2021, pp. 891-918. Porém, fazendo menção a possíveis mecanismos para garantir a precisão das tecnologias de reconhecimento facial, cfr. Vera Lúcia Raposo, “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.

[41] Tambiama Madiega / Hendrik Mildebrath, Regulating facial recognition in the EU.

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 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.

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 equitativa[42].

7.1. A estratégia da União Europeia para a Inteligência Artificial e para os Sistemas de Identificação Biométrica

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,

[42] Tambiama Madiega/ Hendrik Mildebrath , Regulating facial recognition in the EU, cit., pp. 6-9.

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 controle das fronteiras devem ser abordadas no contexto da aplicação coerciva da lei.

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 europeia[43], 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 Europeia[44].

---

[43] 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.

[44] 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, per- mitindo 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.

Apesar da atualidade deste tema, existe um Ac. do STJ de 27-09-2017 que se refere ao reconhecimento facial, definindo este como o *"emprego de técnicas de fotografia forense avançadas que incluem identificação de padrões faciais, elaboração de um perfil antropométrico único e comparação com os padrões que não oferecem dúvidas. Por meio de software de edição fotográfica determina-se a correcção a aplicar sobre a imagem para, deste modo, poderprecisar a localização dos pontos de referência. Por meio de negatoscopio digital pode-se realizar sobreposições entre as imagens que oferecem dúvidas e as isentas de dúvidas, analisando a correspondência entre os pontos de referência"*[45].

Para proceder ao reconhecimento facial, é essencial, que o computador aprenda o que é um rosto, em geral, obtém-se treinado um algoritmo, normalmente uma rede neutral profunda, através do fornecimento de um elevado número de fotografias contendo rostos de pessoas em situações típicas.

Sempre que uma imagem é apresentada ao algoritmo ele estima a localização do desse rosto, com a repetição, o algoritmo vai melhorar a sua fineza, vai realizar um acerto, a vai acabar dor dominar a arte de detetar um rosto humano. Surge o reconhecimento humano que pode operar de diversas maneiras, mas é comum usar uma grande rede neutral 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 demais.

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 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.

---

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

No 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. A situação alterou-se drasticamente nos últimos anos. As análises do ADN tornaram-se mais rápidas e economicamente acessíveis a quase todos[46].

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.

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.

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. Isso 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 trás 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.

Além disso como já referimos traz também discussão sobre a questão da privacidade. A aplicação do reconhecimento facial ainda suscita incertezas concernentes à proteção da privacidade e à potencial utilização indevida das informações captadas. Nesse contexto, é imprescindível que tenhamos total transparência quanto ao propósito pelo qual esses dados são coletados. Além disso, é fundamental que se estabeleçam normas e regulamentações rigorosas para garantir a salvaguarda dos direitos individuais e a segurança dos dados. A disseminação indiscriminada e não autorizada de informações faciais pode acarretar consequências graves, como o risco de vigilância excessiva, discriminação, e até mesmo o uso mal-intencionado para atividades criminosas.

[46] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf

Por outro lado, é importante reconhecer que a tecnologia de reconhecimento facial também apresenta benefícios potenciais em várias áreas, como segurança pública, combate à fraude e aprimoramento da experiência do usuário em certos serviços. No entanto, para alcançar um equilíbrio adequado entre os benefícios e os riscos, é necessário implementar medidas sólidas de proteção de dados, garantindo o consentimento explícito dos indivíduos e a utilização restrita apenas para fins legítimos e éticos. Nesse sentido, é papel das autoridades governamentais e empresas trabalharem em conjunto para estabelecer diretrizes éticas, políticas e técnicas que preservem a privacidade e minimizem os riscos associados ao uso do reconhecimento facial. A conscientização e o engajamento da sociedade também são cruciais para que possamos aproveitar os avanços tecnológicos de forma responsável, respeitando os direitos individuais e garantindo um ambiente seguro e confiável para todos.

Com o aumento da adoção da tecnologia de reconhecimento facial, surge a responsabilidade tanto para os usuários bem como para aqueles que desenvolvem esta tecnologia de garantir o seu uso de forma responsável e ética. O sistema de reconhecimento facial não é apenas uma tecnologia isolada, pois envolve também as pessoas que o operam, aquelas que a ele estão sujeitas e o contexto em que é aplicado.

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 inteligentes [47] .

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.

O reconhecimento facial é uma categoria de software biométrico que mapeia matematicamente as características faciais de um indivíduo e armazena os dados como

[47] Floridi et al., 2017.

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. O software identifica 80 pontos nodais num rosto humano. 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 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 vídeo[48].

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. 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 perceções humanas com a imensa capacidade de processamento e armazenamento dos computadores[49] .

E cuja definição, de acordo com *Lavashov*, pode ser assim descrita:

"Facial recognition technology uses a photographic camera combined with facial recognition software. This software is able to detect and isolate human faces captured by the camera and analyze them using an algorithm that extracts identifying features. The algorithm identifies and measures "nodal points" on the face, which are defined by the peaks and valleys that make up human facial features. Using these measurements, the algorithm determines individual's identifying characteristics, such as distance between the eyes, width of the nose, shape of cheekbones, and the length of the jawline."[50]

A face das pessoas, constitui uma das biometrias mais aceitáveis, por causa da familiaridade, e especialmente porque a aquisição das imagens não é fisicamente

[48] https://www.techtarget.com/searchenterpriseai/definition/facial-recognition.

[49] 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.

[50] "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. , The Rise of a New Type of Surveillance for Which the Law Wasn't Ready (2013). Columbia Science and Technology Law Review, v. 15, p. 164, Fall 2013. Pp. 167-168.

intrusiva. A coleta das informações independe necessariamente do consentimento do sujeito e pode ser feita à distância, ou mesmo com a recolha de dados provenientes da internet e redes sociais. A sua utilização depende de algoritmos para identificar similaridades em características faciais, em aspetos como geometria e aparência. *Sara Smyth* acrescenta que, já 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.*"[51]

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 dados[52].

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. Tais entidades também não revelam que tipo de informação é coletada ou compartilhada, de modo que a principal preocupação se relaciona com a vigilância invisível praticada e o posterior uso para propósitos diversos e desleais, o que pode implicar abuso do poder informacional de que dispõem. Esse 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 inacessível[53].

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)[54].

---

[51] SMYTH, Biometrics, Surveillance and the Law: Societies of Restricted Access, Discipline and Control, pp. 24 e 25.

[52] Tamò-Larrieux, Designing for Privacy and its Legal Framework, pp. 149–5.
[53] Tamò-Larrieux, Designing for Privacy and its Legal Framework, pp. 8.

[54] 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.

O reconhecimento facial utiliza dados enquadrados na categoria de informações biométricas, conforme as definições do artigo 4º /14 do RGPD e artigo 3º/13 da Diretiva UE 2016/680, por abranger elementos resultantes de um tratamento técnico específico relativo a características físicas de uma pessoa singular e que permitem sua identificação.

Os dados biométricos permitem a identificação de um indivíduo com base em fato biológico específico, permanente, relativamente imutável e que dele não pode ser dissociado[55].

O artigo 9º 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 econômica e social[56].

A caracterização dos dados biométricos como dados sensíveis atrai proteções específicas. O artigo 9º/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 nº 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 público[57].

[55] 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.
[56] Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados.
[57] Regulamento UE 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - Regulamento Geral sobre a Proteção de Dados.

Nas hipóteses em que o titular participa da inscrição de seus dados nos sistemas biométricos, deve ser especificamente comunicado, na forma do artigo 13º 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 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 ciber ataques, 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 decentralizado, 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 apagamento*[58].

7.2. Prós e contras do RF

A vantagem primordial destas Tecnologias é a inegável contribuição para a realização da justiça e para a descoberta da verdade material [59].

[58] Opinion 03/2012 on developments in biometric Technologies.

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

Clive Norris, acrescenta que "esta forma de vigilância" torna -se mais democrática uma vez que todos ficam igualmente sujeitos à vigilância, livre de restrições temporais como no caso da presença humana[60].

Não podemos também esquecer o efeito preventivo que podem ter estas tecnologias, uma vez que, sabendo que estamos a ser *"vigiados"* poderão o número de crimes diminuir, isto por receio que através deste sistema se venha a descobrir a identidade do autor[61].

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 de pessoas [62], o que é positivo, uma vez que os agentes quando se encontram a patrulhar não conseguem constantemente vigiar o mesmo local [63].

Ademais, e sendo um fator a favor da utilização destas tecnologias, está o facto de os dados biométricos serem intransmissíveis de pessoa para pessoa, uma vez que assim é, é muito difícil que estes sejam imitados. Destarte, torna-se este um procedimento mais seguro do que o uso de palavras-passe e códigos de acesso, que podem ser perdidos, esquecidos e usados por outrem que não seja o seu titular [64].

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. O aeroporto do Changi, Singapura, está a introduzir Smart Gates com capacidade de RF para reduzir filas de

---

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

[61] Ibidem.

[62] NISSENBAUM, Helen e Introna, Lucas D., "Facial Recognition Technology. A survey of Policy and Implementation Issues", The Center for Catastrophe Preparedness and Response, pp.20-21, disponível emhttps://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy _and_Implementation_Issues.

[63] Ibidem.

[64] RODRIGUES, Sara Raquel dos Santos, "Desenvolvimento de um Sistema de Reconhecimento Facial", pp. 66-67.

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 auto-excluem 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 adopção 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 começo[65].

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

A grande diferença com os primeiros sistemas biométricos está no facto do Reconhecimento Facial não requerer permissão. Dificilmente se obtêm as impressões digitais de alguém sem a sua aceitação, e no caso do reconhecimento de voz só a gravação de centenas de horas permite dar alguma fiabilidade ao sistema. 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 aceitação.

[65] https://observador.pt/opiniao/reconhecimento-facial-democracia-4-0-0/.

Atualmente, as consequências do reconhecimento facial nas nossas vidas pessoais e sociedade como um todo ainda não estão plenamente compreendidas. O risco de perda de privacidade é apenas uma parte da preocupação; 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, 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 desconhecemos.

E apesar da introdução da norma europeia de Proteção de Dados (CNPD) pretender proteger os direitos dos cidadãos na Era Digital, a legislação relativa à instalação de sistemas de videovigilância, por exemplo, vai deixar de ter qualquer controlo prévio, prevalecendo a auto-regulação e abrindo caminho para uma adoção massiva. Um sistema generalizado de vigilância que usa Reconhecimento Facial alimentado por IA, representa ameaça ao respeito pela vida privada, entre outros Direitos e Garantias de um Estado de Direito.

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, China, 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 controle 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 legal. 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 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 funções. 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 socioeconômicas. Isso 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.

A tentação de muitos governos na adoção de um modelo como este 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.

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

A evolução tecnológica é inevitável, assim como o próprio respirar de um organismo. 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 importantes.

Contudo, é importante reconhecer que, apesar dos pontos positivos, a implementação do Reconhecimento Facial deve ser cuidadosamente regulamentada e monitorada. As preocupações sobre o abuso dessa tecnologia por parte dos governos para reprimir oposição política ou violar os direitos humanos são legítimas. Portanto, 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 de forma capaz de afetar a imagem, a intimidade, o bom nome, a vida privada, a igualdade é um problema de enorme dimensão.

Quer o reconhecimento facial se dirija à identificação de pessoas, que seja "apenas" um método de autenticação.

Basta que as redes neutrais tenham sido alimentadas sobre desiguais qualidades e quantidades de dados[66] , por ex., diferente número de faces de diversos grupos sociais.

Se v.g um sistema for treinado sobre milhões de rostos masculinos brancos e apenas milhares de rostos de mulheres ou de pessoas de outras raças, ele será claramente menos preciso relativamente a estes dois últimos grupos, isto significa, que nestes últimos dois grupos poderão 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 subjacentes[67].

Para mitigar, o máximo, possível, estas inexatidões 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"*[68].

Adrienne Yapo - Joseph Weiss, na obra *"Ethical Implications of Bias in Machine Learning"*, diz-nos 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 desejadas.

Os perigos de intromissão desnecessária e desproporcionada em *"direitos, liberdades e garantias",* em direitos de personalidade, oferecidos pelo enviesamento são, portanto mais que muitos.

Quando é certo que: "*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*

---

[66] Como refere Susan Leavy, Gender Bias in Artificial Intelligence, https://aristotle.ucd.ie/files/talks-2019/Susan-Leavy-gender-bias-and-ai.pdf.

[67] Nº 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.

[68] Artigo 9º, nº2 , Lei nº27/2021 de 17/05.

cada caso concreto e estabeleça processos destinados a evitar quaisquer preconceitos e formas de discriminação."[69]

Vejamos o sucedido em 2015, quando a aplicação Google Photos etiquetou duas pessoas de raça negra como gorilas[70].

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.[71]

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 dados[72] .

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 outros[73].

Pode acontecer ainda que, a variação da luz e o ângulodas imagens possa interferir no resultado, podendo conduzir a um resultado erróneo[74]. Ou seja, se não se conseguir garantir a qualidade e fiabilidade das imagens, pode, de facto, comprometer-se a exatidão dos resultados alcançados[75]. Ora, a qualidade de imagensretiradas 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 doreconhecimento facial uma vez que a má qualidade pode conduzir a uma incorreta identificação de um

[69] Artº 9 da Carta Portuguesa de Direitos Humanos na Era Digital.
[70] Google apologises for photos app´s racist blunder.

[71] DUONG, J. Hurtado, J. Kuntjoro , N. Mak, N. Maxwell, N. & Vu, B., "A Technological and Ethical Analysis of Facial Recognition ...", pp. 13-15.
[72] https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
[73] 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,
[74] SANTOS, Hugo Luz dos, "Inteligência Artificial e Processo Penal", Braga: Nova Causa, Edições Jurídicas,2022, ISBN 9789899026308, pp. 163-165.
[75] 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,

indivíduo[76]. Nestes casos a *"fidedignidade depende da exatidão dos meios tecnológicos usados"*[77].

Não obstante, com o avanço dos anos, tem havido um maior rigor nestas tecnologias, sendo que o risco de erro tem vindo a diminuir[78].

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 destes[79].

7.3. Captação de Imagem pessoal para o RF

Poderemos assumir que todas as fotografias que são colocadas na internet são suscetíveis de apropriação por quem controla o algoritmo? 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. 79º do CC., bem como atendendo à natureza de Direito, Liberdade e Garantia Pessoal 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 e 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 goza [80].

---

[76] FRA – European Union Agency For Fundamental Rights, "Facial recognition technology: fundamental rights considerations…", ob. cit., p. 10.
[77] FIDALGO, Sónia, "A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo", p. 142.
[78] FRA – European Union Agency For Fundamental Rights, "Facial recognition technology: fundamental rightsconsiderations in the context of law enforcement", pp. 33-34.

[79] Ibidem, pp. 28-29.
[80] 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?

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 nº2 do artigo 8º da Convenção Europeia dos Direitos do Homem *(ao enumerar as condições de que depende a legitima ingerência no gozo de um direito protegido através dele: the purpose test; the necessity test ; the balancing test. Ou, mediante o manuseio dos princípios orientadores, contidos nos nºs 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"* (Artº 79º nº2 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 (artigo 4º) e se estabeleça no nº1 do artigo 16º 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.

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

A proposta de Regulamento do Parlamento Europeu que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento de IA), 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 publica", 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 especifica , 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 nº2 , nº2 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) é 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 cidadãos.

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 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 monitoramento 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 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.

8. Conclusões

O potencial do RF 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.

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.

Este é uma tecnologia promissora, mas deve ser abordada com cautela e responsabilidade para equilibrar os benefícios com os riscos associados. 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, desta dissertação, 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. Ficou claro que o reconhecimento facial, apesar das suas inúmeras aplicações benéficas, pode representar uma séria ameaça à privacidade individual e coletiva. 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 e tomar consciência 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.

Notamos que 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. É 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.

É necessário um equilíbrio delicado entre o potencial benefício do reconhecimento facial e a salvaguarda dos direitos individuais e coletivos. A decisão de adotar ou restringir essa tecnologia deve ser fundamentada num debate amplo e inclusivo, considerando os valores fundamentais da sociedade e os princípios éticos que norteiam o nosso avanço tecnológico. Ainda há muito a ser explorado neste campo em constante evolução, e esta dissertação oferece uma contribuição para o entendimento dessas questões complexas e desafiadoras.

Bibliografia

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

- COSTA, Adalberto, *o direito à Imagem*, Ano 72, Revista Ordem dos Advogados, , volume IV, 1375, 2012.

- BELLEIL, A. , - "*Privacidade, o mercado dos dados pessoais: proteção da vida privada na internet".* Lisboa: Instituto Piaget, 2001.

- CASTRO, C. S., *direito da Informática, Privacidade e Dados pessoais*, Edições Almedina, SA, Coimbra, 2005.

- CLARK, J.; GAUVIN, P.; ADAMS, C. *Exit node repudiation for anonymity networks*. In: KERR, Ian; STEEVES, Valerie; LUCOCK, Carole (Orgs.). *Lessons from the identity trail: anonymity, privacy and identity in a networked society*. New York: Oxford University Press, 2009.

- CHEN, S., e Levy, D., *Facial Recognition Technology: Issues and Implementation,* 2020.

-DUONG, J. Hurtado, J. Kuntjoro , N. Mak, N. Maxwell, N. & Vu, B., "A Technological and Ethical Analysis of Facial Recognition", 2018.

-FIDALGO, Sónia. *A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo.* In Rodrigues, Anabela Miranda, Inteligência artificial no Direito Penal, Coimbra: Almedina, 2020.

-FRA – European Union Agency For Fundamental Rights, *"Facial recognition technology: fundamental rights considerations in the context of law enforcement".*

- HADDAD, M. Haddad , *"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, 2021, disponível em https://link.springer.com/content/pdf/10.1007/s10610-022-09512-y.pdf.

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

- GONZALEZ, J. A., número 1 e 2, Revista da Faculdade de Direito, Universidade de Lisboa, 2022.

- LEVASHOV, K. 164 COLUM SCI & TECH. L., Vol. XV.

- MARTINS, Lourenço , A. G. e Garcia Marques, J. A. M., 2006, (2.a ed. rev. e act.) *Direito da Informática*, Edições Almedina, SA, Coimbra.

- MARQUES, G., Lourenço, M. (2000), *Direito da Informática*. Coimbra: Edições Almeida.

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

- NISSENBAUM, Helen e Introna, Lucas D., *"Facial Recognition Technology. A survey of Policy and Implementation Issues"*, The Center for Catastrophe Preparedness and Response,https://www.researchgate.net/publication/228275071_Facial_Recognition_Technology_A_Survey_of_Policy _and_Implementation_Issues.

- NORRIS, Clive, *"From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control*", in "Surveillance as Social Sorting. Privacy, risk, and digital discrimination", Routledge, David Lyon, 2003, https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf.

- RODRIGUES, Sara Raquel dos Santos, *"Desenvolvimento de um Sistema de Reconhecimento Facial."*

- RODOTÀ, S., 2013, Vol. 4., No. 2., *"Some Remarks on Surveillance today"*, in European Journal of Law and Technology.

- PEREIRA, Rui Soares, Número 1 e 2, Número temático: Tecnologia e direito, Revista da Faculdade de Direito, Universidade de Lisboa, 2022.

- SALDANHA, N., 2018, Novo Regulamento Geral de Proteção de Dados.

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

- EGBERT, Egbert; LESSE, Matthias, Criminal futures: predictive policing and everyday police work, london, New York, Routledge, 2021.

- MOREIRA, Vital e CANOTILHO Gomes Canotilh, J. J. , 2014, Constituição da República Anotada.

- SMYTH, S., Biometrics, Surveillance and the Law Societies of Restricted Access, Discipline and Control, 2019.

- TAMÒ- LARRIEUX, A, Designing for Privacy and its Legal Framework, 2018.

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

- WEBER, Rolf H.; HEINRICH, Ulrike I. *Anonymisation*. London-Heidelberg-New York: Springer, 2012.

- WELINDER, Y, 2014. *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social.*

-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, disponível em https://doi.org/10.1080/13600834.2022.2054076.

Artigos sobre o tema

- 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

- https://diariodarepublica.pt/dr/lexionario/.

- https://repositorium.sdum.uminho.pt/bitstream/1822/67115/1/ArtigoDtoPrivBD.pdf.

- https://www.techtarget.com/searchenterpriseai/definition/facial-recognition.

- The Columbia Science & Techonology Law Review, 2013.
-https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf
-https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

-https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pt.htm

-https://observador.pt/opiniao/reconhecimento-facial-democracia-4-0-0/.

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

-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/.

-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.

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

-ttps://assets.kpmg.com/content/dam/kpmg/br/pdf/2021/08/privacy.

Legislação

- Carta Portuguesa de Direitos Humanos na Era Digital.

- Código Civil.

- Convenção Europeia dos Direitos do Homem.

- CRP, 2005.

- Declaração Universal dos Direitos do Homem, aprovada pela Assembleia-Geral das Nações Unidas, no dia 10 de dezembro de 1948.

- Diretiva 95/46/CE, de 24 de outubro.

- Lei no 58/2019, de 8 de agosto.

- Lei nº27/2021 de 17/05.

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

- 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)

-RGPD

Jurisprudência

- 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 do TEDH.

-Tribunal da Relação de Évora: Processo no 789/13.7TMSTB-B.E1 (25/06/15).