UNIVERSIDADE D
COIMBRA

Camila Ferreira dos Santos

# O NOVO ESTADO DE VIGILÂNCIA BASEADO EM TECNOLOGIAS DE RECONHECIMENTO FACIAL

## ENSINAMENTOS DO PASSADO, EXPLICAÇÕES DO PRESENTE, RESERVAS DO FUTURO

**VOLUME 1**

**Dissertação no âmbito do Mestrado em Ciências Jurídico-Políticas com Menção em Direito Internacional Público e Europeu orientada pela Professora Doutora Paula Margarida Cabral dos Santos Veiga e apresentada à Faculdade de Direito da Universidade em Coimbra**

Julho de 2023

UNIVERSIDADE D
COIMBRA

Camila Ferreira dos Santos

# O novo estado de vigilância baseado em tecnologias de Reconhecimento Facial

## Ensinamentos do passado, explicações do presente e reservas do futuro

# **The new surveillance state based on Facial Recognition Technologies**

## Lessons from the past, explanations of the present, and reservations for the future.

Dissertação no âmbito do Mestrado em Ciências Jurídico-Políticas / Menção em Direito Internacional Público e Europeu, orientada pela Professora Doutora Paula Veiga e apresentada à Faculdade de Direito da Universidade de Coimbra.

Julho de 2023

*Aos meus pais,*

*Aos amigos do coração,*

*À Doutora Paula Veiga,*

*Ao Doutor Eduardo Figueiredo,*

*A Coimbra,*

*O meu mais profundo e eterno obrigada.*

## RESUMO

Nos últimos anos, temos sido testemunhas de avanços significativos no campo da tecnologia, especialmente no que diz respeito à inteligência artificial. Uma das aplicações mais controversas e impactantes dessa tecnologia é o reconhecimento facial, que tem sido amplamente utilizado em diversos setores da sociedade. No entanto, esse uso generalizado também trouxe consigo uma série de questões ético-jurídicas principalmente no que diz respeito a privacidade, proteção de dados e discriminação, que precisam ser cuidadosamente analisadas e compreendidas.

Esta dissertação tem como objetivo investigar o novo estado de vigilância baseado em tecnologias de reconhecimento facial, abordando sua evolução histórica, o panorama atual e as implicações futuras. Para isso, iniciaremos examinando a história da tecnologia, desde suas origens até os avanços mais recentes em inteligência artificial. Além disso, será apresentada uma explanação técnica detalhada sobre o funcionamento desta nova tecnologia, com ênfase no reconhecimento facial.

Em seguida, faremos uma análise do enquadramento jurídico do reconhecimento facial nos planos internacional, europeu e transnacional. Serão abordados instrumentos jurídicos, diretrizes, opiniões de autoridades competentes e jurisprudência, que buscam regular o uso dessa tecnologia, levando em consideração as preocupações relacionadas aos direitos humanos e fundamentais.

Por fim, examinaremos as soluções trazidas pelo novo Regulamento da Inteligência Artificial, buscando compreender as medidas adotadas para lidar com os desafios apresentados pelo uso do reconhecimento facial. Além disso, analisaremos os aspectos que ainda demandam atenção e discussão no contexto atual, destacando as lacunas e os potenciais impactos para o futuro.



*Palavras-chave:* tecnologia de reconhecimento facial, inteligência artificial, regulamentação.

**ABSTRACT**

In recent years, we have witnessed significant advancements in technology, especially in the field of artificial intelligence. One of the most controversial and impactful applications of this technology is facial recognition, which has been widely used across various sectors of society. However, this widespread use has also brought forth a series of ethical, legal, particularly regarding privacy, data protection, and discrimination, that need to be carefully analyzed and understood.

This dissertation aims to investigate the new state of surveillance based on facial recognition technologies, addressing its historical evolution, the current landscape, and future implications. To achieve this, we will begin by examining the history of the technology, from its origins to the latest advancements in artificial intelligence. Furthermore, a detailed technical explanation of this new technology, with a focus on facial recognition, will be presented.

Next, we will analyze the legal framework surrounding facial recognition at international, European, and transnational levels. Legal instruments, guidelines, opinions from competent authorities, and jurisprudence that seek to regulate the use of this technology will be discussed, considering concerns related to human and fundamental rights.

Lastly, we will examine the solutions brought by the new Artificial Intelligence Regulation, seeking to understand the measures taken to address the challenges presented by the use of facial recognition. Additionally, we will analyze aspects that still require attention and discussion in the current context, highlighting gaps and potential impacts for the future.

*Keywords:* facial recognition technology, artificial intelligence, regulation.

## LISTA DE SIGLAS E ABREVIATURAS

**Ac.** - Acórdão

**ACLU** - American Civil Liberties Union

**AI/IA** - Artificial Intelligence/ Inteligência Artificial

**AIA** - Artificial Intelligence Act

**Al.** - Alínea

**AR** - Assembleia da República

**Art.** - Artigo

**BE** - Bloco de Esquerda

**BLM** - Black Lives Matter

**CAI** - Committee on Artificial Intelligence

**CCTV** - Closed-Circuit Television

**CDS-PP** - CDS Partido Popular

**CDT** - Center for Democracy and Technology

**CEDH** - Convenção Europeia dos Direitos Humanos

**CEN** - European Committee for Standardization

**Cf.** - Confrontar

**CNIL** - Commission Nationale Informatique et Libertés

**CNPD** - Comissão Nacional de Proteção de Dados

**CoE** - Council of Europe

**Coord.** - Coordenado

**DF** - Direitos Fundamentais

**DH** - Direitos Humanos

**DL** - Deep Learning

**DNA** - Ácido Desoxirribonucleico

**DUDH** - Declaração Universal dos Direitos Humanos

**EDPB** - European Data Protection Board

**EDPS** - European Data Protection Supervisor

**EDRI** - European Digital Rights

**EM** - Estados Membros

**EUA** - Estados Unidos da América

**FRA** - European Union Agency for Fundamental Rights

**G20** - Grupo dos 20

**GNS** - Guarda Nacional de Segurança

**GT29** - Grupo de Trabalho do Artigo 29º

**Ib.** - Ibidem

**IBD** - Identificação Biométrica à Distância

**IBM** - International Business Machines

**IL** - Iniciativa Liberal

**ISO** - International Organization for Standarization

**LAPIN** - Laboratório de Políticas Públicas e Internet

**LED** - Law Enforcement Directive

**LGPD** - Lei Geral da Proteção de Dados

**MIT** - Massachusetts Institute of Technology

**ML** - Machine Learning

**NASA** - National Aeronautics and Space Administration

**OCDE** - Organização para a Cooperação e Desenvolvimento Econômico

**OHCHR** - Office of the United Nations High Commissioner for Human Rights

**ONG** - Organização Não Governamentais

**ONU** - Organização das Nações Unidas

**Org.** - Organizado

**PAN** - Pessoas Animais Natureza

**PCP** - Partido Comunista Português

**PE** - Parlamento Europeu

**PEV** - Partido Ecologista "Os verdes"

**PIDCP** - Pacto Internacional sobre os Direitos Civis e Políticos

**PMEs** - Pequenas Médias Empresas

**PS** - Partido Socialista

**PSD** - Partido Social Democrata

**RF** - Reconhecimento Facial

**RGPD** - Regulamento Geral de Proteção de Dados

**RNA -** Redes Neurais Artificiais

**SIB** - Sistemas de Identificação Biométrica

**SIBD** - Sistemas de Identificação Biométrica à Distância

**SRF** - Sistemas de Reconhecimento Facial

**TEDH** - Tribunal Europeu dos Direitos Humanos

**TFUE** - Tratado sobre o Funcionamento da União Europeia

**TJUE** - Tribunal de Justiça da União Europeia

**TRF** - Tecnologia do Reconhecimento Facial

**TUE** - Tratado da União Europeia

**UCLA** - University of California, Los Angeles

**UE** - União Europeia

**UNESCO** - United Nations Educational, Scientific and Cultural Organization

**UNICRI** - United Nations Interregional Crime and Justice Research Institute

**VIP** - Very Important Person

**Vol.** - Volume

# INDÍCE

**NOTA:**

A tradução dos segmentos de obras doutrinais escritas em línguas que não a portuguesa citados na presente dissertação é da responsabilidade da autora da mesma.

## CONSIDERAÇÕES INTRODUTÓRIAS

O avanço tecnológico vertiginoso introduziu nossa sociedade a uma nova era, delineando paradigmas inovadores e desafiando a compreensão acerca dos conceitos de privacidade, controle e dinâmicas de poder. Nesse contexto de sociedades informacionais e baseadas em dados, deparamo-nos com as consequências das tecnologias emergentes, com relevo no campo do reconhecimento facial. Tais tecnologias inauguraram um estado de vigilância distinto, no qual os indivíduos são continuamente monitorados e suas identidades são capturadas e analisadas por algoritmos poderosos.

A atual sociedade em que estamos inseridos é caracterizada por um leque de termos e conceitos, tais como sociedade da informação[1], sociedade datificada[2], sociedade em rede[3], capitalismo de vigilância[4] e sociedade do controle[5]. Esses termos espelham diferentes aspectos da complexa paisagem social em que habitamos, na qual a tecnologia evolui em um ritmo frequentemente superior à nossa capacidade de apreender seu impacto em nossas vidas.

Uma característica proeminente desse panorama em constante mutação é a vigilância evasiva, seja por parte do Estado, seja por entidades privadas, que gradativamente moldou um mundo impulsionado pela coleta, armazenamento e processamento de dados, tornando-os os bens ativos mais preciosos do mercado. Esse fenômeno suscita importantes indagações acerca do equilíbrio entre os benefícios advindos dessas práticas e a possível violação dos direitos fundamentais, humanos e valores democráticos.

A tecnologia de reconhecimento facial, utilizada no contexto da vigilância, promete um mundo mais seguro, ao aprimorar processos de identificação e reconhecimento, suplantando a subjetividade inerente ao juízo humano. Não obstante, a tecnologia também revelou seu potencial para perpetuar práticas discriminatórias, tais como a transfobia, homofobia, misoginia, xenofobia, idadismo e racismo, pondo em causa a confiança em sua suposta objetividade. Desse

[1] COUTINHO, Clara, "Sociedade da informação, do conhecimento e da aprendizagem: Desafios para a educação no século XX1", 2011, 5-22.
[2] COULDRY, Nick, CAMPANELLA, Bruno, "Nick Couldry: Do mito do centro mediado ao esvaziamento do mundo social - as mídias e o processo de ratificação da sociedade", 2019, 77.
[3] CASTELLS, Manuel, "A Sociedade em rede", 1999, 45.
[4] ZUBOFF, Shoshana, "A Era do Capitalismo da Vigilância - A disputa por um futuro humano na nova fronteira do poder", 2020, 43-81.
[5] DELEUZE, Gilles, "Post-scriptum sobre as sociedades de controle", 1992, 219-226.

modo, instaura-se um acalorado debate em torno do emprego generalizado da tecnologia para fins de vigilância, especialmente no caso da biometria facial, a qual se encontra intrinsecamente associada a essas práticas discriminatórias e à invasão da privacidade.

Os estudos sobre tecnologia de reconhecimento facial remontam à década de 1960, quando um projeto de pesquisa liderado pelo cientista Woodrow W. Bledsoe, em colaboração com Helen Chan e Charles Bisson, visava programar computadores para reconhecer rostos humanos[6]. Desde então, a utilização dessa tecnologia na segurança pública, tem vindo a impulsionar o surgimento de uma sociedade de vigilância digital. Tal realidade apresenta semelhanças com a visão distópica descrita pelo britânico George Orwell em sua obra "1984"[7], na qual é retratada uma sociedade pós-guerra dominada por um regime totalitário, que suprime a privacidade dos cidadãos por meio do constante monitoramento exercido pelo "Grande Irmão" mediante o uso de "teletelas", dispositivos de vigilância instalados em espaços públicos e nas residências.

Nos últimos anos, temos testemunhado um crescimento exponencial dos mecanismos de poder relacionados aos dispositivos de controle. Câmeras de vigilância estão presentes em todos os lugares[8], sejam eles públicos ou privados, expondo o comportamento individual à análise das instituições de poder e às decisões sobre quem pode ingressar, sair ou permanecer em determinados espaços. A justificativa de uma maior segurança para a população ganhou força pós os ataques de setembro de 2001 em Nova Iorque.

A reflexão sobre o argumento da segurança no uso da tecnologia de reconhecimento facial nos remete a uma questão crucial: até que ponto esse discurso de segurança é válido e até que ponto ele pode ser usado como uma justificativa para medidas intrusivas e potencialmente violadoras dos direitos individuais. É importante reconhecer que o argumento da segurança pode ser empregado tanto por regimes democráticos quanto por estados totalitários, mas é no contexto destes últimos que sua utilização pode ser particularmente preocupante.

Os estados totalitários são conhecidos por sua tendência a explorar o medo e a ameaça de segurança para impor suas vontades sobre a população. Ao criar um ambiente de constante

[6] MAKHIJA, Yashoda; SHARMA e Rama Shankar. “Face recognition: novel comparison of various feature extraction techniques”, 2019, 1189-1198.
[7] ORWELL, George. 1984, 2003.
[8] BRANDÃO, Hemerson. “As cidades mais vigiadas por câmeras no mundo; poucas são do Brasil”, 2022.

vigilância e monitoramento, esses regimes buscam controlar e reprimir qualquer forma de dissidência ou oposição. A tecnologia de reconhecimento facial, com sua capacidade de rastrear e identificar indivíduos em tempo real, pode servir como uma ferramenta poderosa para a implementação dessa vigilância opressiva.

Nesse contexto, a frase emblemática de George Orwell em seu livro "1984", "Big Brother is watching you", ressoa com profunda relevância. Essa afirmação enfatiza a importância de refletir sobre o equilíbrio entre o poder e os direitos individuais em uma sociedade cada vez mais vigiada. A referência ao "Big Brother" ilustra o temor de um estado onipresente e autoritário que monitora constantemente as ações e comportamentos dos cidadãos. Essa visão distópica nos alerta sobre os perigos da vigilância indiscriminada e nos instiga a ponderar cuidadosamente sobre os limites e salvaguardas necessários para preservar a privacidade e a liberdade individual diante dos avanços tecnológicos.

Em face desse cenário desafiador, a presente dissertação propõe-se a aprofundar nas múltiplas dimensões da tecnologia de reconhecimento facial, investigando seus benefícios, riscos e considerações éticas. Por intermédio da análise de suas raízes históricas, das implicações sociais e do amplo debate em torno da vigilância, esta pesquisa almeja contribuir para a compreensão dos desafios e soluções potenciais perante esse novo estado de vigilância em constante mutação. Desse modo, almejamos enriquecer o diálogo em curso acerca do papel desempenhado pela tecnologia de reconhecimento facial na configuração de nossa sociedade e suas ramificações para a esfera da privacidade, discriminação e direitos individuais.

Na primeira parte da dissertação, será empreendida uma minuciosa exposição acerca da trajetória histórica da tecnologia até o advento da inteligência artificial. Especial ênfase será atribuída à análise dos termos técnicos pertinentes, visando proporcionar uma compreensão clara e concisa, considerando a sua não familiaridade como fundamento do conhecimento jurídico. Nessa etapa inicial, será devidamente esclarecido o raciocínio técnico subjacente às tecnologias de reconhecimento facial, a fim de se alcançar uma compreensão aprofundada do seu funcionamento efetivo. Partindo desse arcabouço tecnológico, torna-se lógico e imprescindível a apresentação da emergente sociedade de vigilância em massa, destacando-se os impactos consubstanciados na esfera da privacidade, proteção de dados e discriminação.

Na segunda parte da dissertação, efetua-se uma análise jurídica detalhada acerca dos instrumentos normativos disponíveis com o desiderato de regulamentar as tecnologias de reconhecimento facial em âmbito global. Dessa forma, além de examinar as diretrizes emanadas por órgãos internacionais, do Conselho da Europa e da União Europeia, proceder-se-á a uma abordagem transnacional, a fim de escrutinar tanto os diplomas normativos de natureza flexível quanto aqueles dotados de força coercitiva, notadamente explorando a jurisprudência e casos concretos que contribuam para a configuração de um panorama elucidativo quanto à tutela dos direitos fundamentais e humanos ante os prejuízos acarretados por essa tecnologia.

Por derradeiro, a terceira e última parte convoca uma análise abrangente acerca do primeiro regulamento de caráter vinculante sobre inteligência artificial no mundo, estendendo-se desde a sua gênese até o ponto atual, bem como explorando a proteção conferida às tecnologias de reconhecimento facial nesse intervalo temporal. A partir dessa perspectiva, promover-se-á um debate incisivo acerca da efetividade do referido regulamento na salvaguarda dos direitos afetados por essas tecnologias, discorrendo-se acerca dos desafios remanescentes que aguardam resolução e do impacto antecipado no âmbito global.

Ao término desta dissertação, almeja-se proporcionar uma análise abrangente acerca do estado atual da vigilância fundamentada em tecnologias de reconhecimento facial, examinando as lições extraídas do passado, as implicações atuais e as perspectivas futuras. A compreensão das ramificações éticas, jurídicas e sociais dessa tecnologia reveste-se de importância primordial para assegurar a proteção dos direitos individuais e promover um equilíbrio adequado entre segurança e privacidade em nossa sociedade cada vez mais interconectada e digitalizada. A presente pesquisa busca contribuir para o arcabouço de conhecimento sobre essa temática, a fim de subsidiar decisões informadas, políticas públicas e debates no âmbito jurídico, alicerçando-se na busca incessante pela preservação dos valores democráticos e dos direitos humanos em face dos desafios trazidos pelo avanço tecnológico.

# PARTE I

# TRANSIÇÃO ENTRE O PASSADO E O PRESENTE -

# DISCURSOS TÉCNICOS E JURÍDICOS

# CAPÍTULO 1

# O DESENVOLVIMENTO HUMANO E AS SUAS DIFERENTES RELAÇÕES COM A TECNO-LOGIA

*"Innovation is the outcome of a habit, not a random act."*

**Sukant Ratnakar**

O diálogo que intersecciona o desenvolvimento do Ser Humano e a Tecnologia data da própria existência do Homem, tendo em vista que a história do homem converge, desde o seu princípio, com a história das técnicas.[9] Entretanto, essa conversa acabou por ganhar outros contornos na década passada, resultado de significativos avanços da tecnologia e o consequente surgimento da Inteligência Artificial. Perante esta nova realidade mundana se mostrou pertinentemente necessário uma compreensão legítima de como o Ser Humano se relaciona com a Tecnologia e que tipo de impactos podem advir desta relação.

É pacífica a noção de que a Tecnologia tornou-se uma ferramenta indispensável para o cidadão (in)comum[10] que convive em sociedades que sejam consideradas desenvolvidas – nestas a tecnologia se tornou "omnipresente, ubíqua"[11]. Esta conseguiu infiltrar-se e consolidar-se no quotidiano da população de forma silenciosa, sem precisar de grandes juízos de consenso ou aceitação. A sua exigibilidade para pertença às redes de contatos, para ter acesso a informações, para resolver processos burocráticos ou até mesmo para indicar rotas para chegar a um certo destino concretizou e caracterizou a sua indispensabilidade.

Para que se possa abrir um debate centrado na confluência entre o Ser Humano e a tecnologia, há que se esclarecer a definição de ambos os conceitos. Num pólo deste diálogo encontra-se o Ser Humano, a espécie considerada humana. Estes, que segundo estudos da

---

[9] VERASZTO, Estéfano Vizconde / DA SILVA, Dirceu / MIRANDA, Nonato Assis / SIMON, Fernanda Oliveira, "Tecnologia: buscando uma definição para o conceito", 2009, 21

[10] Segundo o relatório publicado em dezembro de 2021, da União Internacional de Telecomunicações, o número estimado de pessoas que têm acesso a rede de internet cinge-se a 63% da população mundial - na África apenas um terço da população possui acesso à internet, em contrapartida, na Europa, 90% da população está conectada. – Dados acessados no dia 13 de novembro 2022 - <https://brasil.un.org/pt-br/161450-29-bilhoes-de-pessoas-nunca-acessaram-internet>

[11] KISSINGER, Henry / HUTTENLOCHER, Daniel / SCHMIDT, Eric, "A Era da Inteligência Artificial e o nosso futuro humano", 2021, 20.

origem das espécies de Darwin[12] evoluíram de um ancestral comum ao dos macacos há cerca de 3.5 milhões de anos atrás - sendo a primeira espécie capaz de andar de forma ereta a espécie *Australopithecus*[13]. Pela sua adaptação e desenvolvimento de características ao longo das épocas, são agora (cerca de 30.000 anos atrás) considerados pertencentes à espécie Homo Sapiens.[14] Como propõe KANT, vemos o homem enquanto ser natural racional situado numa encruzilhada entre a virtude e o prazer.[15]

Abordar o termo da tecnologia, por sua vez, mostra-se mais complexo e desafiador. A dicotomia do tema inicial se mostra necessária para compreender o conceito. Isso por que a história do desenvolvimento do homem se relaciona com a história das técnicas[16] - com a utilização de objetos (extracorpóreos) que eram transformados em ferramentas e que orientavam as pessoas nos diversos processos de desenvolvimento ao longo da história . Essas ferramentas vão progredindo consoante o avanço dos contextos socioculturais da humanidade - que se retroalimentam desta evolução.[17]

O desenvolvimento destas técnicas ao longo da história, foi inerente à existência do ser humano. Ou seja, não se limitou à fronteiras geográficas que possuíam (à priori) o monopólio da prática. Desde os primórdios da evolução humana, todos os povos que habitavam a terra, que se agruparam e percepcionam-se como uma "comunidade", independente de suas localizações no globo, acabaram por desenvolverem as suas próprias técnicas. Estas podiam divergir a partir da matéria prima fornecida, dinâmicas de trabalho e de aperfeiçoamento, dedicação ao seu aprimoramento, mas sobretudo por uma escolha de prioridade – O que a técnica deveria servir? O que ela deveria aprimorar e/ou transformar? Melhores formas de se defender de adversários, estruturas de proteção e abrigo, meios para alimentação? A técnica foi se desenvolvendo consoante as necessidades consideradas primárias e as capacidades intelectuais do ser.

---

[12] Cf. DARWIN, Charles "A origem das espécies", 1859 "o homem é um mamífero, que pela sua adaptação no mundo, caminham eretos". Esta teoria vem contrariar os cientistas ocidentais que acolhiam a tese de que o homem havia sido criado por Deus à sua imagem.

[13] Segundo DRAKE, Nadia, "A Evolução Humana".

[14] *Ibiden.*

[15] Como elucida RODHEN, Valerio, "O humano e racional na ética", 307.

[16] VERASZTO, Estéfano Vizconde / DA SILVA, Dirceu / MIRANDA, Nonato Assis / SIMON, Fernanda Oliveira. "Tecnologia: buscando uma definição para o conceito", 21.

[17] *Ib.*, 23.

A palavra "Tecnologia" vem a ser cunhada a partir do século XVII, quando GALILEU e DESCARTES começam a dar bases para uma modernidade científica e filosófica, incitando a fusão de *techné*, (originária do vocabulário grego, precisamente da palavra *techné*, sendo uma das variáveis de um verbo que elucida a transformação e a modificação, num contexto prático, sem grandes referências a uma contemplação científica – o *teuchô ou tictein*)"[18] e do *logos* (o sufixo "Logia" que também tem origem grega, de *logos*, remete à ciência, ao discurso, à teoria ou o estudo.)[19] Sendo assim, pode se conceber que a tecnologia passa a ser entendida como o estudo, os conhecimentos e as razões em torno da técnica – esta vista como a forma (maneira) de alterar as práticas com intuito de satisfazer às necessidades humanas.

Segundo KISSINGER, a humanidade sempre se preocupou com a exploração da realidade e a busca de conhecimento, com a plena convicção de que com a diligência certa, a aplicação da razão humana na resolução de problemas concretos, teria a possibilidade de alcançar resultados imensuráveis.[20] Ou seja, aquando de realidades desconhecidas, como as mudanças de estações, a concepção do tempo, a propagação de doenças, a interação do humanos com os animais, a gestão de alimentação – sempre coube ao ser humano o papel de raciocinar estas questões, adquirir conhecimentos sobre esses fenómenos, encontrar definições sobre esses conceitos e encontrar o caminho mais racional possível para lidar com estas situações. É precisamente nesta lógica de pensamento que a técnica acaba por ser desenvolvida pelo humano, para o auxiliar na adaptação à vida. Foi fruto da sua razão, do seu conhecimento e da sua contemplação dos fenômenos, que os humanos acabaram por utilizar da técnica, aqui posta como tecnologia, para atingir certos objetivos.

O polimento da pedra, o manuseio do fogo, a criação da roda, o desenvolvimento da agricultura, a manipulação dos metais, o despertar da cerâmica, a criação de alavancas e de embarcações, são apenas alguns dos primeiros exemplos de como o homem foi absorvendo e moldando a técnica nos seus primórdios.[21] Foi sempre na lógica de contemplação,

---

[18] Como evidencia RUDIGER, Francisco, "Tecnologia" in FILHO, Ciro, "Dicionário da comunicação", 2014, 442.

[19] *Ib.*

[20] KISSINGER, Henry; HUTTENLOCHER, Daniel; SCHMIDT, Eric. "A Era da Inteligência Artificial e o nosso futuro humano"22.

[21] ARAÚJO FARIAS, James Magno, "Direito, Tecnologia e Justiça Digital: O uso de ferramentas digitais em busca da razoável duração do processo em Portugal e no Brasil", 2022, 19.

experimentação e aprimoramento, guiados pela razão inerente ao ser, que a tecnologia vai ao longo dos anos se desenvolvendo e revelando o seu impacto na vida humana. Com o domínio (temporal) da técnica, os seres humanos começaram a se agrupar em comunidades e desenvolver a agricultura com o auxílio dos animais. A partir da produção de bens, houve espaço para as trocas, e assim também vem a surgir o comércio. Foi então, a partir dessa base, que foram criadas as primeiras cidades e civilizações datadas (4.000 a. c. - Fins do período neolítico).[22]

Com maiores condições de vida proporcionadas pelo avanço tecnológico, a população que habitava a terra teve uma crescente exponencial[23], o que permitiu que outras problemáticas fossem encaradas pela razão e pela técnica. É desse interesse que surge a matemática, as primeiras formas de comunicação, o estudo da astronomia, a análise geográfica, a preocupação com a arquitetura e construção de grandes estruturas, a medicina, a biologia e diversos outros ramos de estudo.

Ao chegarmos na Idade Média, a tecnologia vem mudar de forma definitiva a maneira de vivenciar e encarar o mundo. É a partir da criação da bússola que se consegue fazer melhores expedições e criar bases para explorar-se o desconhecido. A pólvora possibilita uma técnica completamente nova para o uso e manuseio de armas, com capacidades avassaladoras de extermínio de adversários.[24] Nesta mesma época, e com enorme relevância atual, Guttenberg cria a imprensa que vem a ter um grande impacto por alargar o alcance de disseminação de informações, teorias e ideologias numa escala global.[25]

Posterior a isso, na Era Moderna, com o avanço da navegação e das trocas de conhecimento e informações, foi-se possível ir ainda mais longe. É a partir da Revolução Industrial em 1760 que as primeiras máquinas são criadas – estas, que alimentadas pela queima do carvão, viriam a ser o primeiro motor totalmente autônomo.[26] Este feito conseguiu alterar

---

[22] ABIKO, Kenya Araújo / PLÁCIDO DE ALMEIDA, Marco António / FERREIRA BARREIROS, Mário António, "Urbanismo: História e Desenvolvimento", 1995, 5.

[23] Como exposto em RODRIGUES, Pedro Eurico, "Tecnologias na Pré História", 2022.

[24] ROXO BELTRAN, Maria Helena / BROMBERG, Carla / TRINDADE, Laís dos Santos Pinto / SAITO, Fumikazu, "A Imprensa, a Pólvora e a Bússola: ciência e técnica nas origens da ciência moderna", 2017.

[25] KISSINGER, Henry / HUTTENLOCHER, Daniel / SCHMIDT, Eric, "A Era da Inteligência Artificial e o nosso futuro humano" 205.

[26] MARQUES FARIAS, Leonel. "Uso da energia ao longo da história: evolução e perspectivas históricas", 2011, 10.

drasticamente o desenvolvimento das cidades, sendo a porta de abertura à criação de novas tecnologias.

Foi a partir do surgimento destes motores que foi possível a criação dos primeiros veículos movidos a vapor. Por sua vez, estes proporcionaram uma deslocação da produção e de pessoas, internacionalizando cada vez mais as sociedades.[27] Como consequência a isso, as primeiras indústrias vêm a ser criadas, o comércio se intensifica e o modelo capitalista se solidifica. A sociedade se transforma numa sociedade de consumo e a mão de obra que antigamente era exclusiva a força humana (ou animal) agora é assimilada pelo trabalho das máquinas.

A partir desse contexto de grandes avanços da tecnologia uma nova área desta começa a ganhar um maior relevo – a computação e informática. Considerado o "pai da informática" por muitos historiadores, Charles Babbage criou no século XIX uma máquina analítica com capacidade de realizar cálculos matemáticos como a adição, subtração, divisão, logaritmos e afins.[28]

Os computadores, como atualmente os conhecemos, são fruto de diversas transformações e aperfeiçoamentos com base nos avanços das engenharias, da matemática e dos estudos tecnológicos. A primeira geração dos computadores remete a 1951, que demandavam um enorme consumo de energia, eram extremamente caros e requeriam um grande espaço físico para exercerem as suas funções – sendo estas diminutas quando comparadas às diversas tarefas que um computador desempenha hoje.[29]

Cerca de 20 anos depois da criação do primeiro computador, surge um modelo mais compatível e logisticamente menos complexo, com o intuito de se transformar numa ferramenta indispensável na vida dos cidadãos. Estes diminuem o seu tamanho, dispõem de uma acrescida velocidade de processamento de dados, de infinitas funções e consomem consideravelmente menos energia do que os seus antecessores.[30] Dessa forma, o seu comércio foi facilitado, incentivado e acaba por atingir uma escala global.

---

[27] GODINHO, Renato Domith. "Como foi inventado o automóvel?", 2020.
[28] ROBALO SANTOS, António. "Gestão estratégica: conceitos, modelos e instrumentos", 2008, 56.
[29] SOUZA, Thiago. "História e Evolução dos Computadores".
[30] *Ib.*

Os computadores, desvirtuando das suas premissas iniciais, acabaram por se tornar um relevante canal para disseminação de informação. Substituindo os meios tradicionais (telefones, jornais, telégrafos), a criação da *World Wide Web* em 1989 por Tim Banners-Lee[31] vem a ser concebida como o marco do desenvolvimento da Internet, que agora saía dos laboratórios, governos e da academia, e era distribuído para o público geral requerendo o acesso a computadores para seu uso. A internet, no seu princípio, era utilizada como um recurso de comunicação (através de trocas de e-mails) e também para o acesso à informações. O seu desenvolvimento ao longo dos anos a possibilitou a absorção de mais recursos e formas de utilização, estendendo sua utilização e estando agora presente em todos os "objetos e coisas que tragam valor".[32]

Foi precisamente nesse contexto que começamos a assistir aquele que pode ser considerado o expoente máximo da tecnologia (até hoje vivenciado): o desenvolvimento da inteligência artificial (que será pormenorizado no próximo capítulo). Ao passo que os computadores iam se desenvolvendo, simultaneamente a isto, diversos cientistas focaram os seus estudos e investigações em criar uma técnica para a construção de entidades artificiais com capacidades cognitivas semelhantes às dos seres humanos.[33]

Foi Alan Turing que utilizou pela primeira vez o termo "inteligência artificial".[34] O matemático refere o conceito de forma inovadora em seu famoso artigo "Computing Machinery and Intelligence" (1950) no qual propôs o desafio *"Can Machines Think?".*[35] Há mais de sete décadas Turing afirmou que "podemos esperar que as máquinas vão competir com todos os homens na área da inteligência". Seu empenho foi entrever se seria possível construir uma máquina capaz de simular a inteligência, ideia que foi concretizada posteriormente, como aponta Doura Kaufmann.[36]

---

[31] PENATTI, Giovana "25 anos de World Wide Web: as primeiras aparições de tudo que forma a internet hoje", 2014.

[32] *Ib*. Aqui podemos falar da "Internet of Things" como " uma enorme rede de dispositivos conectados que possuem a capacidade de transferir dados através de uma rede sem a necessidade de interferência humana- completar explicação

[33] MEIRELES SEYLLER, Andrea. "A concepção da Inteligência Artificial na Administração Pública" in SADDY, André, "Inteligência Artificial e Direito Administrativo", 2022, 32.

[34]BUYERS, John. "Artificial Intelligence – the practical legal issues", 2021, 33.

[35] "As máquinas têm capacidade de pensar?" (Tradução livre)

[36] KAUFMAN, Dora. "A inteligência artificial irá suplantar a inteligência humana?",10, 2018,

Ou seja, o intuito foi criar ferramentas extracorpóreas (seguindo a lógica natural do desenvolvimento tecnológico) que pudessem simular a inteligência humana, replicando as habilidades cognitivas do ser – esta poderia resolver problemas, criar soluções e até mesmo tomar decisões no lugar do ser humano, fornecendo um auxílio que visa facilitar diversas áreas do cotidiano.[37]

Por mais que possamos ter acompanhado diversas inovações tecnológicas que causaram um enorme impacto no desenvolvimento humano, a IA difere dos outros exemplos citados supra pela velocidade extraordinária em que se estabeleceu, acusando, desde logo, a sua inevitabilidade - isso porque atualmente é quase impossível se pensar em tarefas que, ao serem percepcionadas no macro, não tenham sofrido sequelas da Inteligência Artificial – o futebol e o uso do "VAR"[38], as deslocações usando rotas pré-estabelecidas pela IA, a recomendação de músicas e filmes em plataformas de *streaming,* a predição de condições climáticas ou até mesmo os pagamentos virtuais são apenas alguns exemplos do seu uso diário.

Pela abrangência desta tecnologia no quotidiano dos dias atuais, o debate sobre o desenvolvimento da Inteligência Artificial ser positivo ou negativo se mostra irrelevante dado a sua omnipresença. Contudo, discutir os seus benefícios e principalmente seus pontos negativos é de extrema importância, mas a tentativa de conter o seu avanço é inútil, pois como todas as tecnologias desenvolvidas que auxiliam e facilitam tarefas desenvolvidas por humanos, a IA não irá fugir a regra e o seu uso é uma realidade que não será contida. Como afirma KISSINGER "Quaisquer tentativas de travar o seu desenvolvimento só servirão para entregar o futuro ao setor da humanidade que for suficientemente corajoso para encarar as implicações do seu próprio espírito inventivo."[39]

No entanto, a velocidade na qual esta disruptiva tecnologia se desenvolveu não conseguiu ser acompanhada pelas Ciências que sempre tentaram moldá-la, regulá-la e também

---

[37] TACCA,Adriano e ROCHA Leonel. "Inteligência Artificial: Reflexos no Sistema do Direito",2018, 59.

[38] O VAR (sigla em inglês para árbitro assistente de vídeo) é uma das tecnologias que estão sendo usadas na Copa do Mundo de 2022, no Catar. A função do VAR é auxiliar as decisões do árbitro de campo em lances específicos por meio das imagens captadas por câmeras espalhadas pelo estádio. Informação disponível em: https://www.techtudo.com.br/noticias/2022/12/o-que-e-var-veja-como-funciona-o-arbitro-de-video-no-futebol.ghtml Acessado em 28 de dez de 2022.

[39] KISSINGER, Henry; HUTTENLOCHER, Daniel; SCHMIDT, Eric, "A Era da Inteligência Artificial e o nosso futuro humano", 21.

explicá-la. A engenharia ainda se questionam como os algoritmos fazem certas previsões; a sociologia ainda se questiona qual será o impacto social que a irá advir desse desenvolvimento; a filosofia começa questionar a própria razão, a par de por exemplo, a existência de um ser (no caso robôs tecnológicos) capazes de realizarem tarefas como a de executar um adversário em um contexto de conflitos, sem estes atos serem acompanhados pela razão, emoção e discernimento; o direito não foge a lacuna, e agora persiste (e resiste) em dar respostas que possam tentar maximizar o uso destas tecnologias, sem que ao longo desse desenvolvimento, os valores e princípios básicos que sustentam um Estado de Direito no qual toleramos atualmente, sejam violados.

Como aponta KISSINGER "os humanos estão a criar e a fazer proliferar formas não humanas de lógica com um tal alcance e acuidade que, ao menos no discreto cenário em que foram destinadas a operar, podem exceder as deles. (...). Quando softwares intangíveis adquirirem competências lógicas e papéis sociais antes reservados a humanos (além de outros que os humanos nunca experimentaram), teremos de colocar a nós próprios uma pergunta fundamental: como é que a evolução da IA afetará a percepção, a cognição e a interação humanas? Qual será o impacto da IA na nossa cultura, no nosso conceito de humanidade, e, em última análise, na nossa história?"[40]

É precisamente nessa lógica que irá entrar o papel do Direito (e de todos os outros campos de reflexão) como mediador desta prática. Como o Doutor Henrique Antunes aponta: "Se o lugar do Direito é convocado pela dinâmica própria das relações sociais, o modo do Direito é, agora, desafiado pelo caráter disruptivo da inteligência artificial."[41] Contudo, cabe relevar a interdisciplinaridade que está em causa entre duas áreas tão distintas – o Direito e a Tecnologia. Nesta lógica, se revela necessário uma compreensão literal do que vem a ser a inteligência artificial, para que assim o Direito consiga absorvê-la, compreendê-la e regulá-la. Assim como o Direito já se deparou com a função de mediar certas áreas que lhe eram estranhas – como o ambiente ou as estradas – caberá aos juristas um conhecimento profundo deste novo campo, para que estejamos aptos para regular a IA, sem cairmos no erro de não compreendermos a sua extensão ou as problemáticas que advém do seu uso. É necessário percepcionar o Direito

[40] *Ib*.
[41] ANTUNES, Henrique Sousa. "Direito e Inteligência Artificial", 2020, 7.

como a ferramenta que irá guiar uma IA que se mostre efetivamente "inteligente" , pois como elucidou Stephen Hawking na abertura do Web Summit de 2017 "a inteligência artificial pode ser a melhor ou a pior coisa que já aconteceu à humanidade"[42]

## CAPÍTULO 2

## DECIFRANDO OS CÓDIGOS – UM "GUIA" SOBRE INTELIGÊNCIA ARTIFICIAL

*"Voice command: Alexa, is this the real life?*
*Alexa's response: Is this just fantasy, caught in a landslide, no escape from reality."*
**Voice Control do aparelho Alexa, desenvolvido pela Amazon**

### 1. INTELIGÊNCIA ARTIFICIAL - SUA ONIPRESENÇA E SUA CONSEQUÊNCIA

Segundo ANDREA SEYLLER "O fascínio do homem por seu cérebro e a possibilidade de compreendê-lo tem impulsionado a criação de máquinas inteligentes e a busca por seu aprimoramento conduz questionamentos sobre o fundamento do uso da inteligência artificial."[43] É precisamente nesta busca sobre o fundamento do uso da IA, que relevará o papel do Direito, impulsionando uma consciência de base que os "sistemas de IA devem ser projetados de maneira a respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade, devendo incluir a salvaguardas apropriadas para a garantia de uma sociedade justa".[44]

O que vem aumentar a complexidade da tarefa de uma compreensão plena desta nova área tecnológica é que, de facto, nem os seus próprios criadores (os programadores) têm uma real noção de como estas funcionam. Ainda não há uma explicação concreta do porquê certos

[42] Vídeo do Web Summit de 2017 disponível em: https://www.youtube.com/watch?v=H41Zk1GrdRg
[43] SEYLLER, Andrea D.M., "A concepção da Inteligência Artificial na administração Pública", 2022, 28.
[44] *Ib*., 41.

algoritmos predizem certos resultados[45], o que evidencia uma maior dificuldade de assimilação por parte do Direito sobre os meios que dispomos para a maximização dos seus benefícios através da regulação da mesma.

Este capítulo se apresenta com a pertinente função de conseguir englobar as informações fulcrais para uma compreensão do modo de funcionalidade amplo da IA, passando pelos seus subcampos e relevando o papel dos dados, para que consigamos perceber como o desenvolvimento da tecnologia do reconhecimento facial utilizada para vigilância de espaços públicos põe em causa diversos Direitos Fundamentais.

Para iniciar a explicação do conceito da inteligência artificial, vamos analisar a vida (fictícia) da Senhora Maria "Maria acorda todos os dias as 7:00 da manhã com a música *"I want to break free – Queen"*, pois tem um alarme configurado para tocar sempre este mesmo horário para a mesma ir trabalhar. Ela pergunta para a *Alexa* quais são as condições climática, e por descobrir que está chovendo, escolhe a capa de chuva amarela que comprou num anúncio do *Instagram* (na altura, Maria andava obcecada com o filme *"It"* e só pesquisava na internet informações sobre o mesmo, quando viu o anúncio da capa de chuva, sabia que deveria a comprar). Tendo em vista que as condições climáticas não eram as melhores, Maria pediu através do seu aplicativo *Uber*, um veículo para se deslocar até ao trabalho. No caminho, foi ouvindo uma playlist de músicas sugerida pelo *Spotify* - *Rainy days*. Durante o trabalho, pesquisou voos para ir viajar para Roma – notou que durante o dia, toda vez que utilizava uma rede social, apareciam publicidades sobre as famosas pizzas e pastas italianas. Antes de chegar em casa, passou no supermercado para comprar ingredientes para fazer uma Carbonara e ao pagar, utilizou seu cartão virtual. Chegando em casa, cansada do seu dia de trabalho, resolveu jantar enquanto assistia um filme. Ao acessar o *Netflix*, o mesmo sugere: "Cartas para Julieta", uma comédia romântica passada na Itália."

O dia da Senhora Maria não difere dos dias daqueles que utilizam essas tecnologias no cotidiano. A verdade é que no ano de 2022, nas sociedades em que a tecnologia já conseguiu chegar na maior parte da população, parece ser impensável viver sem o recurso a estes sistemas.

[45] EBERS, Martin, "Algorithms and Law", 2020, 48.

O facilitismo criado na execução de tarefas, na obtenção de informações e até mesmo no consumo, virou um grande aliado do indivíduo nos tempos atuais. Contudo, e como abordaremos ao longo deste texto, o recurso a estas tecnologias têm implicações na qual precisamos nos atentar.

As formas de utilização atual desta tecnologia, são inúmeras. Como referem SAMI HADDADIN e DENISA KNOBBE "a IA tem amplos campos de aplicação e grande potencial para ajudar com os desafios de, por exemplo, melhorar o diagnóstico e a terapia médica, encontrar maneiras eticamente aceitáveis de lidar com as mudanças demográficas e reduzir os efeitos de problemas ambientais, como mudanças climáticas ou poluição. Outras aplicações úteis são a promoção da sustentabilidade na vida cotidiana, por exemplo, otimizando o transporte e a logística, promovendo a agricultura sustentável ou reduzindo o trabalho físico extenuante no local de trabalho."[46] Como aponta MARTIN EBERS, as aplicações da IA vêm em diferentes formas "como assistentes pessoais em nossos smartphones, mecanismos de busca, aplicativos de tradução, programas de mineração de dados, sistemas de pontuação, sistemas de diagnóstico médico, algoritmos de preços, sistemas de negociação especializados e em manifestações físicas, como auto -dirigir carros, drones, veículos subaquáticos não tripulados, robôs cirúrgicos, robôs pessoais e robôs sociais".[47] Por mais que ainda não se mostre possível conduzir carros voadores como antigamente se fantasiava para os anos 2000, a verdade é que o mundo modernizou-se e digitalizou-se rapidamente nesta última década.

O desenvolvimento desta tecnologia tem sido acompanhado de um grande entusiasmo por parte da sociedade, levando em consideração de como o seu uso pode ser guiado para solução de problemas que há anos persistem em aberto. O seu uso no ambiente médico e na proteção ambiental evidenciam como a IA pode ter um papel decisivo no futuro incerto que se avizinha. Contudo o seu uso, que tem se estendido a quase todos os campos sociais e virtuais, também levanta diversas questões problemáticas.

---

[46] HADDADIN Sami e KNOBBE Dennis. "Robotics and Artificial Intelligence - The Present and Future Vision, 2020, 16.

[47] EBERS, Martin e GAMITO, Marta Cantero. "Algorithmic Governance and Governance of Algorithms - Legal and Ethical Challenges", 2021, 16.

Como toda tecnologia que se foi gerada ao longo da história, a IA não foge a regra em ter a sua função desvirtuada - seja para interesses próprios de maximização de lucros através de manipulação da consciência humana, para o monitoramento da população, pela desinformação e ameaça à democracia, pelo "técnico-solucionismo"[48], no crescimento de armas inteligentes, ou até mesmo pela utilização de algoritmos enviesados para tomada de decisões relevantes (como vaga de empregos, ou o destino de um órgão para um paciente). Os exemplos são inúmeros e confirmam a premissa de que a IA requer uma enorme assistência do direito para que consiga atingir os seus objetivos, sem que no processo coloque em causa direitos considerados fundamentais.

Para que consigamos entender como a IA efetivamente opera, vamos ter que nos apoiar na matemática para inferir a relevância que possui os algoritmos nesse processo. Isto porque eles são considerados a base do funcionamento da IA, sendo o elemento que dá azo para a ambição desta tecnologia - numa explicação simplista, podemos descrevê-los como cálculos matemáticos que objetivam um resultado, dependendo da intenção que lhes foi proposta.

Conforme propõe GILLESPIE, o conceito do algoritmo "refere-se a procedimentos codificados que, com base em cálculos específicos, transformam dados em resultados desejados. Podemos considerar como algoritmos as instruções de navegação ou fórmulas matemáticas usadas para prever o movimento de um corpo celestial."[49] Contudo, na IA, estes algoritmos são incorporados por novos sistemas tecnológicos alimentados de dados, para responder questões objetivas, como a sugestão de músicas numa plataforma de *streaming* ou a sugestão de anúncios de compras na internet, mas também para decidir questões subjetivas, complexas e que envolvem juízos sofisticados de valor, como: quem deve ser contratado para trabalhar em uma empresa; que contrato deve ser celebrado e em quais bases; qual a probabilidade de reincidência de determinado criminoso".[50]

Neste contexto, cabe relevar que a matéria prima utilizada pelos algoritmos é o *big data,* ou seja, a enorme quantidade de dados disponíveis no mundo virtual que, com o devido

[48] A possibilidade de solucionar qualquer problema, seja de natureza social, econômica ou política, através do recurso à tecnologia.
[49] GILLESPIE, Tarleton. "The relevance of Algorithms", 2014, 167-194.
[50] FRAZÃO, Ana. "Big data e impactos sobre a análise concorrencial."

processamento, pode ser transformada em informações economicamente úteis, que servirão como diretrizes e critérios para o processo decisório algorítmico.[51]Como propõe BJORN, "os algoritmos não podem funcionar sem dados; inversamente, sem algoritmos não seria possível "entender" muitas das massas não estruturadas de dados(...)".[52] Contudo, e como ele mesmo aponta, mesmo o algoritmo mais inteligente não fornece resultados utilizáveis, se a qualidade dos dados subjacentes (estrutura) for ruim. Relevando a importância de uma boa coleção de dados para um bom funcionamento dos algoritmos (veremos melhor infra).

Desta forma, com o expoente crescimento e acumulação de dados nos últimos anos, e com o simultâneo desenvolvimento dos algoritmos utilizados para a análise destes dados, a IA encontrou o seu caminho para atingir resultados imensuráveis. Nesta esteira, mostra-se relevante encontrar uma definição para o que vem a ser essa disruptiva tecnologia.

PAULO VICTOR ALVEO REIS aponta que a IA é compreendida como "a possibilidade das máquinas – aqui assimilada como computadores, robôs e demais dispositivos e sistemas com a utilização de eletrônica, informática, telemática e alcançadas tecnologias algorítmicas – executarem tarefas que são ou demandam características precípuas da inteligência humana, tais como compreensão de linguagens, reconhecimento de objetos e sons, raciocínio, solução de problemas etc".[53] KISSINGER completa expondo que a "IA é um veículo de muitos ramos e facetas da vida humana: investigação científica, manufatura, logística, transportes, defesa, justiça, publicidade, arte, cultura e mais".[54]

Contudo, por mais que esta tecnologia tenha se desenvolvido rapidamente, em diversos campos da sociedade, ainda "não há uma definição única de Inteligência Artificial que seja aceita pela comunidade científica", como aponta ANDREA SEYLLER.[55] Não há consenso (que se mostra necessário) entre os profissionais da tecnologia e os profissionais do direito.[56]

---

[51] *Ib.*

[52] STEINROOTTER, Bjorn. "The (Envisaged) Legal Framework for Commercialisation of Digital Data within the EU - Data Protection Law and Data Economic Law as a Conlficted Basis for Algorithm-Based Products and Services", 2020, 269-271.

[53] REIS, Paulo Victor, "Algoritmos e Direito", 2020, 133.

[54] KISSINGER, Henry; HUTTENLOCHER, Daniel; SCHMIDT, Eric, "A Era da Inteligência Artificial e o nosso futuro humano", 9.

[55] SEYLLER, Andrea D.M., "A concepção da Inteligência Artificial na administração Pública", 32.

[56] HADDADIN Sami e KNOBBE Dennis. "Robotics and Artificial Intelligence - The Present and Future Vision in Algorithms and Law, 41

Muitas das definições da IA, a ligam com a superação ou imitação da inteligência humana. Como exemplo o Oxford Dictionary a define como "o campo de estudo que lida com a capacidade da máquina de simular ou superar o comportamento humano inteligente".[57] Em consonância, John Buyers aponta que "em termos gerais, os sistemas artificialmente inteligentes aspiram, por meio das suas estruturas, ter a capacidade de processar dados não estruturados, extrapolá-los e adaptar-se e evoluir de maneiras comparáveis aos humanos"[58]

De forma simplista, conseguimos constatar que a IA é um "termo abrangente que se refere ao amplo ramo da ciência da computação que estuda e projeta máquinas inteligentes".[59] Contudo, a verdade é que o vasto campo de aplicação de IA se ramifica em variados métodos de execuções, sendo que a tarefa de conceptualização da mesma parece falhar em assimilar toda a sua infinitude. Diversos estudiosos, como MARTIN EBERS, expõem que numa perspetiva legal, isso pode ser problemático, enfatizando que "em qualquer regime regulatório deve se definir o que exatamente se regula, sendo que deve ser encontrada uma definição comum para o termo de IA".[60]

A proposta de um Regulamento de IA por parte do Parlamento Europeu define os sistemas de IA no seu texto como: "Um sistema baseado em máquina projetado para operar com níveis variados de autonomia e que pode, para objetivos explícitos ou implícitos, gerar resultados como previsões, recomendações ou decisões, que influenciam ambientes físicos ou virtuais."

Atualmente, o uso da IA tem se mostrado um mercado extremamente atrativo e lucrativo. Uma pesquisa do McKinsey Global Institute[61] sugere que pelo ano 2030 esta nova tecnologia pode contribuir com 13 trilhões de dólares por ano em valor de mercado. Apenas em 2020 as startups americanas desta nova tecnologia angariaram 38 mil milhões de dólares de financiamento, as suas congéneres chinesas, 25 mil milhões; as europeias, 8000 milhões.[62]

---

[57] Definição apresentada pelo Oxford Dictionary disponível em: https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence?q=artificial+intelligence consultado em 2 de novembro de 2020.

[58] BUYERS, John. "Artificial Intelligence – the practical legal issues", 3.

[59] EBERS, Martins. "Regulating AI and Robotics - Ethical and Legal Challenges", 2020, 41.

[60] *Ib.*

[61] WALTER, Robert e NOVAK, Marko. "Cyber Security, Artificial Intelligence, Data Protection and the Law", 2021, 6.

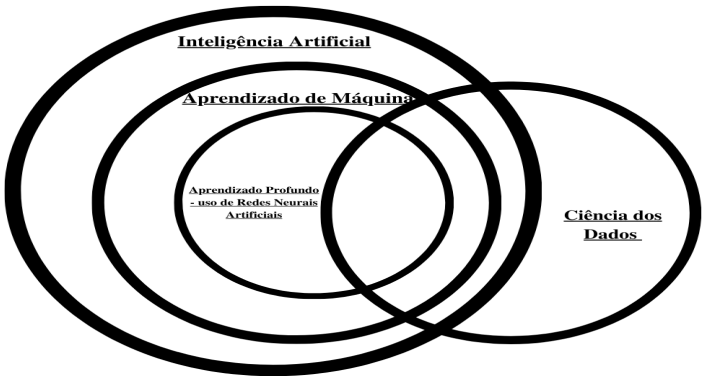
[62] PRIVATE EQUITY WIRE. "AI Startups Raised USD734bn in Total Funding in 2020" 2020.

Tendo seu uso totalmente absorvido pelo mercado, numa velocidade inimaginável, obviamente ensejou-se o cenário de reflexão desta tecnologia, sendo inevitavelmente convocado o Direito como mediador deste conflito. Contudo, para ser o ator de tal prática, é necessário antecipar-se aos conflitos em causa, ao menos no sentido de compreender de forma plena a extensão do problema para conseguir assimilá-lo, através das formas que a Inteligência Artificial consegue pôr em causa os valores que sustentam as sociedades, conduzindo a violações de direitos fundamentais.

Para tal, é necessário acessar o núcleo (i)mutável[63] da IA, àquelas ferramentas condutoras do objetivo, que se desenvolvem e se adaptam numa velocidade inimaginável, dificultando o largo processo de compreensão do objeto em causa. De dados à algoritmos, de aprendizagens de máquinas à redes neurais artificiais - os problemas e erros que prejudicam a IA também se devem ao mal uso destes instrumentos que precisam ser observados e incorporados à questão.

## 2. A RAMIFICAÇÃO DA INTELIGÊNCIA ARTIFICIAL E A IMPORTÂNCIA DOS DADOS

Para ajudar a organização dos conceitos que serão explicados, iremos nos auxiliar de um Diagrama de Venn inspirado na abordagem elaborado por LUIS BORGES GOUVEIA[64] que intersecciona a Inteligência Artificial com os dados, assimilando o aprendizado de máquina e, dentro deste, o aprendizado profundo que encontra a sua justificação nas redes neurais artificiais.




[63] São ferramentas com um desenvolvimento rápido, mas atualmente são as tecnologias que regem a IA e que são mais utilizadas pelas empresas - principalmente no que diz respeito à tecnologia do reconhecimento facial
[64] GOUVEIA, Luis Borges. "O Contexto do digital, a informação e a Inteligência Artificial", 2022.

Tendo em conta que o termo IA já foi pormenorizado no tópico interior, iremos partir para a elucidação da Aprendizagem de Máquina - o *Machine Learning.* Foi no ano de 1959 que um funcionário da IBM chamado Arthur Lee Samuel, considerado um pioneiro norte-americano no campo de jogos de computador e inteligência artificial, cunhou o termo *machine learning*, inaugurando um subcampo da IA.

Conforme iremos observar diversas vezes durante o texto, os dados disponibilizados atualmente cresceram de forma exponencial - estes podem ser fotos, músicas, palavras, vídeos, tabelas, números - e pela forma que as pessoas continuam a recorrer às sistemas de inteligência artificial no seu dia-dia, este número só tende a crescer. Neste contexto, o subcampo da IA denominado *machine learning* traz a promessa de direcionar o significado de todos esses dados, sendo uma ferramenta tecnológica que podemos utilizar para responder questões propostas por humanos, com os dados disponíveis que possuímos.

A tecnologia de ML pode ser dividida em duas grandes operações: a de *training*[65] e de *prediction*[66]. O treinamento refere-se ao uso de dados para informar a criação de um modelo preditivo. Este modelo, pode então ser usado para fornecer previsões sobre estes dados e responder às perguntas propostas. Como propõe MARTIN EBBERS, "em vez de programar máquinas com instruções específicas para realizar tarefas específicas, os algoritmos de ML permitem que os computadores aprendam com "dados de treinamento" e até mesmo se melhorem sem serem explicitamente programados.[67] Esta tecnologia possibilitou o desenvolvimento de sistemas com habilidades para detectar, entender e aprender com os dados que ele analisa. Além disso, o sistema se adapta na medida em que as informações vão sendo acumuladas,[68] sendo que o processamento destas informações são feitas em períodos de tempo menores do os da aprendizagem humana.[69]

Relativamente ao *Deep Learning* - aprendizagem profunda, este se refere a um subcampo da ML, ou seja, persiste a lógica de uma análise automatizada dos dados, mas através de uma

---

[65] Treinamento (Tradução Livre)
[66] Previsão (Tradução Livre)
[67] EBERS, Martins. "Regulating AI and Robotics - Ethical and Legal Challenges", 2020, 43- 44.
[68] TACCA,Adriano e ROCHA Leonel. "Inteligência Artificial: Reflexos no Sistema do Direito",2018, 60.
[69] KISSINGER, Henry; HUTTENLOCHER, Daniel; SCHMIDT, Eric, "A Era da Inteligência Artificial e o nosso futuro humano", 20.

ferramenta que propõe replicar a lógica de funcionamento dos neurônios cerebrais, transformando uma enorme quantidade de dados em informação útil, tal e qual ao funcionamento do nosso cérebro. Como ADRIANO TACCA e LEONEL ROCHA propõem: "sua capacidade engloba a percepção e a assimilação de múltiplos e complexos comportamentos e padrões, sendo que de forma intuitiva, o sistema descobre táticas para solução dos problemas que talvez o talento humano tenha levado muito tempo para aperfeiçoar. A partir dessa percepção, o sistema está apto a apresentar resultados para inúmeras tarefas, assemelhando-se com extrema precisão com aquelas tarefas desempenhadas pelos seres humanos."[70]

Este tipo de aprendizagem de máquina baseia-se em redes neurais artificiais para o seu funcionamento, que são "reproduções de funcionamento de neurônios humanos na busca de uma melhor solução para determinado problema."[71] Estas redes são comumente utilizadas para reconhecimento de imagens, e essa tarefa depende de uma complexa RNA, sendo que quanto mais neurônios ela tiver, mais fácil será dela intuir determinada figura. Como aponta ALEXANDRE DE SOUZA, "o papel mais complicado na programação não é de ensinar a máquina como sucede no ML, mas sim de prever as variáveis e nisso as RNAs possuem um importante papel, sendo capazes até mesmo de aprender sozinhas."[72] Um dos mais conhecidos sistemas de RNA é o algoritmo usado pelas buscas do Google, o qual seleciona tudo aquilo que entende que irá ter relação com determinado usuário - ele aprende por meio de exemplos.[73]

Por último, representando o ponto de intersecção entre a IA, o ML e o DL, temos aquele que vêm sido considerado o "novo petróleo"[74] do século XXI - os dados. Considerados "ativos preciosos nos dias de hoje"[75], os acervos de dados possuem um valor inestimável sendo objeto de disputa por milhares de empresas, órgãos de governos e corporações mundo afora.[76]

---

[70] TACCA,Adriano e ROCHA Leonel. "Inteligência Artificial: Reflexos no Sistema do Direito",2018, 60.

[71] DE SOUZA, Alexandre Magno Antunes. "Administração Pública 4.0 - A mudança por meio da Blockchain e da Inteligência Artificial", 70.

[72] *Ib.*

[73] *Ib.*

[74] STEINROOTTER, Bjorn. "The (Envisaged) Legal Framework for Commercialisation of Digital Data within the EU - Data Protection Law and Data Economic Law as a Conlficted Basis for Algorithm-Based Products and Services", 2020, 269-271.

[75] *Ib.*

[76] FARIAS, James Magno Araújo. "DIREITO, TECNOLOGIA E JUSTIÇA DIGITAL: O USO DE FERRAMENTAS DIGITAIS EM BUSCA DA RAZOÁVEL DURAÇÃO DO PROCESSO EM PORTUGAL E NO BRASIL", 127.

O Relatório do McKinsey Global Institute sobre "Big Data: A Próxima Fronteira para Inovação, Concorrência e Produtividade"[77] propõe que o *big data*[78] cria valor de várias maneiras: "permite a experimentação para descobrir necessidades, expõe a variabilidade de desempenho e melhora o desempenho; permite a segmentação da população para personalizar ações (por exemplo, para publicidade baseada em interesses); substitui/apoia a tomada de decisão humana com algoritmos automatizados; e facilita a invenção de novos modelos de negócios, produtos e serviços ou o aprimoramento dos já existentes."

Há que relevar, como aponta MOROZOV, que a IA só achou espaço para um expansivo desenvolvimento através da enorme quantidade de dados coletados por esse sistemas, através da disponibilização destes pelos usuários da internet, o que acaba por gerar ainda mais aprendizado para a máquina.[79] De acordo com o "Cisco" o volume de dados criados nos últimos anos é maior do que a quantidade produzida em toda a história. Esta produção dobra a cada dois anos, e só no ano de 2021 foram gerados 350 zettabytes de dados, o que corresponde a 35 trilhões de gigabytes[80]o que justifica o triunfo atual da IA.

Podemos dizer, sinteticamente, que os dados nada mais são do que um valor atribuído a alguma coisa, que quando coletados e estruturados se tornam úteis para passar uma informação.[81]Eles constituem a matéria-prima da informação, representando um ou mais significados que, de forma isolada não conseguem ainda transmitir uma mensagem clara.[82] Já no campo tecnológico, podemos analisar que os dados são expressões gerais que descrevem características das entidades sobre as quais operam os algoritmos. Estas expressões devem ser apresentadas de maneiras que possam ser tratadas por um computador. Neste caso, os dados por si só não constituem informação, a menos que esta surja do adequado processamento daqueles.[83]

---

[77] Relatório se encontra disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation Consultado em 14 de novembro de 2022.

[78] Se reporta ao conjunto dos dados que pertencem a um mesmo contexto e que são armazenados sistematicamente para que possam ser usados no futuro.

[79] MOROZOV, Evegny. "Bic Tech: a ascensão dos dados e a morte política. 2022, 184.

[80] CISCO. "A empresa que simbolizou a primeira grande onda da internet aponta para uma nova revolução de negócios baseada nas comunidades e na colaboração online", 2008.

[81] ESCOLA DE DADOS. "Para iniciantes: O que são dados?", 2022.

[82] GUIMARÃES, Leandro. "Qual a diferença entre dado e informação? Entenda agora!", 2022.

[83] Ac. do Tribunal da Relação de Évora - 82/20.9PACTX-A.E1

Segundo a Information Accountability Foundation existem quatro tipos de dados que formam a base das análises de dados. Podemos falar nos dados "fornecidos", sendo este meio o mais tradicional para armazenamento de dados, o que significa que os dados foram fornecidos conscientemente por indivíduos. Falamos também nos dados "observados", que são aqueles que podem ser extraídos, por exemplo, de um sistema de vigilância. Em terceiro lugar temos os dados "derivados", que são dados extraídos diretamente de outras fontes, para produzir novas classes de dados. Por fim, temos os dados "inferidos", que são produzidos normalmente pela análise dos dados existentes para realizarem certas previsões.[84]

A verdade é que a nova realidade mundana baseada no mundo digital, subordina os seus utilizadores à prestação de informações (cedência de dados) de sua própria dimensão existencial para pertença - seja para o acesso a novas redes sociais, seja para acompanhar um certo conteúdo ou informação, seja para se cadastrar em um novo serviço ou até mesmo para resolver algum processo burocrático. Quanto mais utilizamos a internet, os dispositivos móveis, os aplicativos tecnológicos, mais dados fornecemos - mas para quem, e para o quê?

A partir de uma lógica capitalista, é evidente concluir que os dados tornaram-se ativos preciosos para o mercado competitivo. Através das tecnologias de ML, os dados são percepcionados pelo mercado como inestimáveis informações sobre possíveis consumidores - que lugares frequentam, que música escutam, que lojas compram, para que locais viajam, quem são os seus amigos, quem é a sua família e por fim, quem é o seu consumidor. Este tipo de conhecimento profundo dos usuários obtido através da partilha de dados, se tornou um bem valioso para as empresas do mercado. A possibilidade de conseguir moldar produtos e serviços diretamente direcionados para o consumidor vem transformar a forma de consumo de maneiras inimagináveis.

Na caça aos melhores *Data Base*, o valor dos dados vem a ser definido pela sua qualidade - impondo uma extensa diversidade de dados em largas quantidades. Como aponta PETER NORVIG, chefe de ciência da Google, "a Google não detém melhores algoritmos do que as outras empresas e sim mais dados para que os algoritmos possam processá-los."[85] Pois

[84] BUYERS, John. "Artificial Intelligence – the practical legal issues", 28.
[85] Norvig, quoted by Scott Cleland, Google's "Infringenovation" Secrets, Forbes, October

quanto mais dados estiverem disponíveis para um algoritmo de aprendizagem, mais ele poderá aprender e mais preciso ele se irá tornar.[86]

Além do interesse empresarial, aponta-se o interesse por parte dos Governos na recolha, armazenamento e uso dos dados dos seus cidadãos. Muitos Estados atualmente tem adotado uma postura favorável a adoção de Dados Abertos[87] justificando o seu recurso a uma maior transparência de governabilidade e de disponibilização de informações relevantes para a população (taxa de desemprego, taxa de analfabetismo, indicadores gerais de educação e etc.)[88]. Contudo, há riscos inerentes à adoção deste tipo de modelo, como os custos da disponibilização continuada dos dados, a qualidade e usabilidade dos dados em causa, e, com um grande relevo, a privacidade e proteção dos dados pessoais.

Do interesse corporativo ao interesse governamental, suscita-se alguma reticência sobre como a aquisição e o uso dos dados podem extrapolar a sua finalidade, colocando em causa a nossa tão zelada privacidade. No pior dos cenários, a cedência de dados a estes entes podem incitar a criação de Estados totalitários vigilantes dos seus cidadãos e um grande controle por parte das corporações das vidas dos seus usuários.

Perante essas alternativas (nada razoáveis), assistimos nesta última década um grande esforço por parte das instituições na proteção destes dados, principalmente no que diz respeito aos dados pessoais (o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa[89]). Os instrumentos criados (debateremos os mesmos na próxima parte da Dissertação) concentraram os seus esforços em regular a recolha, o tratamento e a gestão dos dados, enfatizando a indispensabilidade do consentimento informado para tal, ou o respeito pelos princípios da proporcionalidade, necessidade e legalidade.

---

3, 2011,135. Disponível em: https://www.forbes.com/sites/scottcleland/2011/10/03/googles-infringenovation-secrets/#78a3795430a6. Acessado em 16 de novembro de 2022.

[86] EBERS, Martins. "Regulating AI and Robotics - Ethical and Legal Challenges", 2020, 61.

[87] "Os dados abertos (da administração) são as informações que os organismos públicos recolhem, produzem ou compram (também chamadas informações do setor público) e disponibilizam a título gratuito tendo em vista a sua reutilização para qualquer fim. A licença estabelece as condições de utilização" conforme a informação disponível em COMISSÃO EUROPEIA. "O que são dados abertos?", 2020.

[88] PORTAL DE DADOS ABERTOS DA ADMINISTRAÇÃO PÚBLICA. "Sobre dados abertos", 2020.

[89] COMISSÃO EUROPEIA. "O que são dados pessoais?", 2019.

Contudo, ainda são inúmeros os exemplos de como diversos serviços disponíveis atualmente encontram a sua disponibilidade na cedência de dados pessoais pelos seus utilizadores. Nessa lógica, não podemos dizer que o consentimento para a partilha destes seja consciente, se a consequência de evitar o compartilhamento seja a inacessibilidade a um certo serviço. Também não podemos dizer que a partilha destes dados seja devidamente clara, quando na maioria das vezes o próprio utilizador não recebe informações suficientes sobre de que forma os seus dados serão utilizados. Em consequência a isso, como apontam ROBERT WALTERS e MARKO NOVAK "um dos desafios a ser enfrentados pelos governos e reguladores da IA e da Big Data, será o de possibilitar o compartilhamento dos dados pessoais dentro das estruturas legais e éticas, objetivando a maximização dos benefícios dos dados de forma sustentável, minimizando os riscos e danos aos titulares destes."[90]

## 3. O RACIOCÍNIO TÉCNICO DO RECONHECIMENTO FACIAL

A Tecnologia do Reconhecimento Facial, apesar de ter sido potencializada pelo surgimento da Inteligência Artificial, precede o desenvolvimento desta. Foi na década de 60 que Woodrow W. Bledsoe realizou a primeira tentativa de imputar a uma máquina o reconhecimento de rostos humanos[91] - auxiliado de uma máquina rudimentar, Bledsoe registrava manualmente as coordenadas de características faciais como a linha do cabelo, nariz e olhos, associando-as a dados numéricos.[92] Em 1970, os pesquisadores Sakai, Nagai e Fujibayashi desenvolveram o primeiro computador capaz de confirmar a existência ou não de um rosto em uma imagem, sem a intervenção humana.[93] Na década de 80, diversos cientistas como Kirby, Sirovich, Matthew Turk e Alex Pentland, concentraram os seus esforços, para que com o auxílio da computação e algoritmos matemáticos, as máquinas conseguissem, de forma autônoma, reconhecer rostos em imagens com uma maior precisão.[94] Foi nos anos 90 que as TRFs começaram a ser comercializadas, com um uso preponderante para sistemas penais e órgãos governamentais, com

[90] WALTER, Robert e NOVAK, Marko. "Cyber Security, Artificial Intelligence, Data Protection and the Law", 72.
[91] LYDICK, Neil. "A Brief Overview of Facial Recognition", 2007, 1.
[92] *Ib.*
[93] GATES, Kelly. "The Past Perfect Promise of Facial Recognition Technology", 2004, 7.
[94] TURK, Matthew e PENTLAND, Alex. "Face Recognition Using Eigenfaces", 1981, 587.

o papel de emissão de documentos, como passaportes e documentos de identificação.[95] Contudo, foi a partir dos atentados de 11 de setembro de 2001 que demonstrou-se uma maior afluência no uso de TRFs por parte de agências governamentais, seja no controlo de fronteiras ou de eventos de grande magnitude, justificando-se o uso destas para um maior controle de segurança.[96]

Antigamente, a identificação de pessoas era operada por humanos, contudo, esta era associada com um número alto de erros. Depois utilizou-se de outros mecanismos como crachás, senhas ou até mesmo digital dos dedos.[97] Contudo com a digitalização do mundo real e a disponibilização de um enorme número de dados, os sistemas de Machine Learning (utilizando as técnicas de Deep Learning e as Redes Neurais Artificiais) popularizaram a introdução das TRFs nos mais variados campos - o sistema de autenticação de desbloqueio de smartphones "*Face ID"* da *Apple*; para o acesso a certos aplicativos ou sites; no controle de migração e processamento de check in nos aeroportos; para cadastros e aprovação de transações nos bancos digitais; para o pagamento de compras virtuais; para o acesso em ginásios, condomínios residenciais, ou até mesmo clubes. A expectativa é que esse mercado, estimado em 3 bilhões de dólares (em 2019), alcance 7 bilhões de dólares em 2024, segundo análise de uma empresa de pesquisa indiana chamada "*MarketsandMarkets*".[98]

Segundo o Article 29 Data Protection Working Party[99] propõe-se que o RF é "definido como o processamento automático de imagens digitais que contêm os rostos de indivíduos para identificação, autenticação/verificação ou categorização desses indivíduos", podendo ser executado através de vários métodos, como sistemas de videovigilância.[100] O Livro Branco de Inteligência Artificial da Comissão Europeia apenas postula duas dimensões do RF - a autenticação e a identificação, sendo que o Article 29 Data Protection Working Party ainda

---

[95] GATES, Kelly. "Our biometric future: facial recognition technology and the culture of surveillance", 27.

[96] MANN, Monique; SMITH, Marcus. "Automated facial recognition technology: Recent developments and approaches to oversight", 121-145.

[97] RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 2022, 5.

[98] MARKETS AND MARKETS. "Facial recognition Market by Component (Software Tools (3D Facial Recognition) and Services), Application (Law Enforcement, Access Control, Emotion Recognition), Vertical (BFSI, Government and Defense, Automotive), and Region . Global Forecast to 2025", 2020.

[99] ARTICLE 29 DATA PROTECTION WORKING PARTY. "Opinion 02/2012 on facial recognition in online and mobile services", 2012, 2.

[100] KOUROUPIS, Konstantinos. "Facial Recognition: a challenge for Europe or a threat to human rights?", 2021, 144.

menciona a categorização[101], e alguma parte da Doutrina[102] alberga ainda a caracterização[103] e a detecção. Contudo, essa presente dissertação irá focar no emprego das TRF para identificação de indivíduos em espaços públicos, em tempo real, de forma não direcionada, sendo essa prática àquela que está associada à diversas problemáticas (como iremos ver infra).

O processo para autenticação/verificação, comumente designado como correspondência "um a um", compara dois modelos biométricos (fotos ou vídeos) pressupostos de pertencerem a uma mesma pessoa para determinarem se a pessoa que aparece nas duas imagens é a mesma.[104] Ele é comumente usado para, por exemplo, o desbloqueio de celulares, ou para controle de fronteiras em aeroportos. Quando utilizamos estes sistemas de emprego, a tecnologia faz para o indivíduo a seguinte pergunta: "Você é quem você afirma ser?".

A segunda possibilidade, do reconhecimento para "identificação", o modelo da imagem facial de uma pessoa é comparado com muitos outros modelos armazenados numa base de dados para saber se a imagem dessa pessoa se encontra nessa base de dados - a pergunta que esta tecnologia dirige ao indivíduo é: "quem é você?"[105]. Neste modelo, o sistema, ao comparar o modelo da imagem da pessoa em questão com um banco de dados, irá inferir um resultado pautado em probabilidades estatísticas, através de um sistema de pontuação (*scoring*), buscando no banco de dados o modelo que possui a pontuação mais semelhante àquela que se quer identificar, de forma a declarar-se uma correspondência.[106] É justamente nessa parte do processo que pode ser desencadeado erros de identificação, pois o algoritmo oferece uma gama de potenciais correspondentes.

---

[101] "Se refere ao processo de estabelecer se os dados biométricos de um indivíduo pertencem a um grupo com alguma característica predefinida (...) não relevando sua identificação ou verificação, mas sim a atribuição deste em uma determinada categoria (homem, mulher, criança, idosos)" segundo - ARTICLE 29 DATA PROTECTION WORKING PARTY. "Opinion 03/2012 on developments in biometric Technologies", 2012, 6.

[102] Como Vera Lúcia Raposo propõe no seu artigo "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 5.

[103] Refere-se ao uso dessa tecnologia para imputar as reações e sentimentos das pessoas com base em suas características faciais e microexpressões cifrando *ib.*

[104] COMISSÃO EUROPEIA. "LIVRO BRANCO sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança", 2020, parágrafo 56.

[105] Cabe ressaltar que a EDPB expressa que é a "identificação" não necessariamente precisa de revelar o nome ou a identidade da pessoa, mas inclui todo o tratamento de dado que torna-se possível distinguir uma pessoa das outras. Cfr. EPDB. "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo", 2019, 18.

[106] WOODWARD, John D., et al. "Biometrics: A Look at Facial Recognition", 2003.

No que diz respeito a sua operacionalização, a lógica que os pesquisadores exploraram para o reconhecimento de imagens antigamente persistiu em certa parte, sendo complementada com o desenvolvimento da IA, pois como aponta SAMUEL OLIVEIRA "enquanto os sistemas inteligentes de vigilância se valiam da detecção de rostos numa imagem ou da confirmação visual de eventos, os sistemas digitais atuais possibilitam o reconhecimento de pessoas a partir de um cruzamento de informações com enormes bancos de dados, a própria imagem torna-se a fonte de informação."[107]

Em termos técnicos, podemos afirmar que a IA teve um papel de relevo para o desenvolvimento da TRFs - são os subcampos da IA previamente citados, o Machine Learning, o Deep Learning e as redes neurais artificiais, as ferramentas utilizadas para a concretização do reconhecimento de imagens. De um modo geral, os sistemas de reconhecimento facial automáticos são formados pelas seguintes 4 etapas: localização de face, normalização, extração de atributos, e correspondência:

Esse processo é explicado da seguinte forma: Em primeiro lugar teremos o *input* de um dado relativo a uma imagem ou vídeo que passará pela primeira etapa - a localização da face (detecção facial) - aqui o sistema irá procurar extrair a região duma imagem que possua uma imagem facial recorrendo a identificação de pontos fiduciais da face - olhos, nariz, boca[108]; na segunda etapa, o sistema normaliza a face para ficar mais consistente com o banco de dados, identificando a geometria (procurando fatores-chaves como profundidade da cavidade ocular, formato da maçã do rosto, distância entre os olhos, contorno dos lábios e queixo, entre outros) e alinhando a fotometria sendo normalizado a iluminação, contraste e outras propriedades da imagem;[109] na terceira etapa, irá se utilizar de ferramentas que permitam extrair as informações mais relevantes das imagens faciais normalizadas para que seja possível diferenciar uma face entre uma variedade de identidades[110] - o sistema vai converter a imagem em dados consoante os atributos extraídos; por último, irá se proceder o reconhecimento facial - ou seja, irá

[107] OLIVEIRA, Samuel R. "Sorria, você está sendo filmado! Repensando direitos na era do reconhecimento facial", 2021, 43-44.
[108] DATTA, Asit Kumar et. al. "Face Detection and Recognition - Theory and Practice", 2015, 19-21.
[109] LI, Stan Z e JAIN, Anil K, "Handbook of Face Recognition", 2011, 39-41.
[110] KORTLI, Y.; JRID, M.; AL FALOU, A.; ATRI, M. "Face Recognition Systems: A Survey." Sensors, 2020, 20(2), 342.

concretizar-se um *template* (assinatura digital) daquela pessoa em questão, que irá ser comparado com cada imagem facial normalizada da galeria (identificação) ou com uma imagem facial em específico (autenticação/verificação) para realizar-se a determinação da identidade de alguém.[111]

Explicado o processo técnico do funcionamento desta tecnologia, cabe relevar que os melhores sistemas de reconhecimento facial, ou seja, os sistemas mais aptos para conseguirem identificar um rosto em uma imagem com uma maior exatidão, irão depender diretamente da qualidade das tecnologias empregadas no sistema em causa. Um bom sistema de *Machine Learning* irá conseguir realizar um melhor treinamento dos dados em questão, permitindo que cada vez que um novo dado for adicionado, ele consiga ser processado com uma maior precisão. Já as redes neurais, que auxiliam a extração de atributos, será fundamental para que se consiga individualizar as características presentes numa certa imagem, sendo que quanto maior for a rede neural, maior será a precisão da extração dos atributos em causa.

Contudo, mesmo empregando as melhores tecnologias do mercado para o reconhecimento de imagens, esta não se bastará se a coleção de dados utilizadas para o processamento de imagens for deficitária ou incompleta, o que pode resultar numa base de dados tendenciosa: por conter muito mais exemplos de homens brancos em detrimento de homens e mulheres negras, o algoritmo entende que os homens brancos são mais equivalentes a "pessoas" que o restante dos exemplos.[112] Não podemos cair no equívoco de transferir aos algoritmos as desigualdades sociais que permeiam a nossa sociedade há tantos anos, e que lutamos há tanto tempo para dizimá-las. Há que persistir a consciência de que um conjunto de dados utilizados para a tecnologia do reconhecimento facial, precisa representar a sociedade na sua totalidade, abraçando toda a sua diversidade e heterogeneidade.

---

[111] *Ib.*

[112] O'NEIL, Cathy. "Weapons of Math Destruction: how big data increases inequality and threatens democracy", 2016,23

# CAPÍTULO 3

## POLÍTICA DO MEDO – VIGILÂNCIA EM MASSA

*"Aqueles que renunciam à liberdade em troca de promessas de segurança, acabarão sem uma nem outra"*

**George Orwell**

No decorrer deste texto, foram analisadas as aplicações da IA em diferentes esferas sociais. O desenvolvimento dessa tecnologia é recebido com grande entusiasmo pela sociedade, devido aos benefícios que ela proporciona em diversas áreas de atuação. No entanto, é cada vez mais comum relacionar o seu uso como um meio de agressão em larga escala, intensificando formas de violência já existentes. Esse cenário resulta em prejuízos para a segurança e o bem-estar da população, ampliando o exercício autoritário do poder, especialmente no que diz respeito ao controle governamental dos cidadãos através do uso da tecnologia de reconhecimento facial à distância em práticas de vigilância em tempo real de espaços públicos de forma não direcionada.[113]

A vigilância, considerada em seu escopo mais amplo, não é uma prática que surgiu com o advento da IA. No entanto, pode-se afirmar que ela foi intensificada pelo desenvolvimento desta tecnologia. Conforme mencionado anteriormente, a adoção por parte dos seres humanos de novas tecnologias, em especial a internet, resultou em uma significativa concessão de dados pessoais aos proprietários desses serviços. Essa prática levanta questões que já haviam, outrora, sido abordadas na literatura, como o conhecido cenário orwelliano de vigilância constante da população e submissão de seus rituais ao "Grande Irmão". No entanto, a vigilância exercida pelo "*Big Brother*" na ficção difere da vigilância atual em um aspecto intrigante: enquanto na fantasia os indivíduos tinham total noção das câmeras que lhe vigiavam, na realidade, os cidadãos não têm plena consciência de que estão sendo constantemente observados; a vigilância ocorre por meios que não parecem "tão prejudiciais", sendo que sua extensão não se revela de forma clara

[113] PATRÃO NEVES, Maria "Política do medo: Amigos ou inimigos? Privacidade e segurança em tempos de medo global", 2021, 20.

para todos. Esta vigilância vem encontrar espaço para um amplo desenvolvimento assentando numa sociedade que não compreende completamente o fluxo de informações coletadas pelos nossos aparatos tecnológicos e de como estas podem ser utilizadas ao exercício de controle e poder. É justamente neste descaso, ou desinteresse por parte da população, que os governos e empresas conseguiram dar azo a um monitoramento ainda mais expressivo com diversos usos e efeitos.

Na contemporaneidade, nada mais simboliza a estética de vigilância como as câmeras de monitoramento. Por mais que o patrulhamento digital ocorra em grande escala, o simbolismo de uma câmera digital é o que efetivamente imputa à sociedade uma sensação de controle e monitorização. O seu uso, sustentado por argumentos de segurança pública, acabam por esbarrar nos princípios de liberdade e privacidade[114] - justificando as problemáticas associadas à sua utilização.

Dessa constância no patrulhamento por câmeras de monitoramento em espaços públicos, pode ocorrer duas severas consequências: o "*profiling"*[115] e a "vigilância em massa". A primeira consequência diz respeito "à qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações"[116] Dessa prática pode decorrer uma perseguição potencialmente mais intensa de certas minorias, conforme exemplificado pelo estudo realizado em 2021 pela FRA. Esse estudo comprovou que a abordagem policial em alguns países europeus foi direcionada em 50% dos casos a indivíduos pertencentes a minorias, aumentando ainda mais o risco de que os sistemas de identificação biométrica intensifiquem a criação de perfis raciais, resultando em um aumento na vigilância de grupos historicamente e atualmente marginalizados.[117]

---

[114] *Ib.*

[115] Definição de Perfis (Tradução Livre)

[116] Segundo o artigo 4º nº4 do RGPD

[117] CDT Europe, "Facial recognition briefing Paper: The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act", 2023, 4.

Relativamente a vigilância em massa, esta diz respeito a "qualquer monitoramento, rastreamento e processamento de dados pessoais de um indivíduo de maneira indiscriminada ou geral, ou de grupos, que não seja realizado de maneira direcionada contra um indivíduo específico"[118] Sendo assim, podemos afirmar que tal prática é fundamentada no monitoramento da sociedade de maneira indiscriminada, sem a necessidade de suspeitas razoáveis ou oportunidades adequadas para que os indivíduos tenham conhecimento do que está ocorrendo, possam consentir ou façam uma escolha genuína e livre para participar desse monitoramento.[119] Como VERA LÚCIA RAPOSO expõe "deste monitoramento indiscriminado dirigido às massas, todos são observados constantemente, e não há anonimato nos espaços públicos. Toda pessoa pode se tornar suspeita, e até mesmo comportamentos casuais (como usar óculos de sol, esconder o rosto ou olhar para o chão) podem ser considerados suspeitos.".[120]

Esta "política do medo"[121], de constante vigilância e monitoramento populacional, ganhou um expressivo destaque  pelo irromper do terrorismo islâmico no Ocidente, que teve sua máxima expressão no atentado às torres gêmeas do World Trade Center em 2001 na cidade de Nova Iorque.[122] Deste episódio, utilizou-se do discurso de prevenção e combate ao terrorismo e de outras formas de criminalidade grave, para instituir medidas de monitorização - de comunicações eletrónicas, de vídeovigilância em espaço público, do recurso a drones para controle das massas e da recolha de informações sobre passageiros no uso de transportes.[123]

O monitoramento a partir de câmeras de vídeo (comumente por CCTV[124]), se reporta a observação das atividades e comportamentos populacionais, em uma determinada área que são

---

[118] JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 2020, 9.

[119] *Ib.*, 10.

[120] RAPOSO, Vera Lúcia. "The use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal", 2022, 5.

[121] "Prática de amedrontar o cidadão, excitando-o emocionalmente, com justificações diversas de acordo com as circunstâncias e objetivos, como uma estratégia facilitadora para a adoção de algumas medidas e regulamentações sociopolíticas que dificilmente seriam aceites se analisadas apenas racionalmente". Cfr. PATRÃO NEVES, Maria "Política do medo: Amigos ou inimigos? Privacidade e segurança em tempos de medo global", 20.

[122] *Ib*. pág 12

[123] URBANO CALVÃO, Filipa. "Privacidade e segurança em tempos de medo global", 2021, 30.

[124] "CCTV significa Closed-Circuit Television (ou Circuito Fechado de Televisão em português) e corresponde ao sistema de vídeo vigilância de uso mais frequente.Um sistema de CCTV consiste, fundamentalmente, num conjunto de câmaras colocadas em lugares estratégicos, que captam e transmitem imagens para um sistema de gestão de

abrangidas por estas câmeras. Esta vigilância é conectada a uma central de monitoramento onde pessoas capacitadas (policiais no âmbito público e guardas de segurança no âmbito privado) analisam visualmente as imagens obtidas. Entretanto, quando uma área é vigiada por um número extensivo de câmeras, o volume de dados que produz é incompatível com a habilidade destes funcionários em conseguirem analisá-los, solucionando esta questão com o recurso de sistemas de reconhecimento facial automatizados para realizar a análise dos dados em questões, com objetivo de manter a ordem social e prevenir atividades criminosas.

Cabe-nos evidenciar como as tecnologias de reconhecimento facial são enquadradas juridicamente na legislação europeia de proteção de dados, para posteriormente conseguirmos aferir da sua possível legalidade e conformação com a legislação exposta. Em primeiro lugar, cabe inferir que os dados coletados pelas câmeras de vídeo vigilância se enquadram, através da LED e da RGPD, como dados biométricos[125], dentro da categoria de dados pessoais[126]. Segundo a LED os dados biométricos são "dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos".[127] Tais dados são alvo de uma proteção específica no âmbito europeu, tendo em vista que "são especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais."[128]

A definição de dados biométricos abrange duas tipologias destes: os relacionados com os comportamentos (ações, maneiras, hábitos) e àqueles relacionados com características físicas (impressões digitais, DNA, altura, padrões de íris, características faciais, impressões

vídeo que permite a gravação e visualização dessas imagens." Cfr. SEGURTEC. "CCTV: tudo o que deve saber", 2020.

[125] Segundo o artigo 4º, nº14 do RGPD e o artigo 3º nº13 da LED.

[126] Segundo o artigo 3º, nº 1 da LED os dados pessoais são: " informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular".

[127] Segundo o artigo 3º, nº13 da LED.

[128] Segundo o considerando 51 do RGPD e o considerando 37 da LED.

palmares)[129], ou seja, além da tecnologia de reconhecimento facial, existem outros tipos de processamento de dados biométricos. Contudo, comparada às outras formas de reconhecimento ou autenticação de pessoas pelos Sistemas de Identificação Biométrico[130], a TRF através de imagens parece ser a menos invasiva, podendo ser utilizada a distância, sem a interação do usuário, em tempo real ou até mesmo por imagens e vídeos já gravados. Para conseguir provar que aquela certa pessoa afirma ser quem é, não será necessário a sua impressão digital, íris ocular, DNA ou comprovação sanguínea, bastando uma foto da sua face.

Conforme enunciado no "Draft IA", estes sistemas de reconhecimento facial à distância possuem duas modalidades: àquelas que ocorrem em tempo real, quando as câmeras de vídeo vigilância produzem a identificação dos cidadãos momentaneamente; ou em diferido, quando as imagens faciais já foram recolhidas e a identificação ocorre após um atraso significativo.[131] A este respeito, cabe também fazer uma distinção entre usos direcionados e não direcionados de sistemas de reconhecimento facial: na primeira objetiva-se identificar uma pessoa específica cruzando a imagem facial dessa pessoa com um rosto em um banco de dados permitido, já na segunda, ambiciona-se escanear todos os rostos em uma multidão para encontrar correspondências no banco de dados.[132]

Como elucida VERA LÚCIA RAPOSO, essa tecnologia é comumente utilizada pelos governos para o propósito de "*law enforcement"*[133](sendo a utilização que iremos nos aprofundar), contudo esta também é utilizada por companhias privadas, na identificação de ladrões de lojas, pessoas que contam cartas em cassinos ou até mesmo pessoas que invadem áreas restritas de arenas esportivas ou locais VIP.[134]

---

[129] RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 3.

[130] Conforme exposto no artigo 3º, nº 36 do *Draft AI,* os "sistemas de identificação biométrica" podem ser definidos como: "sistema de IA que se destina à identificação de pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que se saiba, antecipadamente, se a pessoa visada estará presente e pode ser identificada, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos utilizados."

[131] Segundo o considerando nº 8 do *Draft AI.*

[132] CDT Europe, "Facial recognition briefing Paper: The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act", 2.

[133] Cumprimento da lei (Tradução Livre)

[134] RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 7.

Destaca-se o caso chinês como o exemplo mais notável desta prática no mundo moderno, que além de realizarem o monitoramento da população através de câmeras de reconhecimento facial para controle e represália, adotaram um sistema de *Social Scoring* de controle social[135]. Este sistema opera um cruzamento de dados disponibilizados pelos cidadãos - redes sociais, bancos de fotos, registros de posses dos cidadãos (carros e imóveis) e às suas viagens pelo território chinês (passagens e hospedagens)[136] - com a observância das pessoas por câmeras de reconhecimento facial em espaços públicos através de mais de 600 milhões de dispositivos espalhados em seu território[137]. O sistema qualifica os indivíduos através de padrões de conduta em três categorias: O nível vermelho identifica as pessoas de "maior preocupação" para as autoridades, enquanto o amarelo inclui os cidadãos em geral e o verde se refere a quem "não oferece perigo".[138] Por meio das pontuações obtidas por cada cidadão, há consequências para aqueles que não se comportam de forma plena aos olhos da lei: podem ser impedidos de entrarem em certos estabelecimentos, de se deslocarem por meios de transportes para outras cidades ou até mesmo de pedirem créditos em bancos.

Por mais utópica que possa parecer a prática de pontuação dos indivíduos baseado nas suas condutas diárias, o exemplo chinês elucida o apogeu da utilização dos SRFs no controle social operado por agentes governamentais. Todavia, esses sistemas têm sido utilizados por democracias liberais (com grande expressão nos Estados Unidos e no Brasil) para identificação dos seus cidadãos.

Argumenta-se pela positiva de estatuir sistemas de reconhecimento facial em câmeras de vigilância no auxílio do combate ao terrorismo, do controle da criminalidade e até mesmo para ajudar os órgãos de investigação na procura de pessoas desaparecidas. Há, num contraponto, um grande receio da extensão do seu uso, baseado no fato de que tais tecnologias apresentam uma grande ameaça a diversos Direitos Fundamentais: numa primeira senda, podemos elucidar os erros dos processamentos dos dados biométricos concretizando falsos positivos, exarcebando preconceitos, racismos e vieses, colocando em causa o direito à não

---

135 WONG, K.L.X / DOBSON, Amy shields. "We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Rating Cultures in Westernised Democracies", 2019.
136 CREEMERS, Rogier. "China's Social Credit System: An Evolving Practice of Control", 2018, 20.
137 *Ib.*, 16
138 *Ib.,* 28.

discriminação; contudo, mesmo quando os dados são processados de maneira correta, esta tecnologia têm o potencial de violar o a dignidade humana, a privacidade, a proteção de dados pessoais, liberdade de reunião e associação, a presunção da inocência, entre outros.[139] Por muitas vezes assistiu-se a utilização de tais tecnologia como mecanismos de repressão de territórios e grupos vulneráveis e de perseguição e criminalização de ativistas, protestantes e defensores dos Direitos Humanos.[140]

Perante tais violações de direitos fundamentais, iremos nos focar em duas delas, consideradas mais relevantes pela autora da Dissertação, que precisam ser diluídas para uma real compreensão do enorme problema que estamos lidando.

## 1. DISCRIMINAÇÃO ALGORÍTMICA E FALSOS POSITVOS

> "*Can machines ever see my queens as I view them? Can machines ever see our grandmothers as we knew them?*
>
> **Joy Buolamwini – "AI, Ain´t I A Woman?"**

Há um precedente histórico de como a tecnologia vem sendo usada para pesquisar movimentos da população negra. Em 1713, Nova York aprovou a "Lei das Lanternas", exigindo que qualquer pessoa escravizada com mais de 14 anos, carregasse uma lanterna à noite para que pudesse ser vista facilmente pelos brancos.[141] Por mais que a tecnologia de reconhecimento facial tenha se desenvolvido em larga escala, a associação desta com práticas discriminatórias se mostra ainda muito presente.

Joy Buolamwini, uma americana com descendência ganesa e estudante da famosa universidade MIT, foi uma das primeiras acadêmicas a elaborar pesquisas endereçando o problema da TRF ter vieses discriminatórios. No seu primeiro semestre da faculdade, teve uma disciplina chamada: "Ciência de Fabrico", que tinha como objetivo incentivar os seus alunos,

---

[139] FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement", 2020, 4.

[140]ROHE, Andersson. "O Ecossistema Chinês de vigilância e Reconhecimento Facial: ameaça ou solução tecnológica?" 2022, 8.

[141] KNONDE, Mutale, "Automated Anti-Blackness Facial Recognition in Brooklyn, New York", 2020.

através da leitura de livros de ficção científica, a construir algo inspirador. Joy, por sua vez, teve a ideia de construir um *Aspire Mirror*[142], no qual poderia projetar na sua face imagens inspiradoras, como por exemplo um leão, ou a transformar em ícones famosos - como Serena Williams, ou Michelle Obama. Ao desenvolver o software de reconhecimento facial para a sua criação, a académica se encontrou perante uma problemática: o sistema não reconhecia a sua face, ao menos que ela colocasse sob o seu rosto uma máscara branca. Esta problemática relativamente ao sistema que andava a desenvolver fez com que ela chegasse a uma conclusão: os dados que estão sendo coletados não são capazes de representar a sociedade como um todo, consistindo, majoritariamente, em rostos masculinos e/ou brancos. Ou seja, como os sistemas serão aptos para identificar faces negras, se os dados disponíveis para serem processados por algoritmos não contemplam estes rostos?[143]

A partir desta conclusão, a cientista Joy Buolamwini, começou a investigar questões de preconceitos que poderiam se infiltrar nesta tecnologia. A mesma começou a analisar outros sistemas que popularmente andavam a ser desenvolvidos (IBM, Amazon e Microsoft) para verificar se a sua face poderia ser detectada nestes softwares. No quesito de identificação do gênero de uma pessoa, todas as empresas tiveram um desempenho substancialmente melhor em rostos masculinos do que femininos. Estas empresas tinham taxas de erro não superiores a 1% para identificação de homens de pele clara. Para mulheres de pele mais escura, os erros subiram para 35%.[144] A cientista também constatou que os sistemas de IA analisados não conseguiram classificar corretamente os rostos de Oprah Winfrey, Michelle Obama e Serena Williams, expondo: "quando a tecnologia discrimina até essas mulheres icônicas, é hora de reexaminar como esses sistemas são construídos e a quem eles realmente servem".[145]

Outro caso curioso foi um estudo realizado pela ACLU em 2018, testando o software de reconhecimento facial da *Amazon*, chamado *Rekognition*. Essa tecnologia foi anunciada por fornecer uma "análise facial altamente precisa, comparação de rosto e recurso de pesquisa de

---

[142] Espelho de Aspirações (Tradução Livre)
[143] Resumindo o exposto dos primeiros 25 minutos do Documentário "*Coded Bias*" disponível na plataforma de streaming Netflix.
[144] BUOLAMWINI, Joy. ""Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It", 2019.
[145] *Ib.*

rostos".[146] O experimento testou o software da *Amazon* comparando imagens de membros da Câmara e do Senado americano com um banco de dados de 25.000 fotos disponíveis publicamente. O resultado foi curioso, mas não surpreendente: foram identificados falsamente 28 membros do congresso como outros indivíduos que já foram presos por crimes. Entre os rostos identificados incorretamente, cerca de 40% se tratavam de pessoas negras, apesar de constituírem apenas 20% do Congresso. [147]

Ambos os testes evidenciados destacam o racismo profundamente enraizado destas tecnologias de reconhecimento facial, elucidando a dificuldade que esses sistemas possuem em identificar rostos negros em comparação com rostos brancos. Segundo SIL BAHIA, chamamos esse efeito de "racismo algoritmo" que ocorre "quando sistemas matemáticos ou de inteligência artificial são pautados por informações enviesadas/tortas que alimentam e regem seu funcionamento. As consequências são muitas, mas talvez a maior delas seja o aumento de desigualdades, sobretudo em um momento onde estamos cada vez mais tendo muitos dos nossos gostos e políticas mediadas por máquinas, com o avanço da tecnologia".[148]

Por mais gravosa que seja essa consequência para pretos, a prática de coleta irregular de dados contaminada por vieses discriminatórios tem efeitos em outras minorias, como os asiáticos, latinos, imigrantes, índios e transsexuais[149], indicando como essa tecnologia traz à tona o preconceito estrutural latente nas sociedades. O fato de a tecnologia ainda não apresentar uma eficiência sincrética no reconhecimento destes grupos, possibilita que populações vulneráveis estejam sujeitas à automatização de constrangimentos e violências e quando empregada na vigilância de lugares públicos em tempo real, de forma automatizada, pode levar a sérios casos de discriminação.

Nessa lógica, cabe inferir que discriminação é "quando uma pessoa é tratada de forma menos favorável do que a outra é, foi, ou seria, tratada em uma situação comparável com base em uma notável característica real"[150], sendo que essa "discriminação algoritmica" pode ocorrer por dois expressivos motivos: durante o desenvolvimento, teste e implementação dos algoritmos

[146] AMAZON WEB SERVICES "What is Amazon Recognition", 2021.
[147] SNOW, Jacob. "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots", 2018.
[148] VIEIRA, Kauê. "Reconhecimento facial vira ameaça para negros: maioria entre presos"
[149] ROSE, Adam. "Are Face-Detection Cameras Racist?", 2010.
[150] COUNCIL OF THE EUROPEAN UNION. "Council Directive 2000/43/ EC", 2000, 22-26.

usados para o RF, por vieses que são incorporados; ou, quando a qualidade dos dados usados para desenvolver os algoritmos e softwares, são alimentados com pouca quantidade e qualidade de imagens faciais, privilegiando apenas um tipo de rosto[151] (majoritariamente rostos masculinos e brancos).

Desta prática equivocada, temos a consequência de que quando for feita a comparação de imagens faciais de minorias à bancos de dados deficitários, tais pessoas estarão expostas a uma maior probabilidade de serem erroneamente correspondidas como falsos positivos, fazendo com que tais grupos sejam abordados/presos incorretamente com uma maior frequência, por causa de suas fisionomias.[152]

São inúmeras as situações em que o emprego destas tecnologias em técnicas de vigilância de locais públicos em tempo real apresentou resultados errôneos na identificação de pessoas: Podemos citar o caso do motorista de aplicativo Jeferson Pereira da Silva. Este homem negro se direcionou até o seu antigo estabelecimento de emprego para fazer um acerto de contas, em um shopping na Zona Norte do Rio de Janeiro (Brasil). Chegando ao local, encontrou duas viaturas policiais civis que lhe deram automaticamente voz de prisão. O jovem fora reconhecido, pelo sistema de reconhecimento facial da polícia do Rio de Janeiro, como o autor de um roubo cometido há 15 anos atrás. Jeferson passou seis dias preso por um crime que não cometeu.[153]

Outro caso semelhante a este ocorreu em Detroit nos Estados Unidos no início de 2020. Robert Willians, um homem negro, passou quase 30 horas preso injustamente depois que o software de reconhecimento de facial da Polícia do Estado de Michigan o apontou como o provável autor do furto em uma loja de relógios. A foto da carta de condução de Willians foi adicionada à um banco de dados, junto à outros homens negros e comparada com um vídeo de vigilância do estabelecimento furtado. Robert fora preso em sua casa diante das esposa e das filhas.[154]

Uma situação ainda mais caricata aconteceu no Ceará, um estado brasileiro, no começo de 2022. O método de reconhecimento facial, utilizado pela polícia brasileira em investigações

[151] FRA. Facial recognition technology: fundamental rights considerations in the context of law enforcement“, 27.
[152] *Ib.*
[153] G1 RIO. “Homem preso por reconhecimento fotográfico em foto 3x4 antiga deixa a cadeia no Rio”, 2021.
[154] TECMUNDO. “Reconhecimento facial erra e homem é preso injustamente nos EUA”, 2020.

e inquéritos para identificação de suspeitos, mostrou falhas ao indicar o ator mundialmente conhecido Michael B. Jordan como suspeito da chacina da Sapiranga, que ocorreu no dia 25 de dezembro de 2021.[155]

A realidade é que o software de reconhecimento facial exibe injustiça. O maior problema com esses resultados é que, à medida que esses algoritmos se tornam mais prevalentes, eles continuam a espalhar o viés em uma escala mais massiva e em ritmo acelerado.[156] A máquina reproduz o mundo tal como ele é, tomando decisões matemáticas e não tomando decisões baseadas na ética. Se usarmos modelos de Machine Learning e Deep Learning para a análise e comparação de dados em banco de dados "incompletos" para reproduzir o mundo de hoje, dificilmente teremos progresso social, incorporando às tecnologias as discriminações que permeiam nossa sociedade. Todo o progresso feito até então poderá ser revertido ao abrigo da neutralidade das máquinas.

## 2. VIOLAÇÃO DA PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS

*"To be left alone is the most precious thing one can ask of the modern world."*

**Anthony Burgess, Homage To Qwert Yuiop: Essays**

A temática principal de "Política do Medo" que enuncia este capítulo, vem conceber de que forma certas ameaças externas como o terrorismo ou alta criminalidade parecem contribuir numa cedência da privacidade em prol da segurança. PATRÃO NEVES expõe que "as novas tecnologias têm sido capazes de apresentar algumas respostas para os nossos medos coletivos, como os sistemas de vigilância, para uma antecipação, mitigação ou supressão de ameaças, cujo primeiro e mais evidente impacto negativo é o estreitamento da privacidade"[157]

O conceito de privacidade foi sistematizado, no seu primórdio, por Aristóteles, quando este difere a esfera pública (o espaço da atividade política - *polis*) da esfera privada (espaço da

[155]CAIXETA, Izabella. "Foto de Michael B. Jordan aparece entre suspeitos de chacina", 2020.
[156] SCHNEIDER, Shira. "Algorithmic Bias: A New Age of Racism", 2021, 23-25.
[157] PATRÃO NEVES, Maria "Política do medo: Amigos ou inimigos? Privacidade e segurança em tempos de medo global", 22.

família e da vida doméstica - *oikos*).[158]Com a evolução do estilo de vida social e a inerente sedentarização que se aliou a este desenvolvimento, o espaço privado do lar acaba por se tornar um local "privado", com o simbolismo de paredes interiores que dividiram o interior da casa da esfera pública.[159] Entretanto, ao longo da história, a temática da privacidade não foi particularmente valorizada, não obtendo uma tematização plenamente destacada de conceptualização e relevância.[160]

Foi em 1980 que começou a ensejar-se uma preocupação em determinar-se um efetivo direito à privacidade a partir da publicação de Samuel D. Warren e Louis Branden "*The right to privacy"* sendo um marco na doutrina americana. Estes desenvolveram o conceito do direito de ser deixado só - *the right to be left alone* - em consonância a obra elaborada por Thomas McIntrey Cooley de 1888, no qual propuseram que "cada indivíduo possui uma esfera pessoal inviolável, na medida em que possuem o direito de escolher compartilhar com terceiros informações relativas a aspectos da sua personalidade e de sua vida íntima".[161]

A noção concreta do que vem a ser a privacidade provou-se difícil de ser explicada adequadamente, tanto na sua extensão quanto no seu valor. Percebe-se, desde logo, que o termo privacidade "serve a uma significação bastante ampla (...) expressando as pretensões individuais de proteção legal derivada do direito a ser deixado só ou em paz e contra a disseminação de informações de carácter pessoal."[162]

Esta  vem a ser designada pelo autor americano ALAN FURMAN WESTIN como: "autonomia pessoal e desenvolvimento da individualidade; alívio emocional face ao ambiente social e relacional; auto-análise, reflexão e poder de decisão próprio; e, proteção das comunicações envolvendo relações e sentimentos íntimos."[163] Já o manual austríaco de Educação para os Direitos Humanos "Compreender os Direitos Humanos", expõe que o

---

[158] ARISTÓTELES. "Política de Aristóteles", 2008, 38.
[159] BETÂMIO DE ALMEIDA, Alfredo. "A Privacidade: Um enquadramento geral do conceito e levantamento de questões", 2021, 45.
[160] PATRÃO NEVES, Maria "Política do medo: Amigos ou inimigos? Privacidade e segurança em tempos de medo global", 23.
[161] SAITO, Vitória Hiromi. "Desafios Contemporâneos para a Tutela dos Direitos à Privacidade e aos Dados Pessoais", 2022, 56.
[162] Martins, L. M."O direito civil à privacidade e à intimidade", 2002, 344.
[163] WESTIN, Alan Furman. "Privacy and Freedom", 2015.

conceito de privacidade (em latim *privates* que significa separado do resto) indica que uma pessoa pode separar-se do resto e, desta forma, revelar-se.[164]

No entanto, há que relevar o fato de que o conceito de privacidade possui diferentes sentidos entre a experiência europeia e americana, baseando-se nos distintos processos históricos, culturais e sociais geradores de valores e hábitos distintos.[165]Nesta lógica, o professor JAMES WHITMAN aponta que a principal ameaça à privacidade na perspetiva norte-americana é o poder abusivo do governo e a perda da liberdade individual, o que explica uma tendência libertária e individualista evidenciada nas correntes do liberalismo económico de incentivo ao empreendedorismos e de uma publicidade mais agressiva. Já na ótica europeia, a principal ameaça à privacidade começa por uma imprensa livre, sensacionalista e sem respeito pela vida privada, desconfiando da atuação livre dos mercados relativamente à defesa da dignidade pessoal, o que acaba por explicar uma maior aceitação por parte dos europeus de um Estado Social.[166]

Apesar das fronteiras da privacidade divergirem culturalmente, partilham um entendimento básico comum, que fora consagrado pela primeira vez em instrumentos internacionais - na DUDH e no PIDCP. No primeiro, declarou-se o Direito à Privacidade como "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. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."[167] Já no PIDCP está exposto que "Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação; e toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados."[168]

---

[164] BENEDEK, Wolfgang. "Compreender os Direitos Humanos - Manual de educação para os direitos humanos", 2012, 386.
[165] BETÂMIO DE ALMEIDA, Alfredo. "A Privacidade: Um enquadramento geral do conceito e levantamento de questões", 63.
[166] WHITMAN, James Q.. "The Two Western Cultures of Privacy: Dignity versus Liberty", 2004, 1151 -1221. 2
[167] Previsto no Artigo 12º da DUDH.
[168] Previsto no Artigo 17º do PIDCP.

Este direito também é, atualmente, consagrado na maioria das Constituições nacionais e dos Códigos Penais dos países com um Estado de Direito, como é o caso de Portugal.[169]

Este direito veio a ser consagrado na Carta, no seu artigo 7º, como o Direito de Respeito pela vida privada e familiar, estatuindo que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações".

Já no que diz respeito ao Direito Fundamental de Proteção de Dados, esta é uma área do direito que surgiu da crescente conscientização sobre a importância da privacidade e do controle sobre informações pessoais na era digital. Anteriormente, a proteção de dados era limitada devido ao armazenamento físico e ao compartilhamento restrito de informações. No entanto, com o avanço da tecnologia e a digitalização de dados, tornou-se necessário estabelecer uma estrutura legal para proteger as informações pessoais dos indivíduos. Embora a privacidade e a proteção de dados sejam direitos fundamentais relacionados, as regras da UE sobre proteção de dados criam um sistema de proteção específico e reforçado em comparação com o direito à privacidade (iremos ver infra).[170]

A primeira consagração legislativa do Direito de Proteção de Dados aconteceu em 1981, com a adoção da Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados pelo Conselho da Europa. Essa convenção estabeleceu princípios e diretrizes fundamentais para a proteção de dados pessoais, reconhecendo a importância de preservar a privacidade e a capacidade de decisão das pessoas em relação ao tratamento automatizado de dados. Embora tenha sido um marco importante, releva observar que a evolução do Direito de Proteção de Dados continuou com a adoção de leis mais abrangentes e atualizadas, como a Diretiva 95/46/EC da União Europeia e, posteriormente, o Regulamento Geral de Proteção de Dados (RGPD).

Quando estamos falando de dados pessoais, ou seja, aqueles dados que são passíveis de concretizar a identificação de uma pessoas, sua proteção mostra-se ainda mais evidente. Dessa forma, tal direito foi considerado fundamental através de sua previsão na Carta, onde dispõe no

---

[169] BETÂMIO DE ALMEIDA, Alfredo. "A Privacidade: Um enquadramento geral do conceito e levantamento de questões", 54.

[170] KOKOTT, Juliane / SOBOTTA, Christoph. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", 2013, 227.

seu artigo 8º: "Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação."

Estes direitos, de respeito pela vida privada e proteção de dados remontam ao cerne da preocupação da implantação de TRFs em locais públicos. Tais direitos são distintos e autónomos, contudo, podemos dizer que estão intimamente ligados pois se esforçam para proteger valores semelhantes, a autonomia e a dignidade humana dos indivíduos, a conceder-lhes uma esfera pessoal na qual possam desenvolver livremente suas personalidades, pensar e formar suas opiniões. Dessa forma, constituem, um pré-requisito essencial para o exercício de outros direitos fundamentais, como a liberdade de pensamento, consciência e religião (artigo 10.º da Carta), a liberdade de expressão e de informação (artigo 11.º da Carta) e a liberdade de assembleia e de associação (Artigo 12 da Carta).[171]

Diante dessas considerações, podemos afirmar que as TRFs, utilizadas para coletar, comparar ou armazenar imagens faciais com o propósito de identificar indivíduos ou criar bases de dados, representam a incorporação de poderosos sistemas de IA. Essas tecnologias têm a capacidade de coletar cada vez mais dados altamente sensíveis e pessoais, o que as torna progressivamente mais invasivas em relação à privacidade individual e à proteção de dados.[172] Sendo esta técnica utilizada no poder investigatório para identificação, buscas, análise comportamental e interações sociais, tornou-se evidente a elevada intromissão da vida alheia - tal ingerência na vida privada e nos dados pessoais dos indivíduos, se torna ainda mais gravosa quando empregada de maneira excessiva ou desproporcional, pois acaba gerando um estado de monitoramento contínuo, que não se coaduna com uma democracia saudável.

A utilização destas tecnologias possuem a capacidade de gerar uma vigilância massiva por parte do Estado, que passará a ter informações precisas sobre a sua população, podendo observar todas as atividades realizadas pelos cidadão - os locais que frequentam, com quem se relacionam, como se vestem, o que consomem, quais rotas realizam e que tipo de atividades

[171] FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement", 23.
[172] EPRS, "Regulating facial recognition in the EU", 2023, 6.

praticam. A partir dessa prática, destaca-se uma excessiva violação de liberdades individuais, comprometendo o direito a privacidade, o desenvolvimento da personalidade e autodeterminação, além de violar direitos da personalidade e intimidade. [173]

Como exemplo claro desta situação, podemos elucidar o contexto dos protestos do *Black Lives Matter,* que eclodiram a partir do homicídio de George Floyd em 2020 nos Estados Unidos, no qual as agências governamentais americanas utilizaram de técnicas de reconhecimento facial para identificar os protestantes em questão.[174]A utilização das TRF em âmbitos públicos onde estão a decorrer protestos, está a ser aproveitada para identificar, seguir e assediar pessoas que estão apenas a exercer os seus direitos de liberdade de reunião e associação, violando os direitos elucidados acima, na invasão de privacidade e na coleta ilegal e desproporcional de dados biométricos.

Já na China, temos como exemplo os protestos realizados contra medidas excessivas de combate à Covid-19, no qual diversos protestantes foram identificados através de câmeras de reconhecimento facial  sendo perseguidos pelos agentes governamentais em suas próprias residências com o objetivo de punir a prática do protesto. Diversos manifestantes recorreram à bonés, óculos de sol e balaclavas no intuito de não serem reconhecidos pelas câmeras e conseguirem protestar sem receios de punição.[175]

Estes exemplos elucidam a controversa da temática em causa. A verdade é que "o simples fato de participarmos desta época é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que produzimos diariamente, seja em redes sociais, ou através do uso dos dispositivos conectados à Internet das coisas"[176] Isso significa que, voluntária ou involuntariamente, vivemos sob o constante monitoramento possibilitado pelo avanço tecnológico. Voluntariamente, pois em diversas ocasiões cedemos livremente nossos dados pessoais ao governo e a corporações privadas; involuntariamente, pois em diversas

---

[173] ALMEIDA, Eduarda Costa. "Reconhecimento facial e segurança pública: como garantir a proteção de dados pessoais e evitar os riscos da tecnologia", 2020, 270-275.

[174] AMNISTIA INTERNACIONAL. "EUA: Tecnologia de reconhecimento facial reforça policiamento discriminatório", 2022.

[175]N MOZUR, Paul / FU, Claire / CHIEN, Amy Chang. "China usa reconhecimento facial para rastrear manifestantes contra Covid zero" 2022.

[176]COSTA, Ramon Silva / OLIVEIRA, Samuel Rodrigues de, "O uso de Tecnologias de Reconhecimento Facial em Sistemas de Vigilância e Suas Implicações no Direito à Privacidade", 2020, 11.

outras situações encontramo-nos vigiados, sem que a nós seja dada a oportunidade de consentirmos no que diz respeito a tal vigilância.[177] E o armazenamento destes dados biométricos capturados a partir destas tecnologias, formando uma base de dados centralizada por parte dos Governos, constitui um sério motivo de preocupação, pois tal prática aumenta os riscos de insegurança na informação ao deixar os indivíduos vulneráveis em relação ao Estado.[178]

A partir destas práticas de alta ingerência por parte dos Governos na vida privada dos seus cidadãos, clamou-se por uma compreensão efetiva sobre a necessidade do uso desta tecnologia na prevenção criminal. Na Europa, segundo um recente estudo, 80% dos seus cidadãos não gostam da ideia de compartilhar os dados de seus rostos com autoridades.[179] Em 2020, a UCLA decidiu proibir a tecnologia para vigilância municipal.[180]

O uso de Reconhecimento Facial sob que emprega práticas de vigilância tem sido duramente criticado na Europa. Um destes exemplos é a iniciativa "*Reclaim Your Face*", uma petição que junta várias organizações de direitos na União Europeia e pretende promover uma mudança na regulação, para impedir que o reconhecimento facial seja utilizado nos sistemas de videovigilância. A petição dispõe: "Estes sistemas intrusivos não devem ser desenvolvidos, aplicados (mesmo a título experimental) nem utilizados por entidades públicas ou privadas, uma vez que podem interferir desnecessária ou desproporcionalmente com os direitos fundamentais dos cidadãos"[181]

Perante a exposição das problemáticas associadas ao seu uso, será necessário expor de que forma o Direito tem conseguido absorver tais obstáculos, evidenciando se a sua utilização pode ser sustentada pelos princípios basilares de um Estado Democrático de Direito. É justamente nesta temática que realizaremos a exposição da 2ª parte desta dissertação.

---

[177] *Ib.*

[178] BENEDEK, Wolfgang. "Compreender os Direitos Humanos - Manual de educação para os direitos humanos", 392.

[179] NICOLÁS, Elena Sánchez. "Pandemic speeds calls for ban on facial recognition", 2020.

[180] PAUL, Kari. "'Ban this technology': students protest US universities' use of facial recognition", 2020.

[181] Cfr. petição disponível em: https://reclaimyourface.eu/pt/

# PARTE 2

# A EXPLICAÇÃO DO PRESENTE

# CAPÍTULO 5

# O DIREITO E A TECNOLOGIA DE RECONHECIMENTO FACIAL

*"Quand je vais dans un pays, je n'examine pas s'il y a de bonnes lois, mais si on exécute celles qui y sont, car il y a de bonnes lois partout."*
**Montesquieu**

## 1. A NECESSIDADE DE UMA ANÁLISE JURÍDICA DA QUESTÃO

Chegando até aqui, conseguimos inferir certos problemas que derivam do desenvolvimento de novas tecnologias, especificamente da inteligência artificial, sendo lógico se afirmar que estas avançaram a uma velocidade que, tragicamente, o direito não conseguiu acompanhar. Isto se dá pelo fato da regulamentação das tecnologias ser um desafio constante, pois estas avançam rapidamente, e muitas vezes os órgãos não conseguem acompanhar o ritmo. Sendo assim, a partir do desenvolvimento pleno das tecnologias, elas são inseridas no mercado para serem comercializadas sem antes ser realizada uma reflexão profunda sobre as consequências dos seus usos. Isto aconteceu com as TRFs, mas também com outras novas formas de tecnologias que incorporaram a IA no seu uso, pois, a par do modelo capitalista que vivemos, numa corrida entre o consumo imediato e a reflexão duradoura, sabemos quem será o inevitável ganhador, mesmo que da sua utilização advenham danos e riscos explícitos.

Além da velocidade da inovação tecnológica, evidenciam-se outras dificuldades na tentativa de regular as tecnologias: estas são complexas e muitas vezes são difíceis de entender e monitorar, tornando árduo o trabalho dos órgãos reguladores para entender plenamente o funcionamento destas e de identificar os possíveis impactos positivos e negativos; o fato dos órgãos reguladores terem de equilibrar os interesses conflitantes de todas as partes interessadas, sendo interesses comerciais, de privacidade e de segurança; por último, podemos relevar as pressões políticas e económicas que afetam a regulação das tecnologias, tornando difícil para os órgãos reguladores adotarem medidas que possam prejudicar empresas ou a economia em geral.

No caso das TRFs incorporadas nos sistemas de identificação biométrica à distância, analisamos alguns dos problemas que estas tecnologias apresentam quando utilizadas para fins

de segurança pública e manutenção da ordem pública. A partir desta análise tornou-se claro que, do seu uso, estamos ameaçando a segurança da nossa sociedade civil a par de sérias violações de direitos fundamentais e direitos humanos principalmente no que diz respeito ao direito a não discriminação, o direito a privacidade e o direito a proteção de dados.

Assim sendo, esta segunda parte da presente Dissertação tem como objetivo analisar os instrumentos legislativos criados para regular o uso das TRFs pelos governos e empresas privadas – num plano internacional, europeu e transnacional, explorando as decisões judiciais que se debruçaram sobre este tema, com a tenção de escrutinar as soluções oferecidas e perceber se estas conseguiram colmatar os problemas demonstrados. Será através de uma análise jurídica profunda dos instrumentos legislativos e da jurisprudência atual, a par dos problemas evidenciados, que teremos a legitimidade para ensejar uma discussão sobre quais os próximos passos deverão ser tomados em relação ao seu uso.

## 2. PANORAMA INTERNACIONAL

Nos últimos anos, surgiu uma crescente preocupação com o uso de tecnologias de reconhecimento facial para fins de identificação de indivíduos. Essa preocupação tem se intensificado em todo o mundo em virtude da ampla disseminação dessas tecnologias e das crescentes implicações éticas, de privacidade e discriminação que as acompanham. Em particular, as apreensões em torno do uso dessas tecnologias por agências governamentais e policiais foram ampliadas com a intensificação dos protestos do movimento *Black Lives Matters*.[182] Esse movimento trouxe à tona a necessidade de um maior escrutínio do uso de TRF para vigilância de comunidades marginalizadas, dadas as preocupações com os erros e preconceitos embutidos nessas tecnologias, bem como como a possibilidade de se desencadear uma efetiva vigilância em massa.

Contudo, não existe uma regulamentação global padronizada sobre o uso de tecnologias de reconhecimento facial e nem um real consenso sobre de que forma e em que situações as mesmas deveriam/poderiam ser utilizadas, deixando nas mãos das empresas privadas e dos

[182] VICENT, James. "NYPD used facial recognition to track down Black Lives Matter activist / Mayor Bill de Blasio says standards need to be "reassessed"", 2020.

governos a possibilidade de uso indiscriminado das mesmas. Perante este fato, a sociedade civil tem pressionado as organizações internacionais para que abordem adequadamente essa problemática. Em vista do atual contexto, em que o uso dessas tecnologias pode vir a violar diversos direitos humanos e fundamentais, tornou-se inviável continuar a utilizá-las sem uma adequada regulação.

De forma inovadora, a Organização das Nações Unidas foi a primeira organização internacional a endereçar os problemas que derivam deste uso indiscriminado de TRF. Foi diante dos protestos do movimento *BLM* e do aumento do uso de tecnologias incorporadas pela inteligência artificial, que o *United Nations High Commissioner for Human Rights* publicou, em 2020, um relatório intitulado "*Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*"[183]. Pela primeira vez em escala global, o relatório vem abordar algumas preocupações relacionadas ao uso de TRFs. O documento enfatiza o uso dessas tecnologias no contexto dos direitos de reunião e associação pacífica[184], ressaltando a importância desses direitos para a sustentabilidade das democracias, propondo que, para o seu uso, se deva demonstrar o cumprimento das normas de privacidade e proteção de dados, bem com a ausência de problemas significativos de precisão e impacto discriminatório.[185]

O relatório sugeriu a proibição do uso de técnicas de vigilância quando esta for indiscriminada e não direcionada perante aqueles que exerçam o direito de reunião e manifestação pacífica, tanto em espaços físicos quanto online. No caso de vigilância direcionada, esta apenas deveria ser autorizada quando houver suspeita razoável de que um

---

[183] UNITED NATIONS. "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Report of the United Nations High Commissioner for Human Rights", 2020, 15.

[184] Direito esse assegurado pelos artigos 20ºnº1 da DUDH, 21º da PICPD e 12º da Carta.

[185] Segundo Michelle Bachelet, Alta Comissária das Nações Unidas para os Direitos Humanos "o Conselho também apontou para desafios novos e emergentes, como a vigilância ilegal ou arbitrária de manifestantes, tanto em espaços físicos quanto online, inclusive por meio do uso de ferramentas de rastreamento digital. Além disso, observou como o uso indevido das novas tecnologias impediu o acesso das pessoas à informação em momentos políticos chave, com impacto na capacidade de organizar e realizar assembleias. A Alta Comissária disse que a proteção dos direitos humanos no contexto de protestos pacíficos continua a ser uma prioridade para o seu Gabinete. Ela concluiu elogiando especificamente o trabalho de jornalistas e outros membros da sociedade civil que desempenharam um papel essencial na promoção e proteção dos direitos humanos no contexto de protestos pacíficos." cfr. UNITED NATIONS. "High Commissioner: the Human Rights Council Has Given a Disturbing Diagnosis of Human Rights Violations Occurring in the Context of Peaceful Protests", 2021.

determinado indivíduo cometeu ou está cometendo um crime, ou está envolvido em atos que representem uma ameaça específica à segurança nacional. Contudo, estando perante uma violação à privacidade, deve se assegurar a conformidade com as leis internacionais de Direitos Humanos, incluindo os princípios de legalidade, necessidade e proporcionalidade.[186]

O diploma também sugere que seja sistematicamente assegurada a devida diligência em matéria direitos humanos antes de implantar dispositivos de TRF e, também, durante todo o ciclo de vida das ferramentas implantadas. Foi proposto, igualmente, o estabelecimento de mecanismos de supervisão eficazes, que sejam independentes e imparciais para o uso desta tecnologias.[187] Por fim, o documento pediu pela moratória do uso de tecnologias biométricas em espaços públicos até que as autoridades provem que os sistemas cumpram com altos padrões de privacidade, proteção e não discriminação, impondo regras baseadas no respeito aos Direitos Humanos.[188]

O *website* "Privacy International" veio a considerar este relatório como um passo extremamente positivo para minimizar os danos que estas novas tecnologias representam para o exercício de certos direitos humanos e fundamentais, contudo eles expõe que "ainda há necessidade de determinar os padrões e condições para a implantação de novas tecnologias de vigilância (...) para garantir o cumprimento das normas de Direitos Humanos."[189] Podemos, portanto, considerar a postura da ONU altamente progressista, uma vez que, já em 2020, a instituição estabeleceu diretrizes que proibiam o uso indiscriminado de TRFs para a vigilância em tempo real de locais públicos. Além disso, recomendou que a vigilância direcionada somente fosse adotada quando necessária, proporcional e respaldada pela legislação vigente.

Já em novembro de 2020, as entidades INTERPOL, POLITIE (Polícia Holandesa), UNICRI, WORLD ECONOMIC FORUM se juntaram para lançar uma iniciativa política global e multissetorial para projetar uma estrutura de governança concreta para o uso responsável de

---

[186] UNITED NATIONS. "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Report of the United Nations High Commissioner for Human Rights", 6.
[187] *Ib.,* 11 - 12.
[188] *Ib.,* 15.
[189] PRIVACY INTERNATIONAL. "New UN High Commissioner report highlights the impact new technologies have on the right to protest", 2020.

TRF para investigações policiais.[190] Como resultado parcial do projeto, que propõe-se continuar ativo até 2023, foi lançado o relatório *"A Policy Framework for Responsible Limits on Facial Recognition 2022"* no qual explorou-se um conjunto de princípios orientadores para um uso responsável das TRF, acompanhados por um questionário de auto avaliação, para apoiar as agências de segurança pública na criação e revisão de políticas destas tecnologias em consonância com os princípios expostos. Além de fornecer uma orientação prática, o documento busca enaltecer o debate público sobre o uso da TRF nos níveis nacionais, regionais e internacional, fornecendo uma estrutura concreta para maximizar os benefícios da TRF enquanto mitiga seus riscos a par de uma abordagem *multistakeholder*, incluindo os legisladores, os membros da indústria e a sociedade civil.

O documento em questão divide-se em três partes: definições da TRF e usos desta para investigações, princípios, e um questionário de auto avaliação. Relativamente a primeira parte, o documento explica, de forma técnica, como se dá o processamento destas tecnologias, assim como foi feito na primeira parte desta tese, elucidando os desafios éticos, jurídicos e tecnológicos que esta tecnologia apresenta, incluindo o risco de discriminação, a violação de privacidade e a possibilidade de uso indevido.[191] No quesito de possíveis usos das TRF para investigações, eles ilustram exemplos do seu uso em tempo real e a diferido.

No caso do uso das TRFs em tempo real, que logicamente se reporta ao assunto mais complexo e sensível do debate, o documento explica que certas situações, que se apresentem como uma ameaça sensível, substancial e iminente à vida ou à segurança física, impõe-se, excepcionalmente, recorrer-se ao uso de sistemas de TRFs, sendo exemplo a procura por terroristas em espaços públicos.[192]

Na possibilidade de utilização das TRFs em diferido elucida-se: encontrar a identidade de um criminoso de fraude de caixa eletrônico, descobrir a identidade de um agressor de policiais durante um protesto não pacífico; procurar a identidade de um ladrão de museus;

---

[190] Este projeto teve como foco o uso destas tecnologias para a identificação de suspeitos através do método de "comparação" (comparar uma imagem de um potencial suspeito a um banco de dados biométricos).
[191] INTERPOL, et. al. "A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations", 2022, 4 – 9.
[192] *Ib.,* 17

combater o abuso infantil de crianças dadas como desaparecidas; encontrar pessoas desaparecidas; e, verificar a identidade das pessoas nos controles de fronteiras.[193]

Na segunda parte do documento, foi estabelecido um conjunto de princípios identificados como as bases para garantir a o uso responsável das TRF em investigações policiais, nas situações de tempo real e em diferido. Em primeiro lugar, coloca-se o respeito pelos DH e DF, sendo considerado o princípio abrangente dessa estrutura e visto como a motivação subjacente dos outros princípios em causa, sendo estes: necessidade e proporcionalidade, objetivando um equilíbrio justo entra a segurança da sociedade e a proteção dos direitos humanos dos indivíduos; supervisão e responsabilidade dos humanos, impondo que as linhas de responsabilidade pelo resultado de um determinado uso de TRF devem ser bem definidas e transparentes, sendo que as análises e conclusões deste uso devem ser feitas por uma pessoa com uma certa experiência para tal; otimização do desempenho do sistema, exigindo aos fornecedores desta tecnologia, um cumprimento à rigor de padrões estabelecidos pela ISO ou CEN para avaliar o desempenho de seus algoritmos; mitigação de erros e viés, exigindo a mitigação ao máximo possível através de estratégias de avaliação *ex ante* e *ex post;* legitimidade de imagens de base e de bancos de dados de referência, impondo a conformidade destas imagens com as leis e/ou políticas internacionais, regionais e nacionais, com critérios de armazenamento, limitação de finalidade e período de retenção, sendo que a coleta dessas imagens deve ser feita através de uma base legal, com um propósito específico e com a autorização das autoridades competentes; integridade das imagens e metadados, na qual deve-se estabelecer critérios para avaliar a qualidade da imagem em causa a fim de mitigar o risco de erros; interface humana qualificada para tomada de decisões, que implica que estas tecnologias apenas devem ser utilizadas por pessoas treinadas, seguindo os procedimentos com conformidade; por último, aponta-se a transparência, que implica que as informações sobre a TRF devem estar disponíveis ao público, deixando claro a definição destas tecnologias bem como sua finalidade e objetivos.[194]

Por último, expõe-se o questionário de auto avaliação, projetado para fazer-se uma reflexão sobre os princípios citados acima, destinando-se a apoiar as autoridades públicas a

[193] *Ib.,* 15 - 17
[194] *Ib.*, 18 - 26

desenvolver e revisar as políticas em torno do uso da TRF, levando-os a reflexão de como abordam este uso e quais as regras e procedimentos que devem ou não ter em vigor para fazer um uso responsável desta tecnologia. Esse questionário se apresenta como uma ferramenta para servir de apoio aos entes que cogitam usar desta tecnologia, que deve ser utilizado antes de implementar as TRF, antes de empregá-la no contexto de um novo uso, após cada atualização de software para o algoritmo em causa e após mudanças nas políticas que têm impacto no software ou banco de dados. Para obter as respostas deste questionário, será necessária uma consulta com as várias partes interessadas, incluindo o provedor do sistema de TRF, especialistas em biometria, especialistas em tecnologias e consultores jurídicos. Da resposta a este questionário, expecta-se que se chegue as conclusões de que aquele uso: (1) está em conformidade, (2) não está em conformidade esclarecendo o porquê, (3) não está em conformidade declarando-se as ações que podem ser tomadas para melhoria ou (4) não está em conformidade declarando-se quais ações não podem ser executadas e esclarecendo o porquê.[195]

Podemos afirmar, com facilidade, que este é o documento internacional que abordou de forma mais detalhada o uso das TRF, guiando um caminho para a regulação do seu uso e não da sua proibição, apostando em *standards* que deverão ser seguidos pelos entes que fizerem uso da mesma, através de uma abordagem inovadora, estabelecendo princípios e um questionário de auto avaliação. O documento objetiva padronizar a forma que a TRF é regulada, assegurando respostas uniformes para os problemas evidenciados. No entanto, conforme se pode observar, este relatório apresenta uma diferença curiosa em relação à proposta do OHCHR: enquanto o primeiro advoga a proibição do uso indiscriminado de TRF em tempo real em locais públicos, o segundo permite sua utilização para riscos iminentes à vida, estabelecendo assim uma notável exceção nessa tipologia de aplicação.

Segundo KAY FIRTH-BUTTERFIELD, chefe de IA e *Machine Learning* do Fórum Económico Mundial, "esse relatório mostra a profundidade e a amplitude de como o Fórum é capaz de reunir várias partes interessadas e encontrar soluções para os desafios tecnológicos mais difíceis do nosso tempo. Estamos muito satisfeitos por ter criado um documento que já está sendo adotado por outros para seus regimes de governança e por nossos parceiros no

[195] *Ib.,* 18 – 33.

trabalho".[196] Já IRAKLI BERIDZE, chefe do Centro de Inteligência Artificial e Robótica da UNICRI expõe que "Estamos particularmente orgulhosos da estrutura política para o uso da tecnologia de reconhecimento facial e estamos confiantes de que ajudará as agências de aplicação da lei a garantir que o uso dessa tecnologia respeite os direitos humanos e fundamentais. Isso também pode ser um recurso valioso para o público em geral e encorajamos todos os interessados ou preocupados com essa tecnologia a refletir sobre ela."[197]

O Conselho de Direitos Humanos das Nações Unidas e o UNICRI foram os primeiros órgãos internacionais a abordar de forma direta e objetiva a problemática associada ao uso das TRF. No entanto, algumas instituições emitiram relatórios e documentos sugerindo certas recomendações para um uso responsável da Inteligência Artificial, que incluem algumas diretrizes que podem ser relacionadas ao uso destas tecnologias.

Em primeiro lugar podemos destacar o trabalho concretizado pela OCDE na elaboração do documento "*Recommendation of the Council on Artificial Intelligence"* em 2019, sob proposta do Comité de Política de Economia Digital, sendo o primeiro *standard* intergovernamental sobre a IA. Este documento visa promover a inovação e a confiança da sociedade na IA através de uma utilização responsável destas novas tecnologias, garantindo o respeito pelos direitos humanos e valores democráticos.

Há que relevar que o diploma em causa foi inovador ao tentar harmonizar certas diretrizes e princípios de uma IA responsável a nível internacional. Conforme elucidado pelo advogado WILSON BELCHIOR, "embora os princípios e recomendações não vinculem legalmente os países membros aderentes da OCDE ao documento, eles fornecem perspectivas sobre as leis e regulamentações nacionais que estão em discussão ou elaboração no momento, sendo que a relevância está associada ao fato de essas diretrizes se tornarem padrões internacionais e referência para os interessados".[198]

Embora o documento não aborde especificamente as TRF, ele estabelece uma série de princípios e diretrizes para a IA que podem ser empregues a diversas tecnologias, inclusive o

---

[196] MODERN DIPLOMACY. "Proposed Law Enforcement Principles on the Responsible Use of Facial Recognition Technology", 2022.
[197] *Ib.*
[198] BELCHIOR, Wilson Sales. "Artificial Intelligence, OECD principles and recommendations (Part I)", 2021.

reconhecimento facial. Em primeiro lugar, o documento da OCDE destaca a importância da transparência e explicabilidade na IA[199]. Isso é particularmente importante no contexto do reconhecimento facial, pois partindo de uma hipótese que estas tecnologias estejam a ser empregadas, as pessoas precisam saber quando, como e por quem os seus dados biométricos estão sendo coletados e usados; como os sistemas de reconhecimento facial chegam a certas conclusões; e, onde as pessoas estão a ser monitoradas. A transparência e explicabilidade podem ajudar a garantir a justiça e equidade na aplicação desses sistemas.

Em segundo lugar, o documento enfatiza a importância da privacidade e proteção de dados no desenvolvimento de sistemas de IA, realçando a importância de se respeitar as leis de privacidade e proteção de dados vigentes.[200] Como no contexto do reconhecimento facial tratamos de dados biométricos, que são informações altamente sensíveis que podem ser usadas para identificar e rastrear pessoas, podemos inferir que as empresas e governos que usam sistemas de reconhecimento facial devem garantir que os dados sejam protegidos e usados apenas para fins legítimos, seguindo as leis e regulamentos de privacidade de dados.

No que diz respeito a inclusão e não discriminação na IA, o documento reconhece a importância da não discriminação no desenvolvimento e implementação de sistemas de IA, enfatizando que tais sistemas devem ser projetados e desenvolvidos de maneira a respeitar os direitos humanos, incluindo o princípio da não discriminação.[201] O documento destaca que os sistemas de IA não devem ser usados para discriminar indivíduos ou grupos com base em suas características pessoais, como raça e etnia, gênero, idade ou deficiência.

Por fim, o documento da OCDE destaca a importância da cooperação internacional na regulação da IA sendo que esta pode ajudar a garantir que os sistemas de reconhecimento facial sejam regulamentados de maneira consistente em todo o mundo, protegendo principalmente os direitos humanos e fundamentais, com relevo a privacidade, proteção de dados e a não discriminação.

Em novembro de 2021 foi a vez da UNESCO fazer suas próprias recomendações através do documento *"Recommendation on the ethics of artificial intelligence"* abordando questões

---

[199] OECD, "Recommendation of the Council on Artificial Intelligence", OECD/LEGAL/0449, 2022, 8.
[200] *Ib.,* 7-8.
[201] *Ib.,* 7.

éticas relacionadas ao campo da inteligência artificial. Ela oferece um marco holístico, abrangente e multicultural de valores, princípios e ações interdependentes que podem orientar as sociedades para lidar de forma responsável com os impactos conhecidos e desconhecidos das tecnologias de IA sobre seres humanos, sociedades, meio ambiente e ecossistemas. A Recomendação dá atenção especial às implicações éticas mais amplas dos sistemas de IA em relação às áreas centrais de atuação da UNESCO: educação, ciência, cultura e comunicação e informação.

Na análise da Recomendação iremos relevar as seguintes 3 secções: (1) objetivos, (2) princípios e valores, (3) e áreas de atuação política. No que diz respeito aos seus objetivos, a UNESCO propõe uma estrutura universal para orientar os Estados na legislação e políticas relacionadas à IA, de acordo com o direito internacional. Seu objetivo é incorporar a ética em todas as fases do ciclo de vida dos sistemas de IA, protegendo os direitos humanos, a igualdade de gênero e a diversidade cultural. Além disso, busca preservar o meio ambiente, promover o diálogo entre várias partes interessadas e garantir acesso equitativo aos desenvolvimentos e conhecimentos em IA.[202]

Sobre os valores em causa, o documento considera que estes, em consonância com os princípios, servirão como a base que irá sustentar a formação de políticas e legislações. São estes: respeito, proteção e promoção dos direitos humanos e liberdades fundamentais e da dignidade humana; ambiente e ecossistema próspero; garantir a diversidade e a inclusão; viver em sociedades pacíficas, justas e interconectadas.[203] relativamente aos princípios consagrados, que foram posteriormente adotados pelos sistemas das nações unidas,[204] incluiu-se: proporcionalidade e não maleficiência; segurança e proteção; justiça e não discriminação; sustentabilidade; direito à privacidade e proteção de dados; supervisão e determinação humana; transparência e explicabilidade; responsabilidade e prestação de contas; conscientização e literacia; governança e colaboração numa abordagem *multistakeholder.*[205]

---

[202] UNESCO, "Recommendation on the ethics of artificial intelligence", 2021, 14 - 16
[203] *Ib.,* 18 - 20
[204] UNITED NATIONS SYSTEM. "Principles for the Ethical Use of Artificial Intelligence in the United Nations System", 2022.
[205] UNESCO, "Recommendation on the ethics of artificial intelligence, 10.

No que tange às áreas de atuação política, estas irão operacionalizar os valores e princípios estabelecidos, ensejando aos Estados a implementação de medidas efetivas (como estruturas ou mecanismos políticos) que garantam que todas as partes envolvidas, como os Governos, empresas do setor privado, instituições académicas e a sociedade civil, respeitem os DH, o Estado de Direito e a Democracia num todo. Estas áreas dividem-se em: avaliação de impacto ético; governança e administração ética; política de dados; desenvolvimento e cooperação internacional; meio ambiente e ecossistemas; gênero; cultura; educação e pesquisa; comunicação e informação; economia e trabalho; saúde e bem-estar social.[206]

Podemos destacar a ação da UNESCO em tornar como princípio de atuação da IA o direito à privacidade e proteção de dados e a justiça e não discriminação. Em relação ao primeiro a recomendação destaca a privacidade como um direito essencial para proteger a dignidade, autonomia e capacidade de ação humana, devendo ser respeitada, protegida e promovida ao longo do ciclo de vida dos sistemas de IA. Também ressaltou-se a importância de coletar, usar, compartilhar, armazenar e excluir dados de maneira compatível com o direito internacional e os valores estabelecidos, sendo necessário estabelecer marcos e mecanismos de governança adequados para proteção de dados, levando em consideração as partes interessadas e garantindo a proteção por meio de sistemas judiciais. Propõe-se que os sistemas algorítmicos devam passar por avaliações de impacto na privacidade, considerando também aspectos sociais e éticos, sendo que os atores de IA devem assumir responsabilidade pelo projeto e implementação dos sistemas, garantindo a proteção das informações pessoais ao longo do ciclo de vida.[207]

No que diz respeito ao princípio de justiça e não discriminação, a recomendação expõe que os atores de IA devem promover a justiça social, equidade e não discriminação, garantindo que os benefícios da IA sejam acessíveis a todos, incluindo grupos marginalizados. Ela expõe que os Estados devem promover o acesso inclusivo à IA, abordando exclusões digitais e desigualdades entre áreas rurais e urbanas. No cenário internacional, aconselha-se que países avançados tecnologicamente têm a responsabilidade de compartilhar os benefícios da IA com os menos avançados, sendo crucial minimizar a discriminação ao longo do ciclo de vida da IA e abordar exclusões digitais e de conhecimento. Completa-se a exposição do princípio expondo

[206] *Ib.,* 25 – 39.
[207] *Ib.,* 20.

que todos devem ser tratados de forma equitativa em termos de acesso e participação na IA, em conformidade com os marcos jurídicos relevantes.[208]

Conforme aponta ANDY VAN PACHTENBEKE "A recomendação é inovadora porque é o primeiro instrumento jurídico global sobre a ética da IA, mas também devido ao seu forte foco nos direitos humanos e ao reconhecimento da importância dos atores privados (...). Contudo a Recomendação não é perfeita. A sua implementação não está garantida e sem dúvida surgirão alguns novos desafios que nem mesmo o amplo texto deste instrumento foi capaz de prever. Tal é a natureza eterna da própria lei. Quem pode dizer se a singularidade, o ponto em que a humanidade perde o controle sobre a tecnologia, pode ser totalmente evitada? No entanto, para aqueles que desejam aplicar uma abordagem ética baseada em direitos humanos à inteligência artificial, esta recomendação fornece uma base muito sólida." [209]

A Recomendação da UNESCO converge em muitos pontos com o documento concretizado pela OCDE, pelo que retira-se de forma muito semelhante, algumas conclusões sobre como este documento se coaduna com as problemáticas associadas ao uso das TRF, principalmente na proteção de dados, discriminação e privacidade. Contudo, podemos destacar o êxito do trabalho elaborado pela UNESCO por denunciar de forma objetiva a proibição de sistemas de inteligência artificial utilizados para vigilância em massa e *social scoring*[210].O documento proporciona um guia abrangente aos Governos sobre a elaboração de seus instrumentos legislativos, levando em consideração os princípios propostos. Essa assistência se revela extremamente valiosa para orientar a regulamentação e o estudo aprofundado do desenvolvimento de sistemas de reconhecimento facial. Caso os Governos optem por adotar tais sistemas, é imprescindível que eles sejam pautados pela ética, transparência e justiça, assegurando a proteção dos direitos humanos e fundamentais da sociedade.

É importante ressaltar que todos os diplomas mencionados representam uma abordagem de *soft law*, ou seja, carecem de qualquer força juridicamente vinculativa. No entanto, devemos reconhecer seus êxitos ao estabelecerem *guidelines* e princípios para orientar uma IA

---

[208] *Ib.,* 20 – 21.

[209]PACHTENBEKE, Andy Van. "UNESCO Recommendation on the Ethics of Artificial Intelligence Human Rights-based & Future oriented", 2022.

[210] UNESCO, "Recommendation on the ethics of artificial intelligence", 20.

responsável, enfatizando o absoluto respeito pelos DH e DF. Embora tais documentos não imponham aos Estados a adoção de padrões de regulamentação para o uso de sistemas de reconhecimento facial, eles servirão como base e incentivo para que iniciativas legislativas nacionais sejam concretizadas. No entanto, o debate jurídico sobre o uso de sistemas de reconhecimento facial em práticas de vigilância ou de coleta de dados biométricos ainda está em curso, uma vez que não há um consenso real sobre sua regulação ou proibição. Os instrumentos internacionais apresentados até agora têm sugeriram três caminhos: (1) de moratória, (2) regulamentação quanto ao uso ou (3) proibição.

## 3. O PAPEL PIONEIRO DO CONSELHO DA EUROPA

Na análise de instrumentos jurídicos num âmbito regional, o Conselho da Europa abordou a temática da IA logo em 2017 na sua *Recommendation 2102 - "Technological convergence, artificial intelligence and human rights* evidenciando que o desenvolvimento destas novas tecnologias pode ter um efeito direto nos DH dos europeus. O documento inicia-se destacando a problemática: "A convergência entre nanotecnologia, biotecnologia, tecnologia da informação e ciências cognitivas e a velocidade com que as aplicações de novas tecnologias são colocadas no mercado têm consequências não apenas para os direitos humanos e a forma como podem ser exercidos, mas também para o conceito fundamental do que caracteriza um ser humano."[211]

Nesta lógica e como iremos identificar, é notável a preocupação do CoE com o crescimento da IA e os riscos que lhe estão associados a esta. Sendo uma organização intergovernamental que objetiva a promoção dos direitos humanos, da democracia e do estado de direito, os instrumentos divulgados pela mesma irão ter uma preocupação cabal com a proteção do indivíduo perante excessos que possam derivar destas novas tecnologias. A CoE reconhece os desafios éticos, jurídicos e sociais associados ao desenvolvimento da IA, e traz soluções concretas e objetivas para tal - na adoção de medidas, recomendações, diretrizes e normas que garantam a proteção dos DH e salvaguardem os princípios democráticos.

[211] CoE. "Recommendation 2102 (2017): Technological convergence, artificial intelligence and human rights", 2017, 1.

Sendo assim, iniciaremos nosso enquadramento jurídico pelos documentos emitidos pelo CoE, que desempenhou um papel fundamental na análise das implicações da convergência entre Inteligência Artificial e Direitos Humanos, bem como das problemáticas inerente ao uso das TRFs nos sistemas biométricos à distância. Nesta lógica podemos, desde já, inferir que o Direito ao respeito pela vida privada e familiar e a Proibição de discriminação são direitos protegidos pelos artigos 8º e 14º da CEDH, realçando a sua relevância neste âmbito.

Podemos começar a análise jurídica do CoE pela *Resolution 2045(2015) Mass surveillance* adotada em 21 de abril de 2015 antes da IA ainda ser um grande problema societal. Este documento representa uma resposta às práticas de vigilância em massa que foram reveladas por jornalistas desde junho de 2013 a quem Edward Snowden, ex-contratado da NASA dos EUA, confiou uma quantidade significativa de dados altamente confidenciais. Essas revelações evidenciaram a existência da vigilância em massa em práticas intrusivas da privacidade à escala mundial, previamente desconhecidas tanto para o público em geral quanto para a maioria dos políticos.[212]

Além desta Resolução evidenciar que a vigilância praticada implicou a violação dos direitos à privacidade e a proteção de dados, que são considerados alicerces essenciais de um Estado Democrático de Direito, reconheceu-se um importante aspecto sobre a vigilância (de indivíduos singulares) de um suspeito ao separá-la em duas dimensões - dimensão não direcionada ou direcionada.

Desta dicotomia, conclui-se que a dimensão direcionada pode ser necessária quando estejam em causa suspeitos de terrorismo e outros grupos criminosos organizados, representando uma ferramenta eficaz para a aplicação da lei e a prevenção do crime. Contudo, de acordo com avaliações independentes realizadas nos Estados Unidos, a vigilância em massa não direcionada não parece ter contribuído para a prevenção de ataques terroristas, sendo que recursos que poderiam ser empregados na prevenção de ataques de outras formas foram desperdiçados nas técnicas de vigilância em massa, permitindo que indivíduos potencialmente perigosos, que pudessem ser identificado de outras formas, ajam impunemente.[213]A Assembleia de Ministros também veio afirmar que as consequências decorrentes do acesso de regimes

[212] COUNCIL OF EUROPE - CoE. "Resolution 2045(2015) Mass surveillance", 2015, 1.
[213] *Ib.,* 2.

autoritários a ferramentas de vigilância em massa, como aquelas desenvolvidas pelos Estados Unidos e seus serviços aliados, seriam de proporções catastróficas, sendo que mesmo em democracias consolidadas, em períodos de crise, não é descartada a possibilidade de o poder executivo cair nas mãos de políticos extremistas e a verdade é que já é amplamente conhecido o uso de tecnologias avançadas de vigilância em diversos regimes autoritários, visando, por muitas vezes, localizar opositores e suprimir a liberdade de informação e expressão.[214]

A partir disto, podemos retirar que a Assembleia manifestou uma clara preocupação com as práticas de vigilância que ameaçam os DH, incluindo privacidade, proteção de dados, liberdade de informação e expressão, um julgamento justo e a liberdade religiosa. Ela solicitou aos Estados membros que respeitem plenamente suas obrigações internacionais de direitos humanos, garantindo que qualquer interferência na privacidade seja estritamente necessária e proporcional. Além disso, ela instou os Estados Membros a estabelecerem mecanismos independentes de supervisão para assegurar transparência, responsabilização e recursos efetivos em casos de violações dos direitos à privacidade. [215]

Esta resolução, a par de outros instrumentos legislativos que iremos nos debruçar, teve o seu relevo em abordar as problemáticas associadas a vigilância em massa - aqui posta não a par de sistemas de identificação biométrica, mas sim da coleta e vazamento ilegais e indiscriminado de dados pessoais, que causam sérios prejuízos a privacidade dos indivíduos e afetam a proteção conferida aos seus respectivos dados, recomendando aos Estados tomarem ações efetivas para evitar que tais violações, como as denunciadas por Snowden, voltem a acontecer.

Outro instrumento legislativo de grande relevo da CoE é o tratado internacional inerente à proteção de dados pessoais denominada Convenção 108. Com mais de 55 signatários (incluindo países fora da UE), a Convenção foi instituída em 1981 na França, sendo até os dias de hoje um dos mais relevantes instrumentos desta temática. Ela é uma regulação transversal que estipula um regime de governança para questões de proteção de dados pessoais, consistindo em um marco internacional que começou a pavimentar uma potencial estrutura global de

[214] *Ib.*
[215] *Ib.,* 3.

proteção de dados.[216] Nesta, os Estados signatários são compelidos a estabelecer estruturas jurídicas que regulamentem o processamento de dados pessoais, abrangendo aspectos relacionados à coleta, armazenamento, uso e divulgação. Ademais, a Convenção estabelece princípios fundamentais para a proteção de dados, incluindo a transparência, a limitação de finalidade e a implementação de medidas de segurança adequadas.

Diante da importância do instrumento e levando em consideração o rápido crescimento do compartilhamento e processamento de dados pessoais na era digital, o Conselho da Europa realizou uma atualização desta, que passou a ser chamada de Convenção 108+, em 2018. Essa atualização foi promovida uma semana antes da entrada em vigor do RGPD, com o objetivo de adaptar-se às novas tecnologias e fortalecer os mecanismos de monitoramento do cumprimento por parte daqueles que se comprometem e aderem à convenção.

A Convenção 108+ trouxe contribuições significativas na proteção dos indivíduos perante técnicas de reconhecimento facial automatizadas: em primeiro lugar podemos citar o reconhecimento explícito dos dados biométrico dentro da categoria de dados especiais[217]; estabeleceu-se que para realizar-se o processamento de dados biométricos será necessário o consentimento livre, específico, informado e inequívoco do titular dos dados[218]; a garantia de um processamento justo e transparente dos dados biométricos[219], sendo mecanismos relevantes para monitorar e regular o uso de TRF; e, a importância dada aplicação de medidas de segurança adequadas para proteger os dados pessoais[220], incluindo aqueles utilizados no reconhecimento

[216] FACHINETTI, Aline Fuke / CAMARGO, Guilherme. "Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil", 2021.

[217] Na Convenção 108 tínhamos no artigo 6º a consagração de uma categoria especial de dados que expunha: "Os dados pessoais que revelem a origem racial, as opiniões políticas ou religiosas ou outras crenças, bem como os dados pessoais relativos à saúde ou à vida sexual, não podem ser processados automaticamente, a menos que a legislação nacional forneça salvaguardas adequadas. O mesmo se aplica aos dados pessoais relativos a condenações penais.". O que a Convenção 108+ fez foi fazer uma lista taxativa de quais dados são pertencentes a esta categoria especial, incluindo o exposto no seu antigo artigo 6º e adicionando outras tipologias de dados, como os dados biométricos.

[218] Previsto no artigo 5º nº2 da Convenção 108+ Cfr. COUNCIL OF EUROPE - CoE. "Convenção 108+ Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal", 2018. Curiosamente a antga convenção só cita a palavra consentimento 3 vezes e em nenhuma vez relacionada com a permisão para o processamento de dados.

[219] Artigo 8º da Convenção 108+.

[220] Artigo 7º da Convenção 108+.

facial, sendo que isso pode ser útil para garantir a integridade e confidencialidade dos dados coletados e processados por essas tecnologias.

Assim sendo, em 28 de janeiro de 2021 o Comitê Consultivo da Convenção para a Proteção das Pessoas Físicas em Relação ao Tratamento Automático de Dados Pessoais, composto por especialistas representando os 55 Estados Partes da Convenção, bem como 20 países observadores[221], adotou um novo conjunto de diretrizes sobre o reconhecimento facial[222] direcionadas a legisladores, governadores e empresas, fornecendo algumas medidas para servirem de referências à estes atores, para garantir que o uso das TRFs não afetem negativamente a dignidade humana, os direitos humanos e as liberdades fundamentais de qualquer pessoa.[223]

A Secretária-geral do Conselho da Europa, Marija Pejčinović Burić, expôs sua opinião sobre as novas diretrizes: "Na melhor das hipóteses, o reconhecimento facial pode ser conveniente, ajudando-nos a superar obstáculos em nossa vida cotidiana. Na pior das hipóteses, ameaça nossos direitos humanos essenciais, incluindo privacidade, igualdade de tratamento e não discriminação, capacitando autoridades estatais e outros para monitorar e controlar aspectos importantes de nossas vidas – muitas vezes sem nosso conhecimento ou consentimento. Mas isso pode ser interrompido. Estas diretrizes asseguram a proteção da dignidade pessoal, dos direitos humanos e das liberdades fundamentais das pessoas, incluindo a segurança dos seus dados pessoais."[224]

Neste sentido, o documento em questão se divide em três partes que serão analisadas: as diretrizes para legisladores e tomadores de decisões; para desenvolvedores, fabricantes e prestadores de serviços; e, por último, para as entidades que façam uso das tecnologias de reconhecimento facial.

No que diz respeito a primeira parte do documento, destacou-se, desde logo, a importância do princípio da legalidade, previsto no artigo 6º da Convenção 108+, destacando que o processamento de dados biométricos "só deve ser autorizado se esse processamento se

[221]COUNCIL OF EUROPE. "Facial recognition: strict regulation is needed to prevent human rights violations", 2021.
[222] COUNCIL OF EUROPE - CoE. "Guidelines on facial recognition", 2021.
[223] *Ib.,* 3.
[224]EUR-LEX. "O direito primário da União Europeia", 2016.

basear em uma base legal apropriada e se garantias complementares e apropriadas forem estabelecidas na legislação nacional"[225] e que a "necessidade do uso de tecnologias de reconhecimento facial (TRF) deve ser avaliada em conjunto com a proporcionalidade em relação à finalidade e ao impacto nos direitos dos titulares dos dados"[226]

O documento expõe certas limitações que devem ser impostas ao uso das TRFs, nomeadamente "com o único propósito de determinar a cor da pele de uma pessoa, crenças religiosas ou outras, sexo, origem racial ou étnica, idade, condição de saúde ou condição social devem ser proibidas, a menos que salvaguardas apropriadas sejam previstas por lei para evitar qualquer risco de discriminação".[227] Também é restrito o *affect recognition* "para detectar traços de personalidade, sentimentos internos, saúde mental ou envolvimento dos trabalhadores a partir de imagens faciais. Vincular o *affect recognition*, por exemplo, à contratação de pessoal, acesso a seguros, educação pode representar riscos de grande preocupação, tanto no nível individual quanto social, e deve ser proibido."[228]

No que diz respeito à formação de modelos biométricos e à construção de uma base de dados, o documento afirma que "os legisladores devem assegurar que as imagens disponibilizadas em formato digital não possam ser tratadas (...) sem base legal específica para tal, quando essas imagens foram inicialmente captadas para outros fins (de redes sociais, por exemplo) (...) apenas para fins legítimos superiores, previstos por lei e estritamente necessários e proporcionais para esses fins (segurança pública, ou fins médicos).[229]

Esta secção do documento inclui uma discussão sobre o uso das TRF nos setores público e privados. No que diz respeito ao primeiro, o Conselho da Europa afirma que "o consentimento não deve ser, regra geral, o fundamento jurídico utilizado para o reconhecimento facial (...) considerando o desequilíbrio de poderes entre os titulares dos dados e as autoridades públicas"[230] e que "os legisladores e tomadores de decisão devem estabelecer regras específicas para o processamento biométrico por tecnologias de reconhecimento facial para fins de aplicação da

[225] COUNCIL OF EUROPE - CoE. "Guidelines on facial recognition", 4.
[226] *Ib.*
[227] *Ib.,* 5.
[228] *Ib.*
[229] *Ib.,* 6.
[230] *Ib.*

lei. Essas leis garantirão que tais usos sejam estritamente necessários e proporcionais para esses fins e prescreverão as garantias necessárias a serem fornecidas."[231] sendo que os princípios da necessidade e proporcionalidade devem ser observados tanto na criação do banco de dados, quanto na implementação destas tecnologias em locais públicos.

Em relação ao seu uso no setor privado, o Conselho da Europa lembra a exigência de obter o "consentimento explícito, específico, livre e informado[232] dos titulares dos dados cujos dados biométricos são processados destacando que os titulares dos dados devem ser oferecidas soluções alternativas ao uso de tecnologias de reconhecimento facial."[233] Além disso apontam que as entidades privadas não devem implantar TRFs em ambientes como centros comerciais, especialmente para a identificação de pessoas para fins de marketing ou de segurança privada.[234]

Consequentemente, pode-se inferir que a posição adotada pelo Conselho da Europa implica que o processamento de dados biométricos por meio de tecnologias de reconhecimento facial, em ambientes "controlados" e "não controlados" no setor público, é permitido, mas fica restrito às autoridades competentes no campo da segurança, desde que seja justificada por uma necessidade estrita e proporcional para alcançar seus objetivos. Por outro lado, no caso do setor privado, tais tecnologias só podem ser empregadas com base no consentimento livre, específico, explícito e informado dos indivíduos envolvidos.

De volta à análise da primeira parte do documento, ele, por fim, aborda a questão da participação das autoridades de supervisão, ressaltando que elas devem ser consultadas em relação a propostas de medidas legislativas ou administrativas. Além disso, o documento destaca a importância da certificação dessas tecnologias e da necessidade de melhorar a conscientização das pessoas envolvidas.[235]

A primeira parte das diretrizes objetivaram estabelecer uma base sólida para a aplicação ética e legal de tecnologias de reconhecimento facial definindo orientações louváveis para estatuição responsável de TRF. Tais instruções visaram garantir a supervisão adequada, a conformidade legal e a proteção dos direitos individuais. Na adoção de tais medidas, buscou-se

---

[231] *Ib.*
[232] Previsto no artigo 5º da Convenção 108+.
[233] COUNCIL OF EUROPE - CoE. "Guidelines on facial recognition", 7.
[234] *Ib.*
[235] *Ib.,* 8.

assegurar que o uso dessas tecnologias seja realizado de maneira responsável em conformidade com os princípios da legalidade, da transparência, segurança e ao respeito aos direitos humanos, tanto no setor público quanto no privado.

Contudo, o uso de tais tecnologias por autoridades policiais no zelo pela aplicação da lei pode ser extremamente perigoso e conduzir a graves violações de privacidade, proteção de dados pessoais e a não discriminação. Embora os princípios de estrita necessidade e proporcionalidade sejam considerados como salvaguardas para o uso de TRF, eles podem não ser suficientes para garantir a proteção dos direitos individuais. O princípio da estrita necessidade exige que o uso dessas tecnologias seja justificado por uma necessidade premente, ou seja, apenas quando não houver alternativas menos invasivas disponíveis para atingir o mesmo objetivo.[236] No entanto, a definição do que constitui uma necessidade estrita pode ser subjetiva e sujeita a interpretações amplas por parte das autoridades.[237] Da mesma forma, o princípio da proporcionalidade exige que o uso das tecnologias de reconhecimento facial seja proporcional aos objetivos legítimos perseguidos e que os benefícios superem os potenciais danos e restrições aos direitos individuais. No entanto, determinar o equilíbrio adequado entre segurança pública e proteção dos direitos individuais pode ser um desafio complexo, e há o risco de que os poderes estendidos concedidos às autoridades policiais possam ser abusados ou usados de maneira inadequada.

Já a segunda parte do documento, dirigida a desenvolvedores, fabricantes e prestadores de serviços de TRFs, focou-se em questões objetivas e relacionadas às fases de desenvolvimento e fabricação destas tecnologias, especialmente no que diz respeito aos dados utilizados por tais.

As diretrizes dão especial atenção à representatividade dos dados utilizados, lembrando que há uma obrigatoriedade da veracidade dos dados. Sendo assim, os desenvolvedores e fabricantes "terão que tomar medidas para garantir que os dados de reconhecimento facial sejam precisos" para evitar "discriminação não intencional" ou viés[238]. No que diz respeito à representatividade dos dados, também é abordada a questão da expectativa de vida e

[236]CANOTILHO, Mariana. "O princípio constitucional da proporcionalidade e o seu lugar na metódica constitucional: breves apontamentos a propósito da metáfora da balança", 2021, 29.
[237] *Ib. 23.*
[238] COUNCIL OF EUROPE - CoE. "Guidelines on facial recognition", 9.

confiabilidade dos dados. Neste sentido, o CoE sublinha que "um sistema de reconhecimento facial requer a renovação periódica dos dados (as fotos dos rostos a reconhecer) para treinar e melhorar o algoritmo utilizado"[239], com o objetivo de garantir o melhor nível de fiabilidade possível no sistema.

Por fim, o documento fornece orientações para os desenvolvedores e fabricantes sobre conscientização e responsabilidade. No que diz respeito à primeira, propôs-se realizar recomendações sobre transparência e privacidade, no intuito de auxiliar as entidades que utilizam estas tecnologias, como "fornecendo-lhes um exemplo de linguagem para suas políticas de privacidade ou recomendando sinalização de fácil compreensão que indica que uma tecnologia de reconhecimento facial está implantada em um espaço específico".[240]

Em relação a responsabilidade, as diretrizes apontam que as empresas que desenvolvem e comercializam tecnologias de reconhecimento facial devem adotar medidas específicas para garantir a conformidade com os princípios de proteção de dados. Isso inclui a integração da proteção de dados no design e arquitetura dos produtos e serviços, o uso de ferramentas dedicadas e a exclusão automática de dados brutos, flexibilidade no design para ajustar as salvaguardas técnicas, realização de revisões internas para mitigar impactos nos direitos fundamentais e humanos, integração de uma abordagem de proteção de dados nas práticas organizacionais, designação de equipe dedicada, treinamento de privacidade e realização de avaliações de impacto de proteção de dados. Essas medidas visam garantir a privacidade, segurança e conformidade das TRFs, demonstrando um compromisso ético e responsável no desenvolvimento e uso dessas.[241]

Relativamente a esta segunda parte do documento, abordou-se de forma abrangente as fases de desenvolvimento e fabricação de TRF, destacando a importância da representatividade e veracidade dos dados para evitar discriminação e viés. O documento ressaltou a necessidade de medidas para garantir a precisão dos dados, reconhecendo a importância da renovação periódica dos dados para treinar e aprimorar os algoritmos. Além disso, as diretrizes enfatizaram a conscientização e responsabilidade dos desenvolvedores e fabricantes, buscando promover

---

[239] *Ib.,* 9.
[240] *Ib*., 10.
[241] *Ib.*

uma cultura ética e responsável. Tais diretrizes se mostram essenciais para mitigar riscos e proteger os direitos individuais em um contexto digital orientado por dados.

No que diz respeito à última parte do documento, dirigida às entidades que utilizam destas tecnologias, a CoE propõe que estas "têm de cumprir todos os princípios e disposições de proteção de dados aplicáveis durante o tratamento de dados biométricos na sua utilização de TRF"; "devem ser capazes de demonstrar que essa utilização é estritamente necessária, e proporcionada, no contexto específico da sua utilização e que não interfere com os direitos dos titulares dos dados"; "devem garantir que o uso voluntário da tecnologia não tenha impacto sobre indivíduos que entrem em contato involuntariamente com ela".[242]

Após estas considerações iniciais, o documento dedica-se à legitimidade do processamento de dados e à qualidade dos mesmos. O órgão elabora diretrizes baseadas em princípios fundamentais que devem ser aplicados às tecnologias de reconhecimento facial, incluindo transparência e imparcialidade, limitação de finalidade, minimização de dados e períodos limitados de retenção de dados, bem como a necessidade de garantir a precisão dos mesmos[243], referindo ainda o valor da importância no uso de tais tecnologias, impondo a implementação "fortes medidas de segurança, tanto a nível técnico como organizacional (...) para proteger os dados de reconhecimento facial e conjuntos de imagens".[244]

O enfoque direciona-se, então, à questão da responsabilidade, sendo elencadas uma série de medidas organizacionais a serem adotadas pelas entidades que implementam tais tecnologias, com o intuito de cumprir suas obrigações e evidenciar o controle exercido sobre o tratamento de dados. As novas diretrizes também enfatizam a importância das avaliações de impacto da proteção de dados e da proteção de dados desde o estágio de concepção, buscando fomentar a conformidade com as disposições aplicáveis às tecnologias de reconhecimento facial. Ademais, destaca-se que, além da observância das obrigações legais, conferir uma estrutura ética ao uso dessa tecnologia também se revela crucial.[245]

---

[242] *Ib.*
[243] *Ib.,* 10 - 12
[244] *Ib.,* 13.
[245] *Ib*., 14 - 15.

Como pontua JELENA BRAJKOVIC, “as Diretrizes são significativas representando o primeiro documento, com uma certa autoridade, de escopo tão amplo a avaliar a conformidade do reconhecimento facial com os princípios de proteção de dados e requisitos específicos. Devido à grande semelhança entre o RGPD e a Convenção 108+ do Conselho da Europa, é provável que as Diretrizes sejam uma ferramenta útil ao implantar tecnologias de reconhecimento facial nos países da Europa.”[246] KONSTANTINOS KOROUPIS completa enfatizando que “essas diretrizes reafirmam a necessidade imperativa de atender aos princípios fundamentais de necessidade, proporcionalidade, precisão, legalidade, justiça e transparência”[247] que iremos observar novamente na legislação europeia - nomeadamente a RGPD e a LED.

Em 3 de novembro de 2021, o Comitê de Ministros do Conselho da Europa (doravante referido como "o Comitê") promulgou a Recomendação CM/Rec (2021)8, a qual aborda a salvaguarda dos direitos individuais no âmbito do processamento automatizado de dados pessoais no contexto da criação de perfis (*profiling*).Considerando os avanços significativos ocorridos na última década em relação aos métodos e impactos da criação de perfis, o Comitê reconheceu a necessidade de atualizar sua Recomendação de 2010 e também de alinhá-la com as disposições da Convenção 108+ modernizada para uma maior salvaguarda da proteção de dados e da vida privada dos indivíduos.

Logo no início da recomendação, o Comitê apresenta certas definições para alguns termos dentro do âmbito da IA, como “*machine leaning processing”* e “*categories of data processed”*. No que diz respeito a criação de perfis, esta vem ser definida como: “qualquer forma de tratamento automatizado de dados pessoais, incluindo a utilização de sistemas de aprendizagem automática, consistindo na utilização de dados para avaliar determinados aspetos pessoais relativos a um indivíduo, nomeadamente para analisar ou prever aspetos relativos ao seu desempenho laboral, situação económica, saúde, preferências pessoais, interesses, confiabilidade, comportamento, localização ou movimentos.”[248] Nestas definições também foi

[246] BRAJKOVIC, Jelena. “Council of Europe’s useful guidance concerning facial recognition”, 2021.
[247] KOUROUPIS, Konstantinos. “Facial Recognition: a challenge for Europe or a threat to human rights?”, 147.
[248] COUNCIL OF EUROPE - CoE. “Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling”, 2021, 9.

estabelecido o que se refere a "*High risk profiling*": operações de criação de perfis que produzam efeitos jurídicos ou tenham um impacto significativo no titular dos dados ou no grupo de pessoas identificadas pela referida criação de perfis; a criação de perfis que – devido ao público-alvo, ao contexto ou à finalidade da definição de perfis – especialmente em situação de desequilíbrio do poder de informação, envolva o risco de afetar ou influenciar indevidamente os titulares dos dados, nomeadamente no caso de menores e outras pessoas vulneráveis; criação de perfil que envolva dados qualificados como categorias especiais de dados de acordo com o Artigo 6º da Convenção 108+ ou que vise detectar ou prever esses dados; criação de perfis que afete um grande número de indivíduos, incluindo a criação de perfis realizada por serviços intermediários online para uso próprio ou de terceiros.[249]

Relativamente aos princípios gerais da recomendação, previu-se que o respeito pelos direitos e liberdades fundamentais, nomeadamente a dignidade humana, a privacidade, a liberdade de expressão, a não discriminação, a justiça social, a diversidade cultural e a democracia devem ser garantidos nos setores público e privado durante todas as operações de criação de perfis; que a criação de perfil não possa resultar em discriminação contra indivíduos, grupos ou comunidades; que não se viole nem a dignidade das pessoas nem a democracia; que a utilização de sistemas automatizados de tomada de decisão deve preservar a autonomia da intervenção humana no processo decisório; que os Estados Membros devem encorajar a privacidade desde a criação, através da utilização de tecnologias de reforço da privacidade, e tomar as medidas adequadas para impedir o desenvolvimento de tecnologias destinadas a contornar as proteções da privacidade; e, que nos casos em que a criação de perfis se baseie no consentimento, os serviços em linha devem dar aos titulares dos dados a possibilidade de optar pela criação de perfis ou não e de escolher entre as diferentes finalidades ou graus de criação de perfis..[250]

Para tal, é exigido certas condições para o tratamento de dados pessoais no contexto da criação de perfis, nomeadamente: a legalidade, sendo que o tratamento de dados pessoais para uma finalidade compatível no âmbito da definição/criação de perfis só pode ser efetuado se

[249] *Ib.* 9.
[250] *Ib.* 9 – 10.

estiver previsto na legislação nacional ou se basear no consentimento[251]; a qualidade dos dados e algoritmos, propondo o estabelecimento de medidas adequadas para corrigir imprecisões nos dados e minimizar os riscos de erros e vieses associados à criação de perfis, realização de avaliações periódicas da qualidade dos dados e inferências estatísticas utilizadas e, os responsáveis devem obtenção da documentação necessária para verificar a qualidade e relevância dos dados e algoritmos, quando adquiridos por terceiros;[252] por último, relativamente a categoria especial de dados, propõe-se que o processamento de dados relacionados à origem racial ou étnica, opiniões políticas, filiação sindical, crenças religiosas, saúde ou vida sexual deve ser proibido, exceto quando houver salvaguardas adequadas estabelecidas por lei e quando os dados forem estritamente necessários para fins lícitos e específicos.[253]

Após tais condições, o documento traz mais algumas recomendações que revelam expor: a importância de garantir o fornecimento de todas a informações para atestar a justeza no processo de criação;[254] o direito dos titulares de dados, ao conceder o direito deste de, a toda hora, puderem ter informações sobre o seu processamento de dados e sobre as razões de estarem a ser criado um perfil, bem como outras informações, como se há intervenção humana e qual seu papel ou se há indícios de discriminação no processamento de dados;[255] sobre a segurança dos dados, deve se estabelecer procedimentos em caso de avaria, erros ou inconsistências durante todo o ciclo de vida do sistema, assim como garantir uma avaliação crítica da qualidade, natureza representativa e quantidade dos dados utilizados, e, por último, deve se documentar o treinamento do modelo e realizar avaliações de impacto regulares abordando os riscos específicos da criação de perfis com base em sistemas de IA[256]; sobre as autoridades de supervisão, estas asseguram o cumprimento do direito interno, implementando os princípios enunciados nesta recomendação, sendo que quando a atividade de criação de perfis prevista for de alto risco, os Estados-Membros podem estipular que os responsáveis pelo tratamento

[251] *Ib.,* 12 - 14
[252] *Ib.,* 14.
[253] *Ib.*
[254] *Ib.,* 15
[255] *Ib.,* 5.
[256] *Ib.,* 7.

notifiquem a sua existência aos a autoridade de supervisão[257]; por último, nas medidas adicionais, fala-se da criação de perfis utilizada por autoridades públicas, exigindo que estas devem ser lícitas, proporcionais e necessárias face aos fins dessas operações.[258]

Consequentemente, podemos concluir que a Recomendação CM/Rec (2021)8 desempenha um papel crucial ao fornecer orientações claras e medidas de proteção para mitigar os danos do *profiling*. Ela aborda as possíveis violações de privacidade, discriminação e interferência na vida privada, restringindo o uso do *profiling* a categorias sensíveis de dados, a menos que permitido por lei, e enfatizando a necessidade de consentimento explícito e informado por parte dos titulares dos dados. A recomendação promove transparência, responsabilização e respeito aos direitos fundamentais na criação de perfis, visando proteger os indivíduos contra práticas prejudiciais.

Por fim, como último documento a ser analisado do CoE, iremos brevemente analisar o "*Zero Draft"* da Convenção sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito[259], elaborado pelo CAI e divulgado em 6 de janeiro de 2023. Esta convenção objetiva proteger os direitos fundamentais e humanos contra os danos causados pela IA e busca se tornar uma referência global, com países não europeus, como os Estados Unidos, considerando se tornar signatários.[260]

O documento Zero Draft estabelece que a Convenção-Quadro da AI deve ser aplicada em duas situações: na criação, desenvolvimento e aplicação de sistemas de IA que sejam utilizadas num contexto que envolva questões relacionadas com o respeito pelos direitos humanos e fundamentais, o funcionamento da democracia e a observância do estado de direitos; e, também, ao longo do ciclo de vida desses sistemas de IA, independentemente se tais atividades são realizadas por atores públicos ou privados - exclui-se deste escopo quando os sistemas de IA sejam utilizados para fins relacionados à defesa nacional[261]

---

[257] *Ib.,* 8.
[258] *Ib.,* 9.
[259] COUNCIL OF EUROPE - CoE. "REVISED ZERO DRAFT [FRAMEWORK] CONVENTION ON ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW", 2023.
[260] BERTUZZI, Luca. "US obtains exclusion of NGOs from drafting AI treaty", 2023.
[261] Artigo 4º do REVISED ZERO DRAFT.

A Convenção de IA, prevista para o final de 2023, existirá em paralelo e visa complementar o futuro Regulamento de IA da UE e outras iniciativas regulatórias. Enquanto este último centra-se na comercialização de produtos que utilizam IA no mercado interno da UE, a AI Convention centra-se na proteção dos direitos humanos e fundamentais das pessoas afetadas por sistemas de IA. A Convenção é baseada em princípios e introduzirá direitos humanos individuais juridicamente vinculativos, que também se aplicarão a cidadãos de estados não pertencentes à UE. O escopo exato da Convenção, no entanto, ainda está em discussão, com estados como os EUA, o Reino Unido e o Japão defendendo que ela permaneça limitada ao setor público.[262]

No que tange os princípios fundamentais elencados para a criação, os artigos 12º e 13º da Convenção têm implicações importantes para as tecnologias de reconhecimento facial. O Artigo 12º aborda o princípio da equidade e não discriminação, destacando a necessidade de garantir que os sistemas de IA, incluindo o reconhecimento facial, respeitem a igualdade, incluindo a igualdade de gênero e os direitos de grupos discriminados e indivíduos vulneráveis. Isso significa que as tecnologias de reconhecimento facial devem ser desenvolvidas e aplicadas de forma a evitar discriminação e tratamento desigual com base em características pessoais, protegendo os direitos de todos os indivíduos. O Artigo 13º aborda o princípio da privacidade e proteção de dados pessoais. Ele determina que cada parte deve garantir que a privacidade dos indivíduos seja protegida no projeto, desenvolvimento e aplicação dos sistemas de IA, incluindo o reconhecimento facial. Isso inclui a aplicação de leis e padrões nacionais e internacionais de proteção de dados pessoais e governança de dados. As partes devem garantir que as leis e princípios relevantes de proteção de dados sejam aplicados, e que sejam implementadas garantias e salvaguardas apropriadas para os titulares dos dados. Isso significa que as tecnologias de reconhecimento facial devem respeitar a privacidade das pessoas e garantir a proteção adequada de seus dados pessoais, seguindo as leis e princípios de proteção de dados em vigor.

Contudo, tais artigos podem e devem ser conjugados com os princípios de responsabilidade (todo Estado tomará medidas necessárias para garantir a responsabilidade legal

[262] VAN KOLFSCHOOTEN, Hannah. “The Council of Europe’s Artificial Intelligence Convention: Implications for Health and Patients”, 2023.

por qualquer dano aos DH e às liberdades fundamentais), transparência (todo Estado irá garantir mecanismos de supervisão adequados e requisitos de transparência e auditabilidade dos riscos inerentes aos sistemas) e de segurança (cada Estado irá garantir os requisitos adequados de segurança, proteção, qualidade, integridade dos dados em causa)[263] para uma abordagem abrangente na proteção dos sistemas de reconhecimento facial, promovendo sua utilização ética, justa e segura, em conformidade com os direitos fundamentais dos indivíduos.

Por último, mas não menos importante, segundo o artigo 24º da Convenção, os Estados signatários reservam-se o direito de impor uma moratória ou proibir certas aplicações de sistemas de inteligência artificial quando tais medidas forem consideradas apropriadas e necessárias pela autoridade nacional competente.

A Convenção deverá estar pronta em novembro de 2023, sendo que a próxima reunião para discuti-la será realizada em meados de setembro. Até lá congratula-se os esforços reunidos pelo CAI e pelo CoE, na elaboração de um instrumento jurídico que regule a IA tendo como principal objetivo a salvaguarda e o respeito absoluto pelos Direitos Humanos e Fundamentais.

## 4. QUADRO LEGISLATIVO DA UNIÃO EUROPEIA

O continente europeu foi preconizador na reflexão e atenção dada ao surgimento de novas tecnologias, em específico, a IA. Foi em abril de 2018 que a Comissão Europeia emitiu uma comunicação[264] intitulada "Inteligência artificial para a Europa", tomando os primeiros passos na conceptualização de alguns termos e estipulando um projeto para um quadro europeu sólido, através de uma abordagem coordenada, objetivando maximizar os benefícios trazidos pela IA, garantindo a criação de um quadro ético e jurídico apropriado para esta nova tecnologia, baseado nos valores da União. O documento afirmava que "a UE possui os ingredientes principais para assumir a liderança na revolução da IA" e que "Juntos, podemos colocar o poder da IA ao serviço do progresso humano".[265]

---

[263] Artigos 14º, 15º e 16º do REVISED ZERO DRAFT.
[264] COMISSÃO EUROPEIA. "Comunicação da Comissão: Inteligência artificial para a Europa {SWD(2018) 137 final}", Bruxelas, 2018.
[265] *Ib.,* 21.

Nesta lógica de abordagem, uma das 6 principais prioridades estabelecidas por Ursula Von Der Leyen da Comissão Europeia para 2019-2024 foi uma "*Europe fit for digital age*"[266]. Tal prioridade foca-se no desenvolvimento de uma estratégia digital de alto nível que coloca em primeiro plano a utilização de novas tecnologias para criar novas perspectivas para negócios, aumentar a segurança e fiabilidade na tecnologia e obter maior progresso na sociedade, visando colocar as novas tecnologias em benefício do bem social - produzir uma economia digital justa e competitiva com benefícios para empresas e pessoas, trazendo uma sociedade aberta, democrática e sustentável.[267]

Consequentemente, diversas iniciativas foram concretizadas, nomeadamente na concretização de *guidelines,* recomendações, no investimento na investigação destas tecnologias, instigando o debate público envolvendo diferentes atores, e ao pavimentar o percurso para uma regulação da IA que maximize os seus benefícios e mitigue os seus danos - sendo que a concretização máxima desta idealização se dará no Regulamento sobre Inteligência Artificial que irá ser votado pelo Parlamento Europeu em junho de 2023 (discutiremos sobre este a seguir).

No que diz respeito às tecnologias de reconhecimento facial, a legislação europeia ainda não fornece uma estrutura legal específica para estas[268]. Contudo, inúmeras normas existentes podem ser aplicadas, impondo requisitos, deveres e responsabilidades, especialmente aquelas que envolvam a privacidade e proteção de dados pessoais[269] e não discriminação. Será da conjugação dos diplomas existentes atualmente, da jurisprudência resultante dos Tribunais Europeus que poderemos analisar da legalidade do uso de TRFs para identificação de pessoas.

Começaremos este enquadramento jurídico analisando os instrumentos desenvolvidos pela UE no que diz respeito a IA no seu sentindo amplo para conseguir explorar a existência de certas previsões que, de certa forma, protejam os cidadãos europeus do uso indiscriminado das TRFs.

---

[266] VON DER LEYEN, Ursula. "A Union that strives for more: My agenda for Europe" in POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024, 2019.

[267] KOUROUPIS, Konstantinos. "Facial Recognition: a challenge for Europe or a threat to human rights?", 145.

[268] Tendo indo em vista que o AIA ainda não está em vigor e sim em fase de negociações.

[269] RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 2.

Em primeiro lugar podemos citar o documento concretizado pelo Grupo Independente de Peritos de Alto Nível sobre a IA (criado pela Comissão Europeia em 06/2018) denominado "Orientações éticas para uma IA de confiança" que teve como objetivo fornecer diretrizes para o desenvolvimento e implementação de sistemas de IA confiáveis e éticos na UE.

Podemos dizer que este documento teve a relevância de guiar o desenvolvimento de uma IA que se coadune com os princípios éticos de respeito da autonomia humana, prevenção de danos, equidade e explicabilidade, relevando a atenção que deveria ser dada aos grupos mais vulneráveis que podem ser afetados negativamente por estas tecnologias.

O documento também elencou que o desenvolvimento e a implantação de sistemas de IA teriam de satisfazer os requisito para uma IA de confiança, sendo eles: ação e supervisão humana; solidez, técnica e segurança; privacidade e governação dos dados; transparência; diversidade, não discriminação e equidade; bem-estar ambiental e societal; e responsabilização. A partir destes requisitos, o documento propõe uma lista de avaliação para conseguir detectar se tal sistema de IA está em conformidade com os requisitos elucidados.

No que diz respeito as TRF, esse documento colocou em relevo dois requisitos para a implantação de um sistema de IA que são de extrema importância para os desenvolvedores destas tecnologias: o da não discriminação e da proteção de dados. Contudo, tal instrumento foi ainda mais longe ao elencar, como exemplo de preocupações críticas suscitadas pela IA a "identificação de pessoas". Ela aponta que "A identificação automática suscita fortes preocupações de natureza ética e jurídica, uma vez que pode ter um impacto inesperado a muitos níveis psicológicos e socioculturais sendo necessário fazer uma utilização proporcionada das técnicas de controlo da IA para defender a autonomia dos cidadãos europeus." [270]

De forma ainda mais brilhante, as orientações sugerem que para se alcançar um sistema de confiança, será essencial definir-se quando e como ele pode ser utilizado na identificação automática das pessoas e distinguir a vigilância direcionada da vigilância em massa.[271] É de se louvar a percepção inicial deste grupo de peritos que tal distinção tem efeitos muito distintos e, por isso, devem ser tratados de forma diversa.

---

[270] COMISSÃO EUROPEIA. "Orientações éticas para uma IA de confiança", 2019, 43.
[271] *Ib.*

Logo em fevereiro de 2020, a Comissão Europeia divulgou o "Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para excelência e a confiança" visando definir opções política para alcançar o duplo objetivo estatuído: o de promover a adoção da IA e de abordar os riscos associados a determinadas utilizações desta tecnologia. Neste, a Comissão Europeia destaca de forma explícita que a IA deve se usada em conjunto com a legislação de direitos humanos, especialmente aquelas que abordem a proteção de dados e da privacidade. Relativamente as opções políticas abordadas, relevamos a que diz respeito a criação de um quadro regulamentar para a IA que reforce a confiança dos consumidores e das empresas na IA, acelerando a aceitação desta tecnologia ao promover a capacidade de inovação e competitividade da Europa neste domínio, sem descurar dos valores e princípios fundamentais que a sustentam (diz respeito ao Regulamento da IA que iremos analisar infra).

No que diz respeito ao reconhecimento facial e a outros processamentos biométricos, o documento propôs que, devido aos riscos fundamentais apresentados pelo uso dessa tecnologia, ela deveria ser automaticamente classificada como "alto risco", acarretando avaliações obrigatórias de conformidade. No entanto, o documento não abordou de forma adequada o impacto dessas aplicações consideradas "alto risco" nos direitos fundamentais. O EDRI acredita que "caso tivessem feito isso, acreditamos que a conclusão lógica seria a proibição das tecnologias de processamento biométrico para fins de vigilância em massa."[272]

Destarte, podemos elucidar que no âmbito do ordenamento jurídico da UE, as normas relativas à proteção de dados, privacidade e não discriminação, assim como o regulamento proposto sobre IA (iremos ver melhor infra), estabelecem critérios fundamentais para o desenvolvimento e uso das TRFs. Nesta lógica, é importante destacar que os direitos fundamentais à proteção de dados, privacidade e não discriminação[273] incorporam um conjunto de garantias essenciais no nível primário[274], conforme estabelecido na Carta dos Direitos Fundamentais. sendo que que qualquer limitação ao exercício dos direitos consagrados por ela,

[272] JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 18.

[273] A proteção de dados pessoais está prevista no artigo nº8; o respeito pela vida privada e familiar está previsto no artigo 7º; o direito a não discriminação está previsto no artigo 21º da Carta dos Direitos Fundamentais da União Europeia.

[274] EPRS, "Regulating facial recognition in the EU", 9.

deve ser previsto na lei, ser proporcional, necessária e responder a objetivos de interesse geral ou à necessidade de proteção dos direitos e liberdades de terceiros, conforme exposto no artigo 52º, nº1 da Carta.[275]

À vista disso, o EDRI[276] e o CDT[277] alegam que "*mass surveillance is pohibited in EU law"*[278]pelas graves violações de DF que se mostram inerentes a esta prática e que estão consagrados no Direito Primário da UE. Contudo, na prática, esses DFs ainda estão se concretizando e a extensão de suas aplicações ainda não estão claramente definidas, postulando uma dificuldade para que tais direitos forneçam uma orientação prática para o uso de TRF[279]. Sendo assim, iremos nos apoiar do direito derivado, ou seja, as fontes complementares[280], que apresentam um quadro exequível para a análise do porquê o uso de TRFs em sistemas de identificação biométrica em áreas públicas (o que pode levar a práticas de vigilância em massa) é incompatível com a legislação europeia - para tal, iremos fazer uma análise dos instrumentos que temos ao nosso dispor atualmente: a LED, e o RGPD.

Por conseguinte, uma vez que a utilização de TRFs implica o tratamento de dados para efeitos de (entre outros) identificação e que a sua utilização (principalmente, mas não só) pelas autoridades públicas constitui uma ingerência para os direitos citados supra, a LED, a RGPD, a jurisprudência dos Tribunais Europeus, dos tribunais domésticos e as opiniões das autoridades

---

[275] Sobre o âmbito de aplicação da Carta vale ressaltar que "
O artigo 51º da Carta veio tornar mais claro o âmbito de aplicação dos direitos fundamentais esclarecendo, no seu nº 1, que estes se aplicam às instituições e órgãos da União mas também aos Estados , "apenas quando apliquem" (implementing) o Direito da União, caso em que são agentes da União e, como tal, sujeitos aos mesmos constrangimentos. Neste ponto, há que salientar que, ao considerar os direitos fundamentais aplicáveis no âmbito dos "três pilares", a Carta foi para além do acquis communautaire jurisdicional, dado que o controlo do TJ não se estendia aos segundo e terceiro Pilares.
O inciso "apenas quando apliquem" pode legitimamente levantar a suspeita de um recuo face à jurisprudência do TJ, segundo a qual os Esta- dos devem respeitar os direitos fundamentais sempre que se esteja no campo de aplicação do direito comunitário — ou seja, não apenas quando estejam a aplicar ou dar execução estrita ao Direito Comunitário, mas também quando pretendam derrogar ou invocar uma excepção a essa aplicação." Cfr LEÃO, Anabela Costa. " A Carta dos Direitos Fundamentais da União Europeia: Protegendo os Direitos a um nível Multidimensional", 2006, 61.

[276] JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 12.

[277] CDT Europe, "Facial recognition briefing Paper: The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act", 2.

[278] A vigilância em massa é proíbida no Direito Europeu (Tradução livre).

[279] EPRS, "Regulating facial recognition in the EU", 10.

[280] EUR-LEX. "O direito primário da União Europeia".

de proteção de dados propõem albergar a regulação de todas as fases desta prática, nomeadamente: "a gravação de vídeo inicial, a retenção subsequente da filmagem e a comparação da filmagem com os registros do banco de dados para fins de identificação".[281] Se esses dados biométricos (imagens faciais) conseguirem ser sistematicamente e indiscriminadamente recolhidos, processados e retidos numa base de dados, nos encontraremos perante uma concepção geral de vigilância constante, que certamente não poderá ser tolerada.

Tanto a LED, quanto o RGPD se aplicam ao processamento automatizado de dados pessoais e ao processamento manual (contidos num ficheiro ou a ele destinados por meios não automatizado).[282]Contudo o âmbito de aplicação destes dois instrumentos diferem, sendo que a Diretiva refere-se ao tratamento de dados pelas autoridades competentes para prevenção, investigação, detecção ou repressão de infrações penais ou execução de penalidades criminais[283], reservando à RGPD o tratamento dos dados que não se incluam neste escopo.[284]

No artigo 3º da LED e 4º da RGPD, encontramos definições importante sobre termos relativos às TRFs - em relevo podemos considerar a "definição de perfis"[285] e os "dados biométricos"[286] que coincidem quase na sua totalidade. Posterior a isso, no artigo 4º da Diretiva e 5º do Regulamento, está consagrado os princípios relativos ao tratamento de dados pessoais impondo que o processamento de imagens faciais precisa ser "lícito, justo e transparente; seguir um propósito específico, explícito e legítimo (claramente definido no direito do EM ou da União); e, cumprir com os requisitos de minimização de dados, precisão de dados, limitação de armazenamento e responsabilidade"[287] sendo que o artigo 20º[288] da Diretiva e 25º do Regulamento impõe que os controladores e fabricantes de dados devam respeitar todos os princípios elencados na realização de suas atividades (o processamento de dados).

Relativamente aos princípios elencados nos artigos mencionados, iremos discriminá-los pela exigência de sua importância. Em primeiro lugar, temos a consagração do princípio da

[281] EPRS, "Regulating facial recognition in the EU", 16.
[282] Artigo 2º da LED e Artigo 2º nº1 da RGPD.
[283] Considerando nº11 e nº12 da LED.
[284] Artigo 2º nº1 al.d) da RGPD.
[285] 3º, nº4 da LED.
[286]3º, nº13 da LED.
[287] EPRS, "Regulating facial recognition in the EU", 10.
[288]Que se refere à proteção de dados desde a conceção e por defeito.

legalidade, impondo que para que o processamento de dados pessoais seja lícito ele tem que atender previsões legais específicas[289]. Nesta lógica, até conseguimos encontrar uma base legal para a vídeo vigilância na transposição nacional do artigo 8º da LED[290] e no artigo 6º da RGPD, contudo se esta for utilizada para o processamento de categorias especiais de dados (como são os dados biométricos processados pelas TRFs), deverá ser satisfeito os requisitos adicionais (e rigorosos) do artigo 10º da LED e 9º da RGPD.[291]

A esse propósito temos o exemplo de um caso alemão[292] no qual a autoridade de proteção de dados de Hamburgo considerou que a vídeo vigilância indiscriminada através de TRF em locais públicos, e a subsequente extração biométrica (formando modelos biométricos) e armazenamento desta em um banco de dados durante o *G20 Summit* de 2017, carecia de bases legais para tal, sendo solicitada a exclusão desta base de dados. Após isto, esta decisão foi anulada pela decisão judicial de um tribunal de primeira instância, o que levou a autoridade de proteção de dados de Hamburgo a argumentar no seu recurso que esta falta de base legal violava o artigo 8º, nº2 da Carta[293] e o artigo 4º, nº1, a) da LED e a sua respetiva transposição nacional, considerando que a extração biométrica de todos os rostos capturados nas extensas filmagens, mesmo que a grande maioria das pessoas em questão não estivesse envolvida em atividades criminosas, perturba drasticamente o equilíbrio entre o direito dos cidadãos à autodeterminação informativa e os poderes de aplicação da lei do estado.[294]

Contudo, diversos departamentos de polícias invocam códigos de processo penal, códigos de vigilância ou leis policiais como base legal para justificar o uso destas técnicas na manutenção da ordem pública e aplicação da lei.[295] Em um caso julgado no Reino Unido, o tribunal de apelação anulou uma decisão de primeira instância (entre outras razões), pois o

---

[289] Artigo 4ºnº1a) e Considerando 35 da LED; artigo 5ºnº1a) e Considerando 40 da RGPD.
[290] A Diretiva foi transposta em Portugal dando origem a Lei nº59/2019, de 8 de agosto: DADOS PESSOAIS PARA PREVENÇÃO, DETEÇÃO, INVESTIGAÇÃO OU REPRESSÃO DE INFRAÇÕES PENAIS
[291] Veremos detalhadamente a conjugação destes dois artigos para a permissão do processamento de dados biométricos infra.
[292] Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, Hamburg DPA, 31 de Agosto de 2018, 9-27.
[293] "Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei(...)."
[294]Antrag auf Zulassung der Berufung §§ 124, 124a VwGO, Hamburg DPA, 13 de março de 2020,. 5-6.
[295] EPRS, "Regulating facial recognition in the EU", 11.

quadro legal utilizado para justificar o uso de TRFs, não poderia ser qualificado como base legal, pois era impreciso e oferecia aos policiais alta arbitrariedade sobre quem poderia ser observado por tais tecnologias e onde elas poderiam ser utilizadas.[296]

Por conseguinte, encontramos nos mesmos artigos citados os princípios de transparência e de justeza. O primeiro diz respeito ao fato de "deve ser transparente para as pessoas físicas que os dados pessoais relativos a elas sejam coletados, usados, consultados ou processados e em que medida eles serão processados."[297] Esta transparência pode ser atingida através da divulgação das informações necessárias, por meio de um sinal de aviso, e os outros detalhes poderiam estar presentes em posters ou no site da autoridade.[298] Contudo, o artigo 13º, nº3 da LED impõe certas exceções a esta transparência quando estiver em causa investigações (que seriam atrapalhadas por este aviso), ou a segurança pública e nacional.[299]

No que diz respeito ao princípio da justeza, este exige que os dados pessoais não sejam processados de maneira injustificadamente prejudicial, ilegalmente discriminatória, inesperada ou enganosa para o titular de dados.[300] Alguns académicos sustentam que é justamente a partir desse princípio, que ainda não se encontra totalmente limitado, que propõe-se consagrar a discriminação algorítmica por meio de uma interpretação progressiva.[301]

Desta maneira, podemos avançar para o princípio da limitação da finalidade, que estipula que os dados pessoais só podem ser tratados para uma finalidade determinada, explícita e legítima,[302] sendo que o nº2 deste artigo expõe algumas exceções a este princípio. Nesta lógica e como as TRFs podem ter suas funções desvirtuadas, os sistemas que empregam esta tecnologia deverão ter salvaguardas suficientes para impedir a sua utilização para fins não autorizados.[303]

---

[296] Judgment in Case No. C1/2019/2670, Court of Appeal, 11 August 2020, paras. 90-96.

[297] Considerando 39 RGPD.

[298] CoE. "Guidelines on Facial Recognition", 2021. 11 - 12.

[299] Contudo, como isso impede os titulares de dados a exercer plenamente os seus direitos, deverá haver uma forte justificativa para explicar a necessidade de aplicar tal exceção, conforme ilustra JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 24.

[300] EDPB. "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", 2019, 17.

[301] EPRS, "Regulating facial recognition in the EU", 14.

[302] Artigo 4º, nº1, b) da LED e artigo 5º, nº1, b) do RGPD.

[303] EPRS, "Regulating facial recognition in the EU", 14.

Na alínea c) do nº1 do artigo 4º da LED e na mesma alínea e número do artigo 5º da RGPD , está previsto o princípio de minimização de dados, que impõe que a quantidade de dados em questão deva ser adequada, pertinente e limitada ao mínimo necessário para o propósito definido, sendo que o European Data Protection Supervisor, WOJCIECH WIEWIÓROWSKI já afirmou que "a conformidade da TRF com o princípio de minimização de dados é altamente duvidosa".[304]

Relativamente a estes dois princípios citados supra, importa mencionar uma decisão emitida pela Autoridade Sueca de Proteção de Dados que diz respeito a uma escola no norte da Suécia que utilizou um software de RF para monitorar a presença de alunos na escola. Perante esta prática, além de faltar uma base legal para o seu processamento violando o artigo 9º da RGPD, a Autoridade Sueca ainda argumentou que tendo o processamento ocorrido num ambiente cotidiano das crianças, revelou-se uma grave invasão da privacidade dos alunos, sendo que o objetivo de registrar a presença na escola poderia ser alcançado por medidas menos invasivas. Este uso foi considerado desproporcional ao propósito, violando os princípios de limitação de finalidade e minimização de dados.[305]

Passando ao princípio da exatidão/precisão dos dados previsto na alínea d) do nº1 do art. 4º da LED e 5º da RGPD, é exigido que tais dados sejam precisos e atualizados sempre que necessário, tomando-se medidas para que caso haja dados inexatos, estes sejam apagados ou retificados consoante as finalidades do tratamento. Este princípio é particularmente importante para as TRFs tendo em vista que dados imprecisos e inexatos podem levar a correspondências falsas. Sendo assim, os controladores destes dados "terão de evitar rotulagem incorreta, testando assim suficientemente seus sistemas e identificando e eliminando disparidades de precisão, principalmente no que diz respeito a variações demográficas de cor de pele, idade e sexo, e assim evitar discriminação não intencional."[306] Em consequência a isso, este princípio não exige

[304] WIEWIÓROWSKI, Wojciech. "Facial recognition: A solution in search of a problem?", 2019.

[305] Commission nationale de l'informatique et des libertés, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, 2019. In its Decision in Case N° 1901249 / Swedish Data Protection Authority 20 August 2019, DI-2019-2221.

[306] CoE. "Guidelines on Facial Recognition", 9.

apenas dados de entrada precisos, mas também que os algoritmos das TRFs fossem treinados em conjuntos de dados representativos e contivessem o mínimo possível de viés oculto.[307]

Na alínea e) do artigo 4º da LED e 5º da RGPD está previsto o princípio da limitação do armazenamento, que propõe que os dados não devem ser mantidos de uma forma que permita a identificação dos titulares dos dados, por mais tempo que o necessário para os fins nos quais tais dados serão tratados. Alguns órgãos de proteção de dados apontam que, para casos de detecção de vandalismo, 72 horas são suficientes para perceber se os dados capturados precisam ser armazenados por mais tempo, ou excluídos.[308] A EDPB propõe que "os controladores de dados devem garantir que os dados extraídos de uma imagem digital, para construir um modelo, não sejam excessivos e contenham apenas as informações necessárias para o propósito em específico, evitando processamentos adicionais."[309][310]

A última alínea do nº1 do artigo 4º da Diretiva e 5º do Regulamento prevê o relevante princípio denominado de segurança dos dados, impondo que o tratamento dos dados dever ser realizado de forma a garantir segurança adequada, incluindo proteção contra processamento e contra perda, destruição ou dano acidental, utilizando de medidas técnicas ou organizacionais.[311] O artigo 32º do RGPD e 29º da LED prescrevem que o controlador e processador devem implementar medidas técnicas e organizacionais proporcionais para evitar que os dados pessoais sejam divulgados ou acessados por pessoas ou órgãos não autorizados. O EDPB sugere que o controlador deve proteger adequadamente o sistema e os dados em todas as etapas do processamento, ou seja, durante o armazenamento, transmissão e processamento.[312]

Por último, temos previsto o princípio da responsabilidade no nº4 do artigo 4º da LED e no nº2 do artigo 5º da RGPD, que imputa ao controlador de dados a responsabilidade de demonstrar conformidade com os princípios demonstrados ao realizar o tratamento de dados

[307] EPRS, "Regulating facial recognition in the EU, 16.

[308] EPRS, "Regulating facial recognition in the EU, 15.

[309] EPDB. "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo", 10-11.

[310] Perante esse princípio, vale relevar o caso S. and Marper v UK no qual o TEDH concluiu que a retenção generalizada e indiscriminada de dados biométricos para fins de aplicação da lei em relação a pessoas não condenadas por um crime poder especialmente prejudicial no caso de crianças, dada a sua situação especial e a importância de seu desenvolvimento e integração na sociedade.

[311] A este respeito vale mencionar o artigo 29º da LED que será analisado ao pormenor infra.

[312]EPDB. "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo". 28-32.

pessoais, aplicando as medidas técnicas e organizativas adequadas para assegurar esta comprovação de conformidade.[313] Algumas medidas que podem ser tomadas estão explanadas na LED, como no artigo 27º e 28º (que veremos melhor infra), realizando o registro de atividades do processamento[314] ou até mesmo reportando as violações de dados[315].

Consequentemente a isso, cabe elucidar que qualquer órgão que cogite utilizar de TRFs necessita, impreterivelmente, estar em conformidade com os princípios elencados e também respeitar os artigos que iremos elucidar infra.

Sendo assim, podemos analisar que no artigo 6º da Diretiva estabelece-se distinções entre o tratamento de dados de, por exemplo, pessoas condenados ou suspeitos criminais (exigindo-se motivos fundados para crer que irão cometer uma infração penal)[316] em comparação com aqueles que não são condenados ou suspeitos de atividades criminosas. Segundo o EDRI, tal distinção releva pois demonstra uma diferença entre o uso da TRF de forma direcionada, que parece ser permitida pela LED, à suspeitos ou condenados, do uso das TRFs de forma não direcionada que parecer ser ilegítimo e ilegal por não se enquadrar nesta categoria de titulares de dados.[317]

No enquadramento da LED, relativamente ao tratamento de categorias especiais de dados pessoais, no qual se incluem os dados biométricos, está previsto no artigo 10º da LED que apenas será autorizado se "for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular de dados; a) se for autorizado pelo direito da União ou de um EM; b) se destinar proteger interesses vitais do titular dos dados ou de outras pessoas singular; c) se estiver relacionado com dados manifestamente tornados públicos pelo seu titular."[318] Este artigo deve ser interpretado em conjugação com o artigo 8º da diretiva que expõe

---

[313] Artigo 19º da LED.

[314] Artigo 24º da LED.

[315] Artigo 30º, nº5 da LED.

[316] Artigo 6º, al.a) da LED.

[317] JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 24.

[318] "O GT29 recomenda que se interprete o artigo 10º, alíneas b) e c), como ilustrando meramente situações específicas, em que o direito nacional previu tal tratamento. O artigo 10º, alínea b), ilustra uma situação em que os interesses vitais do respetivo titular dos dados exigem o tratamento de categorias especiais de dados. O artigo 10º alínea c), ilustra uma situação em que o próprio titular dos dados abdicou voluntariamente da proteção dos seus dados sensíveis ao torná-los públicos (sendo que aqui não pode ser considerado a postagem de fotos em mídias

que o tratamento de dados apenas é  lícito e necessário, tendo como base o direito da União ou de um EM - nota-se que o artigo 8º impõe o requisito da necessidade, enquanto o artigo 10º, por se tratar de dados mais sensíveis, obriga que o tratamento seja estritamente necessário, devendo ser criadas garantias adequadas.

Como dispõe o GT29, a diferença entre "necessário" (art. 8º) e "estritamente necessário" (art.10º), reside no fato de que este última deve ser entendida como uma chamada de atenção para o princípio da necessidade no contexto do tratamento das categorias especiais de dados, para prever justificações rigorosas e sólidas para o tratamento destes dados. Nesta senda, o GT29 recomenda que tal tratamento tenha o seu impacto sobre a proteção destes dados avaliado por autoridades competentes, comprovando se a finalidade do tratamento não poderia ser alcançada por um meio que afetasse menos os direitos e liberdades do titular de dados e se tal processamento não apresente um risco de discriminação para este indivíduo.[319]

Já no que diz respeito as garantias adequadas, o recital 33 da Diretiva dispõe que estas podem ser "por exemplo, a possibilidade de recolher esses dados apenas em ligação com outros dados sobre a pessoa singular em causa, afim de garantir devidamente a segurança dos dados recolhidos, o estabelecimento de regras mais rigorosas sobre o acesso do pessoal da autoridade competente aos dados ou a proibição de transmissão desses dados". Já o GT29 propõe outras garantias como: limitações adicionais à finalidade do tratamento e autorização prévia de um tribunal ou de outro órgão independente.[320]

No que diz respeito ao RGPD, a conjugação será feita entre os artigos 6º e 9º, sendo que antes de qualquer entidade realizar o processamento de dados pessoais, os controladores devem encontrar no artigo 6º da RGPD um fundamento legal e adequado para essa prática.[321] O artigo 9º precisa de ser considerado pois esta norma irá proibir o processamento de dados sensíveis (como os dados biométricos), a menos que a situação atenda alguma das situações estabelecidas no número 2 deste artigo.

---

sociais" Cfr. GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)", 2017, 8.

[319] GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)", 10.

[320] *Ib.,* 9.

[321] Conforme imposto pelo princípio da legalidade previsto no artigo 5º, nº1, a) da RGPD.

Neste sentido o RGPD difere da LED por permitir o processamento de dados pessoais especiais através do consentimento (9º, nº1, a)) explícito e para uma finalidade específica. A partir desta abordagem, o EDPB considera que "o uso de vigilância por vídeo, incluindo a funcionalidade de reconhecimento biométrico instalada por entidades privadas para os seus próprios fins (por exemplo marketing, estatística ou até mesmo segurança), exigirá, na maioria dos casos, o consentimento explícito de todos os titulares dos dados"[322]

Dentro do âmbito do artigo 9º do Regulamento, outra fundamentação jurídica frequentemente invocada no contexto da TRF é o parágrafo 2, alínea g), que autoriza o processamento de dados pessoais quando necessário por razões de interesse público substancial, com base na legislação da União ou dos EM que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados.

Desta forma, cabe revelar que tanto a LED quanto o RGPD encaram uma problemática que deriva do uso de TRFs, nomeadamente o *profiling.* No artigo 11º da diretiva está previsto o dever dos Estados-Membros de proibir, de forma geral, as decisões baseadas exclusivamente no tratamento automatizado, incluindo a definição de perfis, que produza um "efeito jurídico adverso"[323] para o titular dos dados ou o "afete significativamente"[324](o efeito deve ser suficientemente substancial para merecer atenção e influenciar o indivíduo)[325]. Contudo, como quase toda regra possui suas exceções, a derrogação a esta proibição só pode ter lugar aquando de uma autorização da União ou de um EM prevendo garantias adequadas dos direitos e liberdades do titular dos dados, pelo menos o "direito de obter a intervenção humana do responsável pelo tratamento"[326]. Todavia, e como expõe o número 2 deste artigo, tal exceção

[322] EPDB. "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo", 18.

[323] Ilustrando o exemplo inserido em GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)",14: "Aplicação de medidas de segurança reforçadas ou de vigilância pelas autoridades competentes."

[324] Ilustrando o exemplo inserido em GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)",14: "o caso em que não é autorizada a entrada de um passageiro a bordo pelo facto de este estar registado numa lista proibida."

[325]GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)",14.

[326] Cfr. o considerando 38 da LED: "em especial, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação ou de contestar a decisão."

apenas se aplica a categoria comum de dados pessoais, excluindo os dados biométricos que objetivam identificar uma pessoa singular, só podendo o fazê-lo se estiverem em vigor medidas adequadas para a salvaguarda dos direitos e liberdades da pessoa em causa, e os interesses legítimos desta.[327] Por último, o artigo 11º ainda proíbe a prática de *profiling* que conduzam à discriminação de pessoas singulares com base na categoria dos dados pessoais referidos no artigo 10º.

Já o RGPD dispõe, no seu artigo 22º, que, em regra, existe uma proibição geral das decisões individuais totalmente automatizadas, incluindo a definição de perfis com efeitos jurídicos ou similarmente significativos. Contudo, há exceções a essa regra, que sempre que aplicadas impõe-se a existência de medidas para salvaguardar os direitos e liberdades e os legítimos interesses do titular de dados.

O 3º capítulo da LED e do RGPD[328] se concentra nos direitos do titular de dados possuem em relação ao processamento dos seus dados pessoais. Sendo assim, dada a natureza do processamento destes dados por meio de TRFs o controlador deve considerar cuidadosamente como (ou se pode) atender os requisitos da LED (e da RGPD) antes de qualquer processamento através destas tecnologias. Deverão analisar: quem são os titulares dos dados (muitas vezes mais do que o(s) principal(is) alvo(s) para efeitos do tratamento); como os titulares dos dados são informados sobre o processamento FRT; e, como os titulares dos dados podem exercer seus direitos.[329]

O primeiro direito destacado na Diretiva, e que possui grande relevância para o uso de TRF, está previsto no artigo 13º da LED , que se reporta ao direito à informação, imputando ao

---

[327] Cfr. GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)", 15: "Devido à natureza especial dos dados e aos óbvios riscos de discriminação decorrentes das decisões automatizadas assentes nesses dados, é particularmente importante que os Estados-Membros, ao aplicarem a diretiva, prevejam garantias estritas para proteger os direitos dos indivíduos."

[328] Iremos nos focar numa análise mais detalhada dos direitos conferidos pela LED, por se coadunar melhor com os direitos que os indivíduos possuem perante o uso de TRFs pelas autoridades públicas objetivando a identificação de suspeitos ao não cumprimento da lei. Contudo, a RGPD impõe os seguintes direitos: Direito a informação (Arts. 12º, 13º e 14º); Direito de acesso e de portabilidade dos dados (Art. 15º); Direito de oposição ao processamento dos dados (Art. 21º); Direito à retificação/correção dos dados (Art. 16º); Direito a ser esquecido (Art. 17º) que podem ser consultados detalhadamente em: https://gdpr-text.com/pt/ e também em https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm

[329] EDPB. "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", 2022, 21.

responsável pelo tratamento de dados, uma "obrigação ativa"[330] de fornecer certas informações aos titulares de dados. O nº1 do artigo impõe que algumas informações, como a identidade e os contatos do responsável pelo tratamento, são obrigadas a serem fornecidas - "por meio do site do responsável ou em formato impresso como em folhetos"[331]. Já o nº2 propõe que em casos específicos (como no processamento de TRFs[332]) poderá ser necessário fornecer informações adicionais como: o fundamento jurídico do tratamento e o prazo de conservação dos dados para definição daquele período. Por fim, é importante mencionar que, de acordo com o nº3, os EM têm a possibilidade de adotar medidas legislativas que restrinjam a obrigação de fornecer informações em casos específicos, para determinados fins. Essas restrições são aplicáveis desde que sejam necessárias e proporcionais em uma sociedade democrática, com pleno respeito aos direitos fundamentais e aos interesses legítimos do titular dos dados.

O artigo 14º da diretiva estabelece o direito geral do titular dos dados de acessar seus dados pessoais, o que implica o direito de obter diretamente, do responsável pelo tratamento, uma confirmação positiva ou negativa sobre o processamento de seus dados pessoais (também conhecido como direito de "acesso direto" pelo titular dos dados). Em caso de confirmação positiva, inclui-se o acesso aos dados pessoais e a determinadas informações específicas.[333][334]Contudo, o artigo 15º impõe limitações ao direito de acesso para os fins indicados neste artigo (proteger segurança pública, evitar prejudicar investigações, entre outros), tendo o titular dos dados o direito de ser informado desta limitação, podendo reclamar a uma autoridade sobre esta prática.

O artigo 16º da Diretiva diz respeito ao direito de retificação ou apagamento dos dados pessoais e limitação do tratamento. Isso releva uma vez que as TRFs não preveem uma precisão absoluta, conferindo aos titulares de dados solicitarem uma retificação dos dados pessoais.

---

[330] GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)", 18.

[331] EDPB. "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", 21.

[332] Conforme elucidada no Considerando 38 da LED.

[333] Conforme proposto no Artigo 14º da LED "Com as finalidades e o fundamento jurídico do tratamento, as categorias dos dados pessoais em causa, os destinatários aos quais os dados pessoais foram divulgados, entre outros"

[334] GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)", 18.

Também é concedido aos titulares a possibilidade de exigirem o apagamento de seus dados pessoais, caso infrinja-se os princípios e a licitude do tratamento desses dados.

Tendo se estabelecido os direitos dos titulares de dados, ainda releva mencionar outros artigos elencados na LED que se coadunam com o foco desta investigação. Em primeiro lugar podemos citar o artigo 27º que exige que seja realizado uma avaliação de impacto das operações de tratamento de dados pessoais realizadas, quando desta prática exista um elevado risco para os direitos e liberdades dos indivíduos, como é o caso das TRFs. Esta avaliação deve conter uma descrição geral das operações de tratamento previstas, uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, as medidas previstas para lidar com esses riscos, salvaguardas, medidas de segurança e mecanismos para garantir a proteção de dados pessoais e demonstrar conformidade. Já nos termos do artigo 28.º da LED, o responsável pelo tratamento ou subcontratante deve consultar a autoridade de controlo antes do tratamento, sempre que: (a) uma avaliação do impacto na proteção de dados indique que o tratamento resultaria num risco elevado na ausência de medidas tomadas pelo responsável pelo tratamento para mitigar o risco; ou (b) o tipo de tratamento, em particular, quando a utilização de novas tecnologias, mecanismos ou procedimentos envolve um risco elevado para os direitos e liberdades dos titulares dos dados. Ou seja, a autoridade que implante a TRF deve realizar uma avaliação de impacto para a proteção de dados pessoais e também consultar uma autoridade supervisora competente antes da implantação do sistema.

Considerando a natureza única dos dados biométricos, torna-se impossível para o titular dos dados modificá-los em caso de comprometimento decorrente de uma violação de dados. Por isso, é de suma importância que a autoridade competente responsável pela implementação e/ou utilização do TRF dedique especial atenção à segurança do tratamento, conforme previsto no artigo 29º da LED. Em especial, a autoridade encarregada da aplicação da lei deve assegurar a conformidade do sistema com as normas pertinentes e adotar medidas de proteção para os modelos biométricos. Essa obrigação assume ainda mais importância se a autoridade policial estiver utilizando um provedor de serviços terceirizado (processador de dados).[335]

[335] EDPB. "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement", 24.

A partir da análise jurídica europeia exposta, podemos concordar com o EDRI e com o CDT, quando afirmam que a prática de vigilância em massa é proibida na Europa. Por mais que a maioria das cidades europeias utilizem de câmeras de CCTV para a manutenção da ordem pública[336], tais câmeras não podem (legalmente) captar a imagem facial de todos indivíduos que por elas passam, a fim de processar esses dados biométricos para construir uma base de dados com os rostos de todos os cidadãos, ou para fins de identificação de pessoas de forma deliberada e indiscriminada. Tal prática, constitui interferências graves com o direito ao respeito pela vida privada à proteção de dados pessoais.

Contudo as TRFs não se restringem apenas ao uso em câmeras de vigilância com o objetivo de realizar uma vigilância em massa de todos os cidadãos. Essas tecnologias têm a capacidade de serem empregadas para diversos propósitos e podem ser utilizadas de maneiras diversas - em tempo real ou em diferido, de forma direcionada ou indiscriminada, apenas para criação de base dados, ou apenas para efeitos de identificação através de comparação, para análise comportamental, para a criação de perfis, para monitoramento de atividades suspeitas, para analisar o fluxo de pessoas ou até mesmo para monitorar as emoções das pessoas. Essas diversas modalidades de uso do reconhecimento facial apresentam diferentes implicações em termos de privacidade e de proteção de dados, necessitando-se aferir da sua legalidade diantes dos diversos diplomas que temos para a matéria.

No que diz respeito ao Direito primário, e dado que o processamento dos dados biométricos constitui uma limitação dos direitos citados supra, o artigo 52º, nº1 da Carta propõe que qualquer restrição a DFs tem de ser submetida ao rigoroso "teste da necessidade e proporcionalidade", incluindo uma base legal clara para fazê-lo e um objetivo legítimo para ser concretizado, sendo que tanto a sensibilidade dos dados ou a maneira como estes dados são usados são importante para o contexto.[337]

Caso o processamento de dados biométricos passe pelo crivo da proporcionalidade e necessidade, ele necessitaria de respeitar, impreterivelmente, os princípios previstos na LED e

[336] MANNING, Jake. "The Story of CCTV in Europe, from resistance to adoption", 2021.

[337] JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", 24.

no RGPD, ou seja, o processamento teria de ser: justo, legal, transparente, seguir um propósito específico, explícito e legítimo previsto pelos EM ou pela União, e cumprir os requisitos de minimização de dados, precisão de dados, limitação de armazenamento, segurança de dados e responsabilidade.

Diante da ausência de uma regulamentação jurídica específica voltada exclusivamente para as várias técnicas de vigilância empregadas, é possível inferir que o processamento de dados biométricos obtidos por meio de câmeras de vigilância e tratados por tecnologias avançadas de RF está sujeito a várias restrições impostas por diferentes instrumentos legislativos, dependendo do objetivo do seu uso, porém, não é inteiramente proibido.

Consequentemente, vale a pena considerar o famoso caso "Bridges vs. The Chief Constable of South Wales Police"[338] que envolveu o uso de TRF pela polícia do País de Gales, no Reino Unido. Esta realizou um projeto piloto de TRF em vários locais e eventos públicos, como jogos de futebol, a partir de 2017. No entanto, em 2019, um habitante de Cardiff chamado Ed Bridges apresentou uma queixa no tribunal alegando que a captação de imagens faciais constituiu violação de direito à privacidade previsto no Artigo 8º da CEDH.

Inicialmente, a queixa foi arquivada em primeira instância, alegando-se que o uso do software de reconhecimento facial foi proporcional.[339] Posteriormente, o tribunal de apelação, a partir de uma análise de conformidade do uso de TRFs pela polícia em locais públicos e em tempo real com a LED e a legislação nacional inglesa, decidiu a favor de Bridges. O tribunal considerou que as políticas relevantes que regulamentavam as TRFs "não possuíam a qualidade necessária de lei"[340], sendo que o seu uso não tinha uma base legal para tal, frustrando o princípio da legalidade.

O tribunal ainda declarou que os policiais não devem ter muita arbitrariedade ao decidir quem visar para vigilância, ou seja, quem pode ser colocado em uma lista de observação e

[338]Case: Bridges vs. The Chief Constable of South Wales Police (Appeal Court) de 11 de agosto de 2020 (Disponível em: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf)

[339] LIBERTY HUMAN RIGHTS. "Legal Challenge: Ed Bridges v. South Wales Police, 2020.

[340] Case: Bridges vs. The Chief Constable of South Wales Police (Court of Appeal of London ) de 11 de agosto de 2020, § 86.

comparado com uma imagem de amostra (questão de "quem"), ou a localização em espaços públicos onde as TRFs podem ser implantadas (questão de "onde").[341]

Conforme o próprio Ed Bridges propôs "A tecnologia é uma forma intrusiva e discriminatória de fazer vigilância em massa… Devíamos poder usar espaços públicos sem estar sujeitos a vigilância opressiva"[342]. Sendo assim, essa decisão conseguiu restringir a definição do que é aceitável no emprego de tecnologias de reconhecimento facial, determinando a relevância de uma base legal, e restringindo a arbitrariedade das autoridades policiais no emprego desta tecnologia.

## 5. UMA ANÁLISE TRANSNACIONAL DAS APLICAÇÕES DE TECNOLOGIAS DE RECONHECIMENTO FACIAL

A partir do exposto, é relevante realizar uma análise transnacional das aplicações de TRFs, explorando como diferentes países têm adotado e implementado essas ferramentas inovadoras, compreendendo as abordagens e regulamentações existentes em relação ao uso destas tecnologias em diferentes contextos nacionais. Para tal, examinaremos os exemplos concreto do uso de TRFs, as políticas governamentais e marcos jurídicos e éticos. Além disso, buscaremos identificar as principais tendências, desafios e impactos sociais decorrentes do uso dessas tecnologias em âmbito transnacional.

A partir de tal, poderemos obter perspectivas valiosos sobre as abordagens adotadas por diferentes países e entender melhor como os aspectos culturais, jurídicos e sociais influenciam a implementação e aceitação desta tecnologia. Essas informações podem fornecer subsídios para aprimorar as políticas públicas, regulamentações e práticas relacionadas a essas tecnologias em escala global..

Nesse contexto, é possível afirmar de maneira clara que o cenário orwelliano, anteriormente limitado à ficção, está progressivamente se tornando realidade. O aumento do uso de sistemas de reconhecimento facial por autoridades policiais, com alegações de interesse

[341] MOBILIO, Giuseppe. "Your face is not new to me - Regulating the surveillance power of facial recognition", 2023, 9.
[342] LIBERTY HUMAN RIGHTS. "Liberty wins ground-breaking victory against facial recognition tech", 2020.

público, juntamente com a recente legislação francesa que legalizou, pela primeira vez na história da UE, a vigilância por vídeo baseada em algoritmos, evidencia a necessidade urgente de uma regulamentação uniforme para os países europeus. Essa regulamentação deve considerar os riscos intrínsecos (já demonstrados) ao uso de sistemas de reconhecimento facial, assim como limitar o seu uso, sua extensão e suas finalidades.

Em Portugal, no dia 6 de novembro de 2021, o Governo Português introduziu na AR a Proposta de Lei 111/XIV/2[343] relativa à autorização e utilização de sistemas de vídeovigilância pelas forças e serviços de segurança, que se tivesse sido aceita nos moldes que foi primariamente formulada, iria dar o título a Portugal do primeiro país a legalizar o uso de TRFs em câmeras de vigilância públicas.

Julgamos que a proposta de lei seria inconstitucional por: retirar a excepcionalidade da utilização da vídeo vigilância, alargando os fins que justificariam a sua utilização, como no artigo 3º d), que propõe que o uso poderia ser autorizado para proteção de pessoas, animais e bens, em locais públicos, quando houvesse uma elevada circulação ou concentração de pessoas (ou seja, em cidades como Porto e Lisboa tal prática seria a regra); no seu artigo 18º nº2 a proposta permitia a captação de dados biométricos e o tratamento destes dados, ou seja, permitia a introdução de TRFs nas câmeras de vigilâncias instaladas; e, também constrangia excessivamente a atuação da CNPD, retirando-lhe competências.

A proposta em causa foi alvo de uma enorme preocupação por parte dos partidos políticos e da CNPD, que concretizou um parecer evidenciando as preocupações elencadas supra. Após uma semana da introdução da proposta pelo Governo, o Partido Socialista apresentou na AR um texto de substituição àquela que mais se adequava com o parecer da CNPD, restringindo alguns aspectos da mesma, como as suas finalidades, e, com grande relevância, a possibilidade de ser realizado a captação de dados biométricos.

Contudo, segundo o artigo 15º da proposta, será possível captar imagens e sons, e proceder a gravação de câmeras fixas ou portáteis quando os sistemas de vídeovigilância tiverem sendo usados para: apoio à atividade operacional das forças e serviços de segurança em

[343]Proposta de Lei 111/XIV/2 de 6 de novembro de 2021 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=121083 Acessado em 23 de abril de 2023.

operações policiais complexas, como em eventos de grande dimensão ou de outras operações de elevado risco ou ameaça, prevenção de atos terroristas, resposta operacional e incidentes de segurança em curso, e para o apoio em operações externas de busca e salvamento.

Após algumas alterações terem sido realizadas[344], a proposta foi aprovada com votos a favor do PS, PSD, CDS-PP e PAN. Votaram contra o BE, o PCP, a IL, PEV e 4 deputados do PS. Justificando os votos contras por razões de extensão da vídeovigilância permitida, o deputado António Filipe expôs: "O texto aprovado visa legitimar o uso da videovigilância para uma imensidão desproporcionada de finalidades utilizáveis por múltiplas entidades, sem que estejam previstas medidas suficientes de salvaguarda quanto ao seu uso indevido e mesmo no que se refere à utilização de câmaras portáteis de uso individual pelas forças de segurança são adotadas formulações de tal modo equívocas que serão mais os problemas criados do que os que alegadamente se visa resolver."[345]

Contudo, para efeitos de emissão de certificados qualificados, o GNS, através de um Despacho em março de 2021[346], permitiu a identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial. Ou seja, o uso destas tecnologias já ocorre em solo português, contudo, é restrito a uma pequena prática e impondo certos requisitos para garantir a segurança do processo, como avaliações de riscos, auditorias de controlo, análise periódica de performance, a necessidade de um consentimento explícito para tal e afins.

Dentro do âmbito europeu, um local que tem sido alvo de uma implantação massiva de TRFs são os estádios de futebol. Na Dinamarca, a TRF é usada para verificação de bilhetes no Estádio Brøndby, sendo que o fornecedor afirma que o sistema Panasonic FacePro pode reconhecer pessoas mesmo que estejam usando óculos escuros. O uso dessa tecnologia foi justificado para a garantia de que torcedores banidos e pessoas conhecidas como "risco de segurança" sejam mantidas fora do estádio.[347] Na França, um clube de futebol que não teve seu nome divulgado, foi alertado pela CNIL sobre a ilegalidade do uso de TRFs, na ausência de um

[344] Texto Final e relatório da discussão e votação na especialidade da Proposta de Lei n.º 111/XIV/2ª (GOV).
[345] PARTIDO COMUNISTA PORTUGUÊS. "Declaração de voto sobre a Proposta de Lei n.º 111/XIV sobre videovigilância", 2021.
[346] GABINETE NACIONAL DE SEGURANÇA. "Despacho n.º 2705/2021", 2021.
[347] BILLINGTON, James. "Panasonic facial recognition in use at Brøndby Stadium", 2019.

texto legislativo específico ou de uma disposição regulamentar. O time utilizou da mesma justificativa da equipa dinamarquesa adicionando ainda o combate ao terrorismo.[348] O vitorioso time holandês AJAX, utiliza do software *MITEK*, para realizar a verificação digital da identidade dos compradores de ingresso online. Tal prática propõe estar em conformidade com a RGDP e objetiva uma melhor experiência online dos adeptos do clube.[349]Um exemplo ainda mais grave ocorreu na final da *Champions League* de 2017 no País de Gales, quando as autoridades policiais decidiram utilizar de TRFs para detectar possíveis criminosos, sendo que dos 2.470 possíveis *matches* com a base de dados, 2.297 estavam incorretas.[350]

O último caso é ainda mais preocupante, por ter sido realizado por autoridades públicas e não entes privados. Essa não foi a última vez que os País de Gales utilizaram de tais tecnologias, tendo um exemplo recente acontecido no show da Beyonce que ocorreu em Cardiff em maio de 2023. O uso foi justificado para a procura de crimes prioritários.[351]

Segundo a "Reclaim your face" "a cultura dos fãs está ameaçada porque a vigilância em massa pode ser implantada para controlar ou dissuadir muitos dos elementos centrais que reúnem as pessoas em shows e estádios. Com certeza, a vigilância biométrica em massa pode criar um "efeito intimidador" nos indivíduos. Saber que está sendo monitorado pode fazer com que as pessoas se sintam desencorajadas a participar legitimamente de encontros prévios aos shows, jogos, marchas de fãs, ou a se juntarem a um protesto."[352]

O uso de TRFs por entes privados, que impõe o processamento de dados biométricos, que estão dentro da categoria de dados faciais, tem de estar em conformidade com a RGPD para poder ser feito de forma legal. Contudo, as exceções consagradas no artigo 9º, nº2 do regulamento que permitam que esse processamento seja realizado, geralmente não conseguem ser justificadas pelas empresas.

---

[348] REUTERS STAFF. "French watchdog warns sports club about unlawful use of facial recognition technology", 2021.
[349] PASCU, Luana. "Football club Ajax Amsterdam deploys Mitek biometrics to improve online experience, privacy", 2019.
[350] BBC NEWS STAFF. "2,000 wrongly matched with possible criminals at Champions League", 2018.
[351] EXPRESSO STAFF. "Polícia do País de Gales criticada por recorrer a reconhecimento facial em concerto de Beyoncé", 2023.
[352] RECLAIMYOURFACE. "Football fans are being targeted by biometric mass surveillance", 2022.

Esse foi o caso da universidade particular Luigi Bocconi, e da cadeia de supermercados denominada Mercadona. No primeiro exemplo, a universidade adotou um software chamado "Respondus" sem informar de forma adequada os seus estudantes. Este software, utilizado para exames online, permitia a verificação de que a pessoa que está em frente da tela é aquela que deveria estar a realizar o exame (para evitar que outra pessoa substitua o estudante na realização deste). A partir disso, os dados biométricos dos estudantes que realizaram estes exames foram coletados, sendo que após o processamento destes dados, o professor recebia um relatório mostrando a imagem dos alunos para fins de identificações posteriores. A Autoridade Italiana de Proteção de Dados multou a universidade em 200.000 euros, alegando não existir disposição legal que autorize expressamente o processamento de dados biométricos com o objetivo de verificar a regularidades dos exames, e que o consentimento não poderia constituir base legal pela desigualdade de posição dos estudantes perante a faculdade.[353]

Já o caso do Mercadona, utilizou-se de SRF, objetivando detectar pessoas com condenações criminais ou ordens de restrição, sendo que o processamento de dados biométricos ocorreu a qualquer pessoa que entrasse no estabelecimento, inclusivamente crianças e funcionários. Perante essa prática, a Autoridade Espanhola de Proteção de Dados impôs uma multa de €2.520.000 à Mercado S.A., ao concluir que esse processamento não se coadunava com as exceções do artigo 9º nº2 da RGPD, sendo ilegal, contrária aos princípios de necessidade, proporcionalidade e minimização de dados nos termo do 5º artigo do regulamento, e, ainda violou os requisitos de transparência dos artigos 12º e 15º.[354]

No que diz respeito ao uso destas tecnologias pelo setor público, já citámos anteriormente o caso da cidade de Hamburgo na Alemanha e na Suécia, em que ambas utilizações foram consideradas ilegais. Contudo, dentro da União Europeia temos alguns casos de desenvolvimento desta tecnologia que, desde logo, sinalizam algumas preocupações.

Primeiramente, podemos mencionar o caso húngaro de implementação do "The Dragonfly Project", que tem como objetivo criar uma base de dados governamental. Essa base de dados é alimentada por informações coletadas de espaços públicos, como parques, ruas e praças. O projeto recebeu um investimento de 160 milhões de euros e pretende instalar cerca de

[353] RECLAIMYOURFACE. "No biometric surveillance for Italian students during exams", 2021.
[354] AEDP. "Procedimiento No: PS/00120/2021", 2021.

35.000 câmeras de circuito fechado de televisão (CCTV) e 25.000 terabytes de armazenamento para os dados coletados em todo o território húngaro.[355]

O país já utiliza tecnologias de reconhecimento facial para buscar crianças desaparecidas e localizar pessoas com mandados de prisão. No entanto, o desenvolvimento desse projeto tem levantado muitas preocupações entre as autoridades de proteção de dados e os cidadãos. Eles apontam a falta de base legal que justifique a implementação de um projeto desse tipo e expressam preocupação com relação à privacidade e aos direitos individuais dos cidadãos.[356]

A Itália decidiu, em novembro de 2022, banir o uso das TRF depois de sérios riscos levantados pela autoridade de proteção de dados italiana. Esta alegou que o uso será banido até que existe uma lei que regule o processamento de dados biométricos. Contudo, como quase toda regra possui sua exceção, o uso de TRF foi liberado quando estas tecnologias tenham um papel importante em investigações judiciais ou no combate ao crime.[357]

Os nossos vizinhos espanhóis decidiram, em junho de 2020, instalar câmeras de reconhecimento facial na entrada de estádios, salas de concertos e grandes locais por toda a Espanha, objetivando ter de reduzir o número de policiais necessários em ocasiões que movimentem um grande público. Os sistemas de reconhecimento facial também serão instalados em áreas rurais para compensar a falta de policiais disponíveis nessas regiões.[358]

A Grécia emitiu, em 2020, o Decreto Presidencial 75/2020, que muito se assemelha com a nova lei de videovigilância portuguesa, sobre a autorização a instalações de sistemas de vigilância que capturam e gravam áudios e vídeos em locais públicos. Os fundamentos para uso destes sistemas incluem a prevenção de atos criminosos e para o gerenciamento do tráfego.[359]

O exemplo francês de vigilância em massa mostrou-se o mais expressivo e preocupante de todos os casos dentro da UE. O parlamento francês adotou a Lei da Organização dos Jogos

---

355 THE GREENS/EFA. "Biometric & Behavioural Mass Surveillance in EU Member States", 2021, 100.

356 *Ib.*

357 MACCIONI, Elvira. "Italy outlaws facial recognition tech, except to fight crime", 2022.

358 MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRATICA. "Resolución de 16 de julio de 2020, de la Subsecretaría, por la que se publica el Convenio entre el Centro para el Desarrollo Tecnológico Industrial, E.P.E., y el Ministerio del Interior, relativo a la contratación precomercial de servicios de I+D en materia de seguridad en el medio rural", 2020.

359 KORONAIOS, Aimilios. "CCTV in public spaces: What changes does the new Presidential Decree bring?", 2020.

Olímpicos, que permite, através do seu artigo 7º, a introdução de Vigilância por Vídeo Algorítmica até 2024, apoiada pelo partido governista e por partidos da extrema direita. O governo relatou que tal lei não está relacionada à biometria, por mais que está tecnologia tenha a possibilidade de identificar, analisar e classificar corpos, atributos físicos, gestos e formas corporais, o que pela legislação europeia é considerado dados biométricos.[360]

O governo utilizou-se do pretexto dos Jogos Olímpicos para permitir a introdução desta tecnologia, justificando que sua principal aplicação será a de identificar comportamentos previamente definidos como "suspeitos" pela polícia, sem explicar concretamente o que poderiam enquadrar comportamentos suspeitos, ou o porquê das câmeras de vigilância (que já são inúmeras em território francês) precisarem da incorporação da IA para tal.[361]

Tal legalização pode criar um precedente histórico dentro da UE e também tem a possibilidade de abrir portas para outras tecnologias de vigilância biométrica. Conforme expõe o "Reclaim Your Face": "Táticas como essas, que permitem ao Estado transformar a realidade de suas prerrogativas de vigilância, devem ser denunciadas. Especialmente em um contexto onde o significado das palavras é deliberadamente distorcido para fazer as pessoas acreditarem que "vigilância é proteção", "segurança é liberdade" e "democracia significa forçá-los a aceitar".

O exemplo francês poderia ser mais facilmente aceite em países nos quais as TRF são a realidade, como no caso do Brasil, Estados Unidos ou China. Contudo, o fato da UE possuir legislações relativas a proteção de dados, circunscreve (ainda que não na medida necessária) as possibilidades do uso de tecnologias de vigilância que são altamente intrusivas à privacidade.

No caso do Brasil, o Instituto Igarapé divulgou um relatório em 2019 demonstrando que havia 47 casos de implementação de TRF em câmeras de vigilância por autoridades públicas e seus parceiros no setor privado desde 2011. A utilização destas está aliada ao auxílio da preservação da segurança pública, do combate as fraudes no transporte público e ao controle de fronteiras.[362]

---

[360] VALENTINA. "France becomes the first European country to legalise biometric surveillance", 2023.

[361] LA QUADRATURE DU NET. "Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée", 2023.

[362] INSTITUTO GARAPÉ. "Reconhecimento facial no Brasil: Desde 2011 vem sendo utilizado o Reconhecimento Facial no Brasil", 2022.

O uso de tais tecnologias ganhou uma maior expressão quando o então Ministro da Justiça e Segurança Pública de Jair Bolsonaro, Sérgio Moro, emitiu uma portaria que incentivava a adoção destas. O projeto-piloto batizado de "Em Frente Brasil" permitiu que municípios se voluntariasse para realizar experimentos para embasar a criação de um programa nacional voltado à investigação de crimes violentos - até 2020 cinco municípios receberam 44 milhões de reais do projeto.[363]

Em 2021, em um estudo divulgado pela LAPIN, foi identificado um denominador comum no uso destas tecnologias: a falta de transparência e de mecanismos garantidores de proteção de dados e segurança na implementação das tecnologias no Brasil. Também foi pontuado que a inexistência de legislação específica aponta para uma margem de discricionariedade no uso dessas tecnologias por parte dos gestores.[364]

Existe um projeto de lei correndo na câmera de deputados brasileira, de autoria do Subtenente Gonzaga do Partido Social Semocrático que procura regular o uso de TRF pelas forças de segurança pública em investigações criminais ou procedimentos administrativos. A tecnologia, de acordo com o projeto, poderá ser utilizada diante da necessidade de identificar autores, coautores, testemunhas ou vítimas relacionadas a algum fato criminoso, ou ainda, na área cível, para auxiliar as forças de segurança na busca por pessoas desaparecidas.[365]Ou seja a lei iria legalizar o uso de tais tecnologias para um âmbito alargado de situações e iria contrariar a posição de governos brasileiros que pretender banir ou declarar moratória no uso destas tecnologias.

Em maio de 2023, o Ministério Público de São Paulo instaurou um inquérito civil para investigar possíveis violações de direitos humanos no programa Smart Sampa, que previa a integração de 20 mil câmeras integradas com TRF em São Paulo até 2024. A decisão do juiz Luis Manuel Fonseca apontou tais tecnologias teriam um risco agravado de violar a Lei Geral

---

[363] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/GABINETE DO MINISTRO. "Portaria nº793: Regulamenta o incentivo financeiro das ações do Eixo Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com os recursos do Fundo Nacional de Segurança Pública, previstos no inciso I do art. 7º da Lei nº 13.756, de 12 de dezembro de 2018", 2019.

[364] LAPIN. "Relatório: Vigilância automatizada: uso de reconhecimento facial pela Administração Pública no Brasil", 2021

[365]CÂMARA DE DEPUTADOS. "PROJETO DE LEI N.º 3.069, DE 2022 (Do Sr. Subtenente Gonzaga)", 2022.

de Proteção de Dados, e que o seu uso poderia apresentar uma grave ameaça a direitos fundamentais, como o racismo estrutural. Contudo, a relatora do processo, Paola Lorena, derrubou a liminar numa decisão que afirmou que não há evidências que a implementação de videomonitoramento reforce eventual discriminação social e racial.[366] Tal declaração contraria os inúmeros casos de falsos positivos que ocorreram no Brasil com pessoas pretas (conforme já relatado nesta presente Dissertação).

Por sua vez, o *Uncle Sam* também possui uma forte cultura na vigilância da população através de TRF. Em 2021 o Escritório de Prestação de Contas do Governo Federal divulgou um relatório que constava que 42 agências federais que empregam agentes de segurança utilizaram tecnologia de reconhecimento facial de alguma forma.[367]

Um estudo realizado pelo Pew Research Center sobre os pensamentos e perspectivas dos americanos em relação ao uso generalizado da tecnologia de reconhecimento facial por parte das forças policiais e além disso, constatou que a maioria do público americano acredita que o uso generalizado do reconhecimento facial provavelmente ajudaria a encontrar pessoas desaparecidas e resolver crimes, mas também acredita que é provável que a polícia use essa tecnologia para rastrear a localização de todos e vigiar comunidades negras e hispânicas mais do que outras.[368]

Em 15 de junho de 2021 a deputada democrata Pramila Jayapal introduziu no Senado americano uma lei que objetiva proibir a vigilância biométrica pelo Governo Federal sem autorização legal explícita e reter determinadas concessões federais de governos estaduais e locais que pratiquem tal vigilância. A lei proibiria o uso de TRF e outras tecnologias biométrica por entidades federais, que só poderia ser concedida através de um ato de congresso. Também proibiria o uso das informações coletadas por meio desta tecnologia que violasse a presente lei, em qualquer processo judicial, além de fornecer um direito de ação para indivíduos cujo dados biométricos forem utilizados de forma errônea.[369]

---

[366] MELLO, Daniel. "Justiça libera edital de câmeras com reconhecimento facial em SP", 2023.

[367] GOODWIN, Gretta. "Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees", 2021.

[368] RAINIE, Lee / FUNK, Cary / ANDERSON, Monica / TYSON, Alec. "Public more likely to see facial recognition use by police as good, rather than bad for society", 2023.

[369] U.S.A. CONGRESS. "H.R.3907 - Facial Recognition and Biometric Technology Moratorium Act of 2021 (by Pramilla Jayapal)", 2021.

No entanto, em março de 2023 a lei foi obstruída sem mesmo ter chego a votações. Perante isso, o senador democrata Senator Edward J. Markey voltou a introduzi-la com o nome de "Facial Recognition and Biometric Technology Moratorium Act of 2023" no qual serviria os mesmos efeitos.

Como conseguimos constatar, a aceitação de tecnologias de reconhecimento facial varia entre os países da UE, Brasil e Estados Unidos e isto se dá por diversas razões. A regulação de proteção de dados desempenha um papel importante nessa diferença, com a União Europeia possuindo legislação mais rigorosa, como o RGPD e a LED, que estabelecem diretrizes claras sobre o processamento de dados pessoais. Isso pode resultar em restrições mais rigorosas ao uso de TRF para proteger a privacidade e os direitos individuais.

A sensibilidade em relação à privacidade também difere entre essas regiões. Como já exposto nessa dissertação, os países da UE geralmente possuem uma cultura mais forte de proteção à privacidade e valorizam mais a privacidade individual. Isso pode levar a preocupações maiores em relação ao uso destas tecnologias, especialmente quando envolvem dados biométricos sensíveis. Também é possível conceber que o histórico de vigilância estatal opressiva em alguns países da UE, em tempos de ditadura, pode contribuir para a desconfiança em relação a tecnologias de vigilância em massa,

Por fim, é notável que a UE tem um enfoque forte na proteção dos direitos individuais e dos direitos humanos e fundamentais. As abordagens regulatórias buscam equilibrar a segurança pública com a proteção da privacidade e dos direitos fundamentais dos cidadãos. Isso leva a uma análise mais crítica e cautelosa em relação ao uso de TRFs.

Os exemplos mencionados destacam a urgência de uma regulação que aborde efetivamente as consequências reais das violações da privacidade, da proteção de dados e da não discriminação, fundamentadas nas práticas de vigilância realizadas por sistemas de reconhecimento facial. É imperativo proibir essa prática, pois ela não é compatível com democracias estáveis e prósperas[370] A UE está trilhando esse caminho por meio do desenvolvimento do seu Regulamento sobre Inteligência Artificial. Esperamos que esse

[370] É notável que quanto mais a democracia de um país esteja enfraquecida, mais espaço há para a admissão de práticas de vigilância em massa, como é o caso do Brasil e Estados Unidos, que recém saíram de governos ultraconservadores, populistas de extrema-direita e da Hungria que se encontra nesta posição.

regulamento traga respostas positivas às nossas preocupações, estabelecendo um marco regulatório que, certamente, influenciará outras nações a seguir o mesmo caminho.

# PARTE 3

# O QUE ESPERAR DO FUTURO

# CAPÍTULO 5

# UM MARCO LEGISLATIVO NA ERA DA INTELIGÊNCIA ARTIFICIAL

*"Follow the leader, leader, leader (Siga-me!)"*

**The Soca Boys**

A nova proposta de um quadro regulamentar da UE sobre a IA concentra-se na utilização específica de sistemas de IA e nos riscos associados a estes, objetivando o estabelecimento de regras regulatórias harmonizadas para os EMs. Perante isso, a Comissão pretende consagrar uma definição que seja tecnologicamente neutra dos sistemas de IA e propõe adotar diferentes conjuntos de regras e exigências consoante uma abordagem baseada em risco, elencando: IA de riscos inaceitáveis, no qual os sistemas de IA configuram um uso prejudicial ao violar valores da UE, devendo assim ser proibidos pelo risco inaceitável que representam; IA de risco alto, que representam sistemas que têm impacto negativo na segurança das pessoas ou em seus direitos fundamentais, sendo que para garantir a confiança e um nível consistente de segurança e dos DF, diversos requisitos obrigatórios serão aplicados e deverão ser respeitados; IA de risco limitado, no qual os sistemas estarão sujeitos a um conjunto limitado de obrigações; e IA de risco mínimo, enquadrando todos os outros sistemas de IA que podem ser desenvolvidos sem obrigações legais adicionais além da legislação europeia.[371]

Pela primeira vez na história, começa a ser delineado um instrumento legislativo vinculativo sobre o uso de diversos sistemas de IA[372], em especial, a TRF que estará incluída dentro dos sistemas de identificação biométricos. A primeira formulação do regulamento conta com definições relevantes de dados biométricos e os sistemas de identificação biométrica à distância (já mencionado), além de descrever o que são sistemas de categorização biométrica expondo ser: "um sistema de IA concebido para classificar pessoas singulares em categorias

[371]COMISSÃO EUROPEIA. "Artificial intelligence act in a Europe Fit for the Digital Age", 2023.
[372]COMISSÃO EUROPEIA. "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS - Draft AI Act", 2021.

específicas, tais como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, origem étnica ou orientação sexual ou politica, com base nos seus dados biométricos".[373]

O *Draft AI* também realiza uma diferenciação do que seria os sistemas de identificação biométricos a distância "em tempo real" ou em "diferido". Aponta-se que essa diferenciação é necessária por terem características e formas de utilização diversas, bem como riscos inerentes diferentes[374] - no caso da identificação biométrica em tempo real de pessoas singulares em espaços acessíveis ao público, aponta-se que tal prática "é considerada particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais(...) sendo que dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam em tempo real, estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais."[375]

Além do risco exposto acima, o *draft* ainda aponta riscos acrescidos tanto para os sistemas de IBD em tempo real e em diferido, apontando que "as imprecisões técnicas destes sistemas podem conduzir a resultados enviesados e ter efeitos discriminatórios (...) devendo, tanto a identificação biométrica à distância como em diferido, ser classificadas como de risco elevado(...) devendo estar sujeitos a requisitos específicos relativos.[376]

O *draft* propõe que ambas as formas de utilizar o sistemas de IBD possuem riscos elevados, porém quando a utilizamos em tempo real, essa impõe riscos acrescidos para os direitos e liberdades das pessoas, sendo que o regulamento introduz esta prática dentro do seu artigo 5º número 1º alínea d), que expressa as práticas de IA proibidas, expondo que: "A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública".

[373] Cfr. o Artigo 3º, nº35 do Draft AIA.
[374] Considerando 8 do Draft AIA.
[375] Considerando 18 do Draft AIA.
[376] Considerando 33 do Draft AIA.

Ou seja, o *draft* propunha proibir as autoridades policiais de utilizarem os SIBD em tempo real, em locais públicos, na manutenção da ordem pública. Temos aqui uma limitação do local, que é em locais públicos; uma limitação dos atores: as autoridades policiais; uma limitação da prática: em tempo real; e uma limitação do propósito: para manutenção da ordem pública. A partir disso conseguimos inferir que nada que caiba nesse escopo está proibido, ou seja: a utilização de SIBD em diferido; utilizado em locais privados; utilizado por companhias para outros fins (como para perceber se certo funcionário está no local que lhe foi designado); utilizado por autoridades públicas para outros fins (contagem do número de pessoas em certo evento) e outras infinitas possibilidades.

Contudo, o *draft* não proíbe completamente a utilização do SIBD em tempo real em espaço acessíveis para o público para efeitos de manutenção da ordem pública, pois propõe 3 exceções que uso dessa prática seria tolerado quando a utilização destes sistemas for estritamente necessária: "a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas; a prevenção de uma ameaça especifica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista; e, a detecção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2º, nº 2, da Decisão-Quadro 2002/584/JAI do Conselho e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro."

O *draft* expõe no número 2 do artigo 5º que estas exceções são permitidas de modo restrito, necessitando ter em conta determinados elementos, em especial no que se refere à natureza da situação que dá origem ao pedido e às consequências da utilização para os direitos e as liberdades de todas as pessoas em causa e ainda às salvaguardas e condições previstas para a utilização. Além disso, a utilização desses sistemas deve estar sujeita a limites espaciais e temporais adequados, tendo em conta os dados ou indícios relativos às ameaças, às vítimas, ou o infrator, sendo que a base de dados utilizada deve ser adequada a cada uma das 3 exceções propostas.

No número 3 do artigo 5º ainda impõe-se que para a utilização desses sistemas, seja necessário a autorização expressa e específica de uma autoridade judiciária ou de uma

autoridade administrativa independente. Tal autorização deve ser obtida previamente à sua utilização, ao menos em situações que demonstram uma certa urgência justificada para seu uso (quando a necessidade de utilizar os sistemas em causa torna efetiva e objetivamente impossível obter uma autorização antes de iniciar essa utilização). Para as situações de urgência, a utilização deve limitar-se ao mínimo absolutamente necessário e estar sujeita a salvaguardas e condições adequadas, conforme determinado pelo direito nacional e especificado no contexto de cada caso de utilização urgente pela própria autoridade policial.

Por último, o número 4 do artigo propõe que o uso do SIBD em tempo real no território de um EM só deve ser permitido quando este tiver decidido explicitamente autorizar esse uso de acordo com as regras de implementação previstas na legislação nacional, sendo que os EM ainda têm a liberdade de não permitir esse uso ou de permiti-lo apenas em relação a alguns dos objetivos que justificam um uso autorizado conforme identificado no *draft.*

Perante as exceções expostas no *draft*, conseguimos concluir que a proibição, por mais que seja considerada regra, ainda comporta diversas exceções que justifiquem o uso de SIBD em tempo real para identificação de pessoas em locais públicos com o fim de manutenção da ordem pública. Por mais que tais exceções requeiram a observação da natureza da situação e as consequências da sua utilização, tais critérios se mostram muito abstratos, faltando objetividade na previsão da lei sobre a possibilidade do uso. Também se impõe atenção à limitação temporal e geográfica das pessoas visadas, mas não determina com clareza quais salvaguardas deveriam ser impostas.

No que diz respeito a terceira exceção proposta, abrir-se-ia espaço para uso dos SIBD para detecção, localização, identificação ou instauração de ação penal a um infrator ou suspeito de uma infração penal de crimes como fraude, burla, extorsão, piratagem de produtos, sabotagem entre outros.

Posto isso, cabe também relevar o enquadramento de sistemas de identificação biométrica em diferido, ou aqueles que sejam em tempo real mas não para os fins que sejam considerados proibidos. Esses sistemas de IA são considerados de risco elevado e estarão sujeitos a certas obrigações antes de serem colocadas no mercado (contudo o *draft* não impõe

que a colocação destas esteja sujeita a uma autorização prévia de uma autoridade judiciária ou administrativa)[377].

As obrigações em causa estão elencadas no capítulo 2 do título III do *draft,* impondo que para a colocação no mercado estes sistemas: realizem uma avaliação adequada de riscos e sistemas de mitigação; tenham uma alta qualidade dos conjuntos de dados alimentando o sistema para minimizar riscos e resultados discriminatórios; realizem o registro de atividades para garantir a rastreabilidade dos resultados; tenham uma documentação detalhada fornecendo todas as informações necessárias sobre o sistema e seu propósito para que as autoridades possam avaliar sua conformidade; disponham de informações claras e adequadas para o usuário; tenham medidas apropriadas de supervisão humana para minimizar riscos; e possuam um alto nível de robustez, segurança e precisão.[378] Cabe relevar que o *draft* também impõe que os EM designem ou criem uma autoridade responsável por estabelecer e executar os procedimentos necessários para a avalição dos requisitos citados.[379]

Após a publicação do *Draft AI* pela Comissão em abril, abriu-se um período de consulta pública para que os cidadãos europeus e as entidades europeias, como ONGs, empresas e universidades, pudessem realizar comentários sobre o *Draft.* Esse período de consulta foi encerrado no dia 6 de agosto de 2021 e recebeu 304 comentários, sendo que diversos comentários endereçaram a problemática inerente ao uso das TRFs nos sistemas de identificação biométrica, criticando ou clamando por ajustes, nas provisões fornecidas pelo *draft.*[380]

Podemos, desde logo, citar a posição da Amnistia Internacional[381] que expôs como os SIBD causam sérios problemas relativos aos DH, com um impacto ainda mais relevantes nas comunidades não brancas que já são, *per si,* excessivamente marginalizadas.[382] A amnistia

[377] Considerando 23 do Draft AIA.
[378] COMISSÃO EUROPEIA. "Regulatory framework proposal on artificial intelligence", 2021.
[379] Conforme exposto no Artigo 30º Draft AIA.
[380] Todas as 304 opiniões podem ser consultadas no seguinte domínio: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Inteligencia-artificial-Requisitos-eticos-e-legais/feedback_pt?p_id=24212003
[381]AMNISTIA INTERNACIONAL. "Amnesty International response to the EU's proposal for an Artificial Intelligence Act ("AIA")", 2021.
[382] AMNISTIA INTERNACIONAL. "Amnesty International response to the EU's proposal for an Artificial Intelligence Act ("AIA")", 1.

chama a atenção para o uso de TRFs[383]e dos SIBD utilizados para manutenção da ordem pública justificando que "permitir que as forças de segurança utilizem tecnologias biométricas à distância em tempo real, mesmo que apenas em circunstâncias limitadas, significa que a tecnologia e a infraestrutura associada ainda terão que ser adotadas e implementadas. Isso cria um sério risco de má utilização das tecnologias pelas forças de segurança, que são intrinsecamente discriminatórias e incompatíveis com os direitos humanos."[384] A amnistia ainda reforça o uso deste sistemas por entes privados, declarando que "a utilização por atores privados pode representar a mesma ameaça aos nossos direitos humanos, não apenas quando atores privados se envolvem em vigilância em nome de governos e agências públicas, mas também quando atores privados implantam tecnologias de reconhecimento biométrico para si próprios, pois tal prática utilizada nos locais de trabalho, no recrutamento e recursos humanos, e em ambientes comerciais, resulta em vigilância corporativa e no uso generalizado de técnicas que constituem uma ameaça aos direitos humanos."

Desta forma, a Amnistia Internacional vem a sugerir a proibição total do uso de reconhecimento facial e tecnologias de reconhecimento biométrico remoto que possibilitem a vigilância em massa e a vigilância discriminatória direcionada; proibição da categorização biométrica e sistemas de reconhecimento de emoções tanto por atores públicos como privados, quando são usados para vigilância em espaços de acesso público e em espaços dos quais as pessoas não podem evitar; e, condições rigorosas que proíbem o armazenamento, compartilhamento e (re)uso de dados biométricos coletados para fins de autenticação biométrica.[385]

A AVAAZ Foundation, uma ONG americana, também fez comentários relativos a previsão do AIA no que toca aos SIBD, demonstrando estar alinhada com as preocupações expostas pela Amnistia Internacional. A AVAAZ instou a Comissão que se proibisse totalmente

---

[383] Consideram que o uso destas tecnologias na vertente de autenticação "podem ser construídos e utilizados de maneira que também permita formas problemáticas de vigilância, como criar grandes bancos de dados biométricos centralizados que podem ser reutilizados para outros fins. Há desenvolvimentos preocupantes de atores privados compilando e compartilhando bancos de dados de indivíduos "suspeitos"". Cfr AMNISTIA INTERNACIONAL. "Amnesty International response to the EU's proposal for an Artificial Intelligence Act ("AIA")", 3.

[384] AMNISTIA INTERNACIONAL. "Amnesty International response to the EU's proposal for an Artificial Intelligence Act ("AIA")", 4.

[385] *Ib.,* 5.

os sistemas de IA que fossem incompatíveis com os DF, como os SIBD, sugerindo uma alteração do artigo 5º do *draft*. Este deveria eliminar o seu número 2, 3 e 4 e deveria reduzir a letra do seu número 1 alínea d) prevendo apenas a proibição para: o uso de sistemas de identificação biométrica remota em tempo real em espaços acessíveis ao público, privados ou espaços online.[386]

A empresa alemã European AI Forum, que também propôs a proibição dos SIBD, justificando que as disposições atuais do AIA não previnem suficientemente o risco de vigilância em massa indiscriminada, sendo que a proibição deveria se estender a atores públicos e privados, e também aos SIBD ex post.[387]

Além destes exemplos elucidados, em 18 de junho de 2021 a EDPB e a EDPS divulgaram uma opinião conjunta sobre o AIA com diversas críticas e preocupações sobre os SIBD. Eles apontam que tais sistemas apresentam sérios problemas de proporcionalidade, uma vez que pode envolver o processamento de dados de um número indiscriminado e desproporcional de sujeitos para a identificação de apenas algumas pessoas (por exemplo, passageiros em aeroportos e estações de trem). Tais sistemas também apresentam um efeito irreversível e severo na expectativa (razoável) das populações de serem anônimas em espaços públicos, resultando em um efeito negativo direto no exercício da liberdade de expressão, de reunião, de associação e também da liberdade de movimento.[388]

Perante isso, a EDPB e a EDPS criticam a extensa excepcionalidade do artigo 5ºnº1d) da proposta, considerando que a abordagem de proibição de SIBD em tempo real para manutenção da ordem pública e suas respectivas exceções é falha em vários aspectos, condenando a proibição apenas em tempo real evidenciando que“ a intrusão do processamento nem sempre depende da identificação sendo feita em tempo real ou não, sendo que a identificação biométrica remota posterior no contexto de um protesto político provavelmente terá um efeito inibidor significativo no exercício dos direitos e liberdades fundamentais, como

---

386 AVAAZ THE WORLD IN ACTION. “Avaaz Feedback on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts”, 2021, 21-22.

387 EUROPEAN AI FORUM. “Feedback to the European Commission’s regulation proposal on the Artificial Intelligence Act”, 2021, 3.

388 EDPB-EDPS. “Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”, 2021, 12.

a liberdade de reunião e associação e, de forma mais geral, os princípios fundamentais da democracia." [389]

Relativamente à proibição apenas para autoridades públicas, eles declaram que "o uso desse sistema para outros fins, como segurança privada, representa as mesmas ameaças aos direitos fundamentais de respeito à vida privada e familiar e proteção de dados pessoais."[390]

Por último, as duas entidades de proteção de dados também expressam que a terceira exceção da proposta poderá ser utilizada com abundância, pois mesmo com as limitações previstas, o número potencial de suspeitos ou perpetradores dos crimes expostos sempre será suficientemente alta para justificar o uso contínuo de sistemas de IA para detecção de suspeitos.[391]

Por todas essas razões elucidadas, o EDPB e o EDPS clama por uma proibição geral de qualquer uso de IA para o reconhecimento automatizado de características humanas em espaços de acesso público e online, em qualquer contexto. Os organismos concluem expondo que "levando em consideração a LED e o RGPD, o EDPS e o EDPB não conseguem discernir como esse tipo de prática seria capaz de atender aos requisitos de necessidade e proporcionalidade, e que em última instância decorre do que é considerado interferências aceitáveis nos direitos fundamentais pelo TJUE e TEDH."[392]

Posteriormente a este período de consulta, em 29 de novembro de 2021, a presidência rotativa do Conselho da UE (assegurada pela Eslovênia) apresentou um primeiro texto de compromisso sobre o AIA[393], realizando algumas mudanças no que diz respeito ao artigo 5º da proposta.

Nesta proposta algumas definições importantes foram alteradas. Em primeiro lugar podemos elucidar o caso dos sistemas de identificação biométrica abrangidos na proposta, que agora já não são mais definidos como "à distância", mas como qualquer sistema que leve à

[389] *Ib.*
[390] *Ib.*
[391] *Ib.*
[392] *Ib.*
[393] COUNCIL OF THE EUROPEAN UNION. "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text", 2021.

identificação de pessoas "sem o consentimento delas"[394]. No que diz respeito à "manutenção da ordem pública" essa se refere não só as atividades realizadas por autoridades policiais, mas também por entidades que atuem em seu nome.[395] Por último, os dados biométricos agora se reportam a dados pessoais resultantes de um procedimento técnico relacionado a características físicas, psicológicas e comportamentais de uma pessoa natural, como imagens faciais ou dados dactiloscópicos - excluindo a previsão que imputava a estes dados a possibilidade de obter ou confirmar a identificação única dessa pessoa singular.[396]

No que diz respeito ao *social scoring*, prática que é proibida pela alínea b) do número 1 do artigo visado, a presidência do Conselho propôs a extensão desta proibição albergando também entidades privadas. Também se albergou as situações na qual seria proibida estas práticas, incluindo agora a exploração de uma "situação social ou económica".

Os SIB (agora sem necessitar ser à distância) em espaços acessíveis ao público, teve seu uso estendido em consonância com o que agora significa a manutenção da ordem pública, ou seja, a possibilidade do uso extravasa as autoridades policiais e inclui entidades que atuem em seu nome.[397]

Em contraste com a consulta pública conduzida pela Comissão e com a opinião do EDPS e do EDPB, a proposta atual não apenas remove a possibilidade de usar SIB para a investigação de crianças desaparecidas, mas também amplia ainda mais o escopo das exceções propostas. Isso pode ser observado no número (ii) da alínea d), que dispensa agora o requisito de ameaça iminente e inclui a possibilidade de uso desses sistemas não apenas para a prevenção de ameaças à vida, segurança física de indivíduos ou ataques terroristas, mas também para a proteção de infraestruturas críticas e da saúde dessas pessoas.

O único reforço que foi feito à proteção dos DF e DH potencialmente violados pelos SIB foi restringir a aprovação destes sistemas por uma urgência devidamente justificada sem autorização prévia, exigindo que essa autorização tem que ser solicitada sem demora indevida

[394] BERTUZZI, Luca. "EU Council presidency pitches significant changes to AI Act proposal" in EURACTIV, 2021.
[395] Artigo 3º, nº, 41da nova proposta do AIA pelo Conselho da União Europeia.
[396] Artigo 3º, nº 33 da nova proposta do AIA pelo Conselho da União Europeia.
[397] Artigo 5º, nº1, al. d) da nova proposta do AIA pelo Conselho da União Europeia.

durante seu, e que se esta autorização seja rejeitada, o seu uso será interrompido imediatamente.[398]

Dois dias posteriores à divulgação da nova proposta do AIA, confirmou-se que as comissões de mercado interno e liberdades civis do PE liderariam em conjunto as negociações sobre o regulamento, com Brando Benifei (da comissão de mercado interno) e Dragos Tudorache (da comissão de liberdades civis) sendo os principais negociadores daquele.

Em 25 de janeiro de 2022, os líderes da negociação do AIA divulgaram a primeira troca de impressões relativo ao desenvolvimento do regulamento. Brando Benifei propôs que “"Nosso objetivo é proteger cidadãos e consumidores e estimular a inovação positiva ao mesmo tempo, com foco especial em PMEs e startups. Um quadro legislativo que garanta que os sistemas de IA que entram no mercado único da UE sejam seguros, centrados no ser humano e respeitem nossos direitos e liberdades fundamentais estimulará a confiança entre os cidadãos, o que é fundamental para uma adoção bem-sucedida e inclusiva da IA em nosso continente. É isso que nos esforçaremos para alcançar".[399]

Já Tudorache expressou que “"O AIA é uma peça central do ambiente regulatório europeu para o futuro digital e a primeira do seu tipo no mundo. Temos a chance de liderar pelo exemplo e moldar as regras do mundo digital de acordo com nossos valores. Como coração da democracia europeia, o Parlamento Europeu tem um papel fundamental a desempenhar: precisamos encontrar o equilíbrio certo entre aprimorar a proteção de nossos direitos fundamentais e impulsionar a competitividade da Europa e sua capacidade de inovar".[400]

Em junho de 2022 acabou o prazo para cada grupo político do PE apresentar emendas ao AIA, sendo que cada grupo apresentou centenas de emenda, estabelecendo uma base para as discussões futuras.

No que diz respeito as práticas proibidas, o grupo político dos Verdes/Aliança Livre Europeia introduziu importantes propostas, sugerindo a ampliação desta categoria para incluir

[398] Artigo 5º, nº3 da nova proposta do AIA pelo Conselho da União Europeia.
[399] PARLAMENTO EUROPEU. “Artificial Intelligence Act: lead committees to launch joint work on 25 January”, 2021.
[400] *Ib.*

a categorização biométrica, reconhecimento de emoções e qualquer monitoramento automatizado do comportamento humano.[401]

No que diz respeito aos SIB, Tudorache, pertecente ao grupo político "*Renew Europe"* (um grupo político que se considera centrista), mudou sua posição relativamente ao uso destes sistemas juntando-se ao Grupo da Aliança Progressista dos Socialistas e Democratas do Parlamento Europeu e ao Grupo dos Verdes, advogando por uma proibição completa do reconhecimento biométricos, eliminando as exceções incluídas na proposta original. Além disso, o Grupo dos Verdes ainda introduziu uma proibição de bancos de dados biométricos privados baseados em informações recolhidas da internet, exemplificando a problemática com o caso da empresa *Clearview AI.*[402]

Posterior a esta discussão parlamentar, na primeira semana de dezembro de 2022, o Conselho divulgou a sua posição comum ("*general approach"*) do AIA. Neste, foi alterado alguns aspectos relevantes sobre os SIBD.

Logo, no considerando 8, expõe-se o conceito de SBID que pormenoriza a diferença entre a identificação e a autenticação. Neste conclui-se que o SBID refere-se apenas para a identificação de pessoas[403], sendo que os "sistemas de verificação/autenticação cujo único objetivo seria confirmar que uma determinada pessoa singular é a pessoa que alega ser, bem como os sistemas utilizados para confirmar a identidade de uma pessoa singular com o único objetivo de lhe conceder acesso a determinado serviço, dispositivo ou instalações" estão excluídos deste escopo pelo fato de serem suscetíveis de ter um impacto menor nos DF das pessoas singulares.[404]

No que diz respeito as proibições dos SIBD, o regulamento faz uma alusão específica para a utilização desta prática "em tempo real"[405], pelo que, segundo o considerando 33 do

---

[401] BERTUZZI, Luca. "AI regulation filled with thousands of amendments in the European Parliament", 2022.

[402] *Ib.*

[403] Que é caracterizada como "Esses sistemas de identificação biométrica à distância são geralmente utilizados para detetar (analisar) várias pessoas ou o seu comportamento em simultâneo, a fim de facilitar significativamente a identificação de várias pessoas sem o seu envolvimento ativo." Cfr. COUNCIL OF THE EUROPEAN UNION. "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach", 2022.

[404]Considerando 8 da General approach of AIA.

[405]Considerando 19 da General approach of AIA.

regulamento, quando tal prática for exercida em diferido, ela estará incluída em situações de alto risco.[406]

No caso do SIBD tempo real, a *general approach* manteve a proibição desta prática em tempo real e as mesmas exceções que possibilitam o seu uso. Contudo, este documento vai além ao preservar (explicitamente) a capacidade das autoridades competentes em matéria de manutenção da ordem pública, controlo das fronteiras, imigração ou asilo para realizarem controlos de identidade na presença da pessoa em causa, permitindo (e incentivando) que estas utilizem de sistemas de informação para identificar uma pessoa que durante um controlo de identidade, se recuse a ser identificada ou não seja capaz de declarar ou provar a sua identidade, sem serem obrigadas a obter uma autorização prévia por força do presente regulamento, justificando que tais situações podem tratar-se de, por exemplo, uma pessoa envolvida num crime, ou que não queira ou não possa, devido a um acidente ou a uma situação médica, divulgar a sua identidade às autoridades policiais.[407]

Relativamente a autorização de autoridades administrativas ou judiciárias competentes para a utilização destes sistemas, esta deve ser obtida antes da utilização do sistema. Contudo tal regra possui exceções que se referem a "situações de urgência devidamente justificadas, ou seja, quando a necessidade de utilizar os sistemas em causa torna efetiva e objetivamente impossível obter uma autorização antes de iniciar essa utilização". Nestas situações, a utilização deve ser mínima e sujeita a salvaguardas e condições adequadas, determinadas pelo direito nacional e pelo contexto de cada caso de utilização urgente pela autoridade policial. A autoridade policial deve buscar obter uma autorização o mais rápido possível, apresentando justificativas caso não tenha feito o pedido mais cedo.[408]

O texto divulgado pelo Conselho introduz um novo requisito no que diz respeito ao SIB, exigindo a supervisão humana para estes sistemas, de modo a que o utilizador não possa tomar qualquer medida ou decisão com base no resultado proferido pela tecnologia, a menos que tenha sido verificado separadamente e confirmado por, pelo menos, duas pessoas singulares.

[406] Considerando 18 da General approach of AIA.
[407] Considerando 33 da General approach of AIA.
[408] Considerando 21 da General approach of AIA.

Justificou-se esse requisito reforçado pelo fato de que se o sistemas opera uma correspondência incorreta, tal erro implica consequências significativas para as pessoas em causa.[409]

No que diz respeito a avaliação de conformidade que tem de ser realizada aos SIBD, a *general approach* impõe que a notificação dos organismos realizada pelas autoridades nacionais dos países membros deverá ser enviada à Comissão e aos outros EM por meio de notificação eletrónica.[410]

No que diz respeito ao artigo nº3 do documento, que diz respeito as definições, tivemos alterações importantes. No que concerne os SIBD, este agora é definido como: " um sistema de IA com o propósito de identificar pessoas naturais geralmente à distância, sem o envolvimento ativo delas, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos em um repositório de dados de referência."[411] Também foi alterado a definição dos SIBD em tempo real, significando ser "um sistema de identificação biométrica remota em que a captura de dados biométricos, a comparação e a identificação ocorrem de forma instantânea ou quase instantânea."[412] O artigo 3ºnº38 que propunha uma definição para SIBD em deferido foi suprimido.

Por último, ainda vale relevar que, no que diz respeito a práticas de IA proibidas, o texto estende aos atores privados a proibição de usar IA para *social scoring*. Além disso, a disposição que proíbe o uso de sistemas de IA que exploram as vulnerabilidades de um grupo específico de pessoas agora também abrange pessoas que são vulneráveis devido à sua situação social ou econômica.[413]

No mês de maio de 2023, foi a vez do Parlamento Europeu revelar sua posição em relação ao AIA[414] por meio dos líderes de negociação designados para essa tarefa, Brando Benifei e Ioan-Dragoş Tudorache da Comissão do Mercado Interno e Comissão das Liberdades

[409]Considerando 48 da General approach of AIA.
[410]Considerando 65 da General approach of AIA.
[411]Artigo 3º, nº36 da General approach of AIA.
[412]Artigo 3º, nº37 da General approach of AIA.
[413]COUNCIL OF THE EUROPEAN UNION. "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", 2022.
[414] EUROPEAN PARLIAMENT. "Artificial Intelligence Act(AIA): Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))", 2023.

Cívicas, respectivamente. Tal proposta teve 84 votos a favor, 7 contra e 12 abstenções com mudanças substantivas relativa aos SIBD em comparação à *general approach* delineada pelo Conselho e do *draft* divulgado pela Comissão.

Em primeiro lugar podemos começar por destacar a adição de um novo termo relativo a dados biométricos, que diz respeito "*biometric-based data"*[415]. Este novo conceito diz respeito aos dados resultantes de processamento técnico específico relacionados a sinais físicos, fisiológicos ou comportamentais de uma pessoa natural. Segundo CHRISTIANE WENDEHORST e YANNIC DULLER, essa definição coincide, em grande parte, com a definição de dados biométricos, mas se diferem no ponto de que os dados baseados em biometria podem ou não permitir a confirmação de identificação de uma pessoa natural. Desta forma estaremos englobando os sistemas de categorização biométrica e sistemas de reconhecimento de emoções, que também são sistemas biométricos, mas que nem sempre confirmar a identificação do indivíduo.[416]

Foi também incluído no AIA a definição de "identificação biométrica" e "autenticação biométrica" na letra do artigo 3º. A primeira diz respeito ao "reconhecimento automatizado de características físicas, fisiológicas, comportamentais e psicológicas humanas com o objetivo de estabelecer a identidade de um indivíduo, comparando os dados biométricos desse indivíduo com os dados biométricos armazenados de indivíduos em um banco de dados (identificação de um-para-muitos)".[417] Em relação a autenticação biométrica, esta é definida como a "verificação automatizada da identidade de pessoas naturais por meio da comparação dos dados biométricos de um indivíduo com os dados biométricos previamente fornecidos (verificação um-para-um, incluindo autenticação)."[418]

No que diz respeito ao artigo 5º do AIA que elucida as práticas proibidas, após uma grande mudança do que estava previsto, os Comités concretizaram a ideia de que o uso de sistemas de identificação biométrica em tempo real em espaços acessíveis ao público tem de ser

---

[415] Dados baseados em biometria (Tradução Livre)

[416] EUROPEAN PARLIAMENT. "Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces", 2021, 68.

[417] Artigo 3º, nº33, al. b) do AIA

[418] Artigo 3º, nº33, al. c) do AIA.

proibido sem nenhum tipo de exceção. No que diz respeito aos SIBD remotos através de análise de imagens gravadas de espaços de acesso público, esta prática é considerada proibida, ao menos que tenham uma autorização judicial prévia que esteja de acordo com a legislação da União e que seja estritamente necessário para a busca direcionada relacionada a um crime grave específico que já tenha ocorrido, conforme expõe o artigo 83ºnº1 do TFUE.[419]

Como podemos analisar, nas propostas anteriores do AIA a utilização de SIBD remoto era considerado um sistema de risco elevado - era legal mas precisava cumprir com os requisitos determinados no AIA. Já o uso de SIBD era proibido, mas albergava exceções que deveriam passar pelo requisitos da estrita necessidade e da autorização por parte de uma autoridade judiciária, quando estes sistemas fossem utilizados para procurar crianças desaparecidas ou vítimas de crimes, para a prevenção de ameaças substanciais e eminentes à vida, à segurança física ou a ataques terroristas, e, para a investigação de suspeitos de cometer crimes expostos no Artigo 2 nº2 da Decisão-Quadro do Conselho 2002/584/JHA62.

Perante a nova formulação do AIA, os SIBD em tempo real estão completamente proibidos, independente do seu objetivo a alcançar, e os SIBD remotos só podem ser utilizados em situação mais restritas do que as expostas no *draft AI* e na *general approach* para os sistemas em tempo real - precisam de uma autorização judicial prévia de acordo com a legislação da União e só podem ser acionados para objetivos estritamente necessários aquando da busca direcionada relacionada a um crime grave específico, conforme definido no artigo 83º/1.

Outra adição importante ao texto foi a proibição da coleta indiscriminada e não direcionada de dados biométricos de redes sociais ou imagens de CCTV com o intuito de criar ou expandir bancos de dados de reconhecimento facial, justificando que tal prática contribui para a sensação de vigilância em massa e pode resultar em violações graves dos direitos fundamentais, incluindo o direito à privacidade.[420]

Além das proibições já mencionadas supra, estas se estendem aos sistemas de categorização biométrica que utilizam características sensíveis (gênero, raça, etnia, status de cidadania, religião, orientação política), aos sistemas de policiamento preditivo (baseado em perfilagem, localização ou antecedentes criminais) e, por último os sistemas de reconhecimento

[419] Artigo 5º, al. e) do AIA
[420] Considerando 26, b) do AIA.

de emoções na aplicação da lei, gestão de fronteiras, local de trabalho e instituições educacionais.

Por fim, cabe mencionar que os sistemas biométricos e os sistemas baseados em biometria foram incluídos explicitamente no Anexo III do regulamento, relativo aos sistemas de alto risco, expondo que configuram tais sistemas os: sistemas de IA destinados a serem utilizados para a identificação biométrica de pessoas naturais, com exceção daqueles mencionados no Artigo 5º e os sistemas de IA destinados a serem utilizados para fazer inferências sobre características pessoais de pessoas naturais com base em dados biométricos ou baseados em biometria, incluindo sistemas de reconhecimento de emoções, com exceção daqueles mencionados no Artigo 5º.[421]

Contudo, o nº1 do Anexo III exclui os sistemas de IA destinados a serem utilizados para verificação biométrica, cujo único propósito é confirmar que uma pessoa natural específica é a pessoa que ela alega ser (conforme já mencionado).

Perante isso, revela mencionar que as regras de classificação para sistemas de IA de alto risco (detalhados no anexo 3 do regulamento) alargaram o âmbito do enquadramento de sistemas, propondo: os sistemas de IA serão considerados de alto risco, além da previsão do primeiro paragrafo do número 1 do artigo 6º[422], se se enquadrarem em uma ou mais áreas e casos de uso críticos mencionados no Anexo III caso representem um risco significativo para saúde, segurança ou DF de indivíduos, ou no caso do ponto 2 se apresentar risco ao meio ambiente. Para tal avaliação, caberá a Comissão, 6 meses antes da entrada em vigor do regulamento e após consulta com o *AI Office,* fornecer diretrizes especificando de forma clara quais sistemas representariam os riscos citados.[423]

---

[421] Anexo III, nº1 do AIA.

[422] "1. Independentemente de um sistema de IA ser colocado no mercado ou utilizado de forma independente dos produtos mencionados nos pontos (a) e (b), esse sistema de IA será considerado de alto risco se as duas seguintes condições forem cumpridas:
(a) o sistema de IA é destinado a ser utilizado como componente de segurança de um produto, ou o próprio sistema de IA é um produto, abrangido pela legislação de harmonização da União listada no Anexo II,
(b) o produto cujo componente de segurança, nos termos do ponto (a), é o sistema de IA, ou o próprio sistema de IA como produto, deve passar por uma avaliação de conformidade de terceiros relacionada aos riscos para a saúde e segurança, com vista à colocação no mercado ou utilização desse produto, nos termos da legislação de harmonização da União listada no Anexo II." Cfr. artigo 6º, nº1 do AIA.

[423] Artigo 6º, nº2 e nº2º, al. a) do AIA.

Também se propôs que quando os provedores, que se enquadram nas circunstâncias de risco, julgarem que os seus sistemas de IA não representa um risco significativo, deverão enviar uma notificação fundamentada à Autoridade de Supervisão Nacional para um parecer sobre a existência ou não de riscos significativos. Já os provedores que classificarem incorretamente seu sistema de IA, colocando-o no mercado antes do prazo para a objeção da Autoridade de Supervisão Nacional, estarão sujeitos a multas.[424]

No dia 14 de junho de 2023, o Parlamento Europeu adotou a sua posição de negociação sobre o Ato de Inteligência Artificial, obtendo 499 votos favoráveis, 28 votos contrários e 93 abstenções. A partir desse momento, deram-se início às negociações com o Conselho a fim de definir a forma final do regulamento. Este documento manteve as previsões relativa aos SIBD.

Após a votação encerrar-se, o co-relator Brando Benifei expôs: "Todos os olhos estão voltados para nós hoje. Enquanto as grandes empresas de tecnologia estão soando o alarme sobre suas próprias criações, a Europa avançou e propôs uma resposta concreta aos riscos que a IA está começando a representar. Queremos aproveitar o potencial positivo da IA para criatividade e produtividade, mas também lutaremos para proteger nossa posição e combater os perigos para nossas democracias e liberdades durante as negociações com o Conselho". Nesta lógica, cabe inferir que esta aprovação no Parlamento configura um marco de extrema relevância no processo de regulamentação da IA na UE e no mundo inteiro. Essa adoção indica que o Parlamento está avançando no desenvolvimento de uma legislação abrangente e coerente para lidar com os desafios e oportunidades apresentados pela IA, refletindo as preocupações e prioridades do Parlamento em relação ao uso ético, responsável e seguro desta nova tecnologia, bem como a proteção dos direitos fundamentais e direitos humanos dos cidadãos europeus.

Essa posição de negociação do Parlamento Europeu também sinaliza sua determinação em desempenhar um papel ativo na definição das políticas relacionadas à IA, em vez de deixar exclusivamente nas mãos de empresas de tecnologia. Ao assumir a liderança nessa questão, o Parlamento busca garantir que tal tecnologia seja desenvolvida e utilizada de acordo com os valores europeus de democracia, direitos fundamentais e direitos humanos e o Estado de Direito. Isso implica encontrar um equilíbrio entre promover o potencial positivo da inteligência

[424] Artigo 6, nº2, al. b) e nº2, al. c) do AIA.

artificial para a criatividade e a produtividade, ao mesmo tempo em que se protege contra os perigos potenciais para a democracia e as liberdades individuais.

Com a adoção dessa posição, o Parlamento estabelece uma base sólida para as futuras negociações com o Conselho e outros atores relevantes. A finalização das negociações até o final do ano demonstra o compromisso de avançar rapidamente nesse processo e estabelecer uma estrutura legal abrangente para a IA na UE. No entanto, é importante observar que essas negociações podem ser complexas, envolvendo diferentes interesses e perspectivas dos EMs, e podem exigir discussões aprofundadas para alcançar um consenso. O resultado final dessas negociações terá um impacto significativo no desenvolvimento, uso e governança da inteligência artificial na UE, e em todo o mundo, nos próximos anos.

# CAPÍTULO 6

# AVALIANDO O PAPEL DO REGULAMENTO SOBRE A INTELIGÊNCIA ARTIFICIAL: UMA SOLUÇÃO PARA NOSSOS PROBLEMAS?

## 1. REVISITANDO A QUESTÃO DA PRIVACIDADE, PROTEÇÃO DE DADOS E DISCRIMINAÇÃO

Conforme demonstrado ao longo deste texto, na constante evolução da IA e das TRFs, a proteção da privacidade, a garantia da proteção de dados e a mitigação da discriminação emergem como questões centrais e desafiadoras. A utilização de sistemas de identificação biométrica, em particular, suscita preocupações relacionadas ao equilíbrio entre a conveniência proporcionada por essas tecnologias e a preservação dos direitos individuais.

A discussão sobre a proibição de TRFs no contexto de SIBD, ou do seu uso (com algumas restrições) foi um dos principais debates desde que a Comissão divulgou a primeira proposta do AIA em abril de 2021. A verdade é que, como pudemos analisar, oscilou-se a previsão no regulamento sobre a restrição, abrangência e proibição do seu uso. Alguns declaravam o seu apoio ao uso de tais tecnologias para a manutenção da ordem pública, clamando que o interesse público na segurança era predominante nesse debate. Do outro lado, clamava-se por uma proibição total de TRFs em espaços públicos, justificando que o seu uso

violava DF e DH e até o próprio Estado de Direito, sendo que o uso destas não convergiam com a ideia de democracia sustentada pela UE.

A discussão acerca da proibição do uso de SIBD em tempo real no contexto da IA, ou de seu uso com determinadas restrições, tem sido um dos principais pontos de debate desde que a Comissão apresentou a primeira proposta do AIA em abril de 2021. Ao examinar as diversas perspectivas apresentadas, observa-se uma oscilação na regulamentação em relação à restrição, abrangência e proibição do uso dessas tecnologias.

Enquanto alguns defendem a utilização dessas tecnologias como meio de manutenção da ordem pública, argumentando que o interesse público em segurança é preponderante nesse debate, outros defendem uma proibição total do uso de TRFs em espaços públicos. Essa posição se fundamenta na argumentação de que o uso dessas tecnologias viola os direitos fundamentais e humanos, bem como o próprio Estado de Direito, expondo, também, que tal uso não está em conformidade com a concepção de democracia sustentada pela UE.

Tal discussão teve lugar no 15 de junho durante a votação do AIA no Parlamento. Embora a proposta do Parlamento contemplasse a proibição total dos SIBD em tempo real, o Partido Popular Europeu, de orientação centro-direita, procurou introduzir exceções para tal uso em circunstâncias como ataques terroristas ou desaparecimento de pessoas.[425] No entanto, é gratificante observar que os membros do Parlamento optaram por levar em consideração os dados, as estatísticas e a ampla participação dos mais de 80 grupos da sociedade civil da campanha "*Reclaim your face*"[426], priorizando assim "a liberdade e a democracia em vez da distopia biométrica"[427] - Foi proibida os SIBD em tempo real, o *social socring*, a categorização biométrica tendo por base características sensíveis (como sexualidade, gênero, raça e etnia), o reconhecimento de emoções em contexto educacional, de trabalho e nas fronteira pela polícia e foi altamente restrito o uso de SIBD em diferido.

A posição tomada pelo Parlamento foi recebida com entusiasmo pela comunidade académica, civil e ativistas de Direitos Humanos. MHER HAKOYBAN disse a este respeito:

---

[425] BORAL, Masha. "EU Parliament approves AI Act amid heated biometrics debates", 2023.

[426] Campanha disponível no website da Reclaim your face: https://reclaimyourface.eu

[427] EUROPEAN DIGITAL RIGHTS, EDRI. "EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act", 2023.

"Nós saudamos a decisão do Parlamento Europeu de adotar uma proibição sobre a tecnologia abusiva de vigilância em massa na votação histórica de hoje. (...) Não há forma compatível com os direitos humanos de utilizar a identificação biométrica remota. Nenhuma correção, técnica ou de outra natureza, pode torná-la compatível com a legislação de direitos humanos. A única salvaguarda contra a SIBD é uma proibição total. Se esses sistemas forem legalizados, isso estabelecerá um precedente alarmante e de amplo alcance, levando à proliferação de tecnologias de IA que não estão em conformidade com os direitos humanos no futuro."[428] CATERINE RODELLI, analista de política da UE da *Access Now* completa expondo: "Nesta votação histórica do AIA, o Parlamento Europeu defendeu uma sociedade livre de vigilância em massa."[429]

Contudo, e como inteligentemente ilustrou PATRICK BREYER, os parlamentares que apoiaram a legalização de SIBD, apoiando assim a vigilância biométrica, estão tentando "entregar aos governos autoritários do presente e do futuro uma arma de opressão sem precedentes"[430]

A controvérsia em torno dessa questão evidenciou a necessidade de equilibrar adequadamente a segurança pública e a proteção dos direitos individuais. A decisão do Parlamento de proibir os SIBD em tempo real e de restringir estes sistemas em diferido reflete um posicionamento que valoriza a preservação dos direitos fundamentais e humanos na era da IA. Essa medida demonstra o compromisso da UE em estabelecer limites e regulamentações que garantam que o desenvolvimento e a utilização da IA estejam alinhados com os valores democráticos e o respeito aos direitos individuais, evitando assim uma realidade orwelliana.

A posição do Parlamento reconhece os riscos inerentes a essas tecnologias, que têm o potencial de monitorar e identificar pessoas de forma indiscriminada e invasiva, além de propiciar identificações incorretas, especialmente em relação a indivíduos não brancos e não cisgênero. Isso abre espaço para o uso abusivo, a vigilância em massa e a discriminação, principalmente em contextos de aplicação da lei e segurança pública. Ao reconhecer esses

[428]AMNISTIA INTERNACIONAL. "EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk", 2023.
[429] WOOLACOTT, Emma. "Draft AI Act Passes, Banning Police Facial Recognition", 2023.
[430] BORAL, Masha. "EU Parliament approves AI Act amid heated biometrics debates".

riscos, a proibição busca salvaguardar os direitos individuais e evitar práticas discriminatórias, reforçando assim a importância de uma abordagem cautelosa e responsável na utilização da tecnologia de reconhecimento facial.

Tal posição também envia um sinal importante para outros países e jurisdições ao redor do mundo. Ao adotar uma postura rigorosa em relação aos SIBD em tempo real, a UE demonstra sua liderança no desenvolvimento de regulamentações que buscam equilibrar o avanço tecnológico com a proteção dos indivíduos. Essa ação pode influenciar outros países a adotarem medidas similares para garantir a privacidade e a segurança dos cidadãos diante do avanço rápido e abrangente desta nova tecnologia.

Por conseguinte, podemos concluir que a proibição do uso de SIBD em tempo real, como as TRFs incorporadas à CCTV conseguem acautelar de forma significativa a proteção de dados, de privacidade e da prevenção à discriminação.

No que diz respeito à proteção de dados, como tais tecnologias conseguiam realizar a coleta e o processamento de informações biométricas sensíveis, como características faciais únicas, sem o consentimento explícito das pessoas envolvidas, tal prática representava um risco significativo na proteção de dados pessoais. A partir da proibição, fica impedido o uso indiscriminado desses sistemas em tempo real, pelo que assegura-se que os dados biométricos dos cidadãos não sejam processados apenas por estarem a se deslocar em áreas públicas.

Além disso, a proibição também contribui para a salvaguarda da privacidade dos indivíduos nestes espaços públicos. O reconhecimento facial em tempo real permite a identificação automática e em massa de pessoas, o que poderia conduzir à vigilância em massa e a consequente falta de anonimato. Ao proibir essas práticas, as pessoas podem se sentir seguras e protegidas em suas interações cotidianas, sem o receio de um constante monitoramento, a ponto de ser mal interpretadas nas suas ações diárias e de serem identificadas sem o seu consentimento.

A questão da discriminação também é abordada pela proibição. Conforme expomos nesse presente texto, estudos demonstraram que as TRF tendem a ter taxas de erro mais altas a identificar pessoas não brancas e não cisgênero (minorias que, via de regra, já são mais marginalizadas). Tal erro imputa à máquina o viés discriminatório que há tanto permeia nossa sociedade, resultando em consequências severas para esses grupos minoritários. Sendo assim, a

proibição de SIBD em tempo real e a severa restrição em diferido contribui para evitar a perpetuação dessas disparidade e promoção de igualdade de tratamento ao restringir o uso de tecnologias que possam causar discriminação involuntária ou intencional. Além disso proibiu-se a categorização biométrica discriminatória e o policiamento preditivo, práticas que demonstravam um alto nível de racismo algorítmico. Contudo e como veremos infra, temos alguns desafios que ficaram pendentes.

É importante salientar que o regulamento estabelece sanções para o descumprimento da proibição das práticas de IA mencionadas no artigo 5º, bem como o direito de apresentar uma reclamação a uma autoridade supervisora nacional, caso haja alegações de violação do AIA por parte de qualquer sistema de IA relacionado ao cidadão.

No que diz respeito às sanções, em conformidade com o artigo 71º, nº 1, do AIA, a violação da proibição das práticas de inteligência artificial mencionadas no Artigo 5º implicará a imposição de multas administrativas de até 40.000.000 EUR, ou até 7% do faturamento anual total da empresa infratora em todo o mundo no ano financeiro anterior, prevalecendo o valor mais elevado.

No que concerne o direito de apresentar queixas, o regulamento prevê no seu "novo" artigo 68º que qualquer pessoa ou grupo tem o direito de apresentar uma reclamação a uma autoridade de supervisão nacional se acreditar que um sistema de IA está violando este Regulamento, sem a necessidade de recorrer a outros meios administrativos ou judiciais, sendo que a autoridade de supervisão informará o reclamante sobre o andamento e o resultado da reclamação, incluindo a opção de buscar um recurso judicial.

## 2. O USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL FORA DO ESCOPO DOS SISTEMAS DE IDENTIFICAÇÃO BIOMÉTRICA EM TEMPO REAL

Celebramos com grande entusiasmo a consagração inequívoca da proibição dos SIBD em tempo real em espaços de acesso público, uma vez que estes são amplamente reconhecidos como uma forma de vigilância por TRF mais grave. Essa gravidade decorre de vários aspectos: a capacidade de monitorar e identificar indivíduos de maneira contínua e ininterrupta, o que

implica em uma vigilância constante e em tempo integral; o maior potencial de abusos, permitindo o rastreamento de pessoas em tempo real sem o seu conhecimento e consentimento; e a maior suscetibilidade a falhas técnicas e falsos positivos, resultando em identificações incorretas e possíveis violações dos direitos individuais.

No entanto, o regulamento permite a possibilidade do uso de SIBD para fins distintos daqueles empregados em tempo real. Um exemplo disso é o uso de SIBD em diferido, que é considerado proibido de acordo com o texto, mas inclui uma exceção: desde que sejam previamente autorizados com base na legislação da União e sejam estritamente necessários para realizar uma busca direcionada relacionada a uma infração penal grave específica, conforme definido no artigo 83º, nº1 do TFUE e que já tenha ocorrido. É importante ressaltar que os domínios de criminalidade abrangidos por este artigo são: terrorismo, tráfico de seres humanos e exploração sexual de mulheres e crianças, tráfico de drogas e armas, lavagem de dinheiro, corrupção, falsificação de meios de pagamento, crimes cibernéticos e crime organizado.

Em comparação ao texto delineado pela Comissão em abril de 2021, o uso de SIBD em diferido em espaços de acesso público sofreu grandes restrições. Anteriormente estes sistemas estavam enquadrados nas tecnologias de risco elevado, pelo que poderiam ser utilizadas, mas deveriam respeitar uma série que de requisitos de conformidade para tal.

Tal permissividade abrangente do uso de SIBD em diferido pelo AIA elaborado pela Comissão, foi alvo de crítica pelo EDPB, EDPS e CDT. Os dois primeiros órgãos expuseram que "O fato de o processamento ser intrusivo nem sempre depende da identificação ser feita em tempo real ou não. A identificação biométrica remota em contexto de protesto político provavelmente terá um efeito inibidor significativo no exercício dos direitos e liberdades fundamentais, como a liberdade de reunião e associação, e mais geralmente nos princípios fundamentais da democracia."[431] Já o CDT postulou que "A distinção entre o uso em tempo real e em diferido da tecnologia é arbitrária. As autoridades policiais podem simplesmente armazenar imagens faciais obtidas por meio de vigilância não direcionada e buscar identificar quaisquer indivíduos em seus bancos de dados depois que as imagens forem registradas. Tal uso violaria os direitos humanos tanto quanto a vigilância em tempo real: em ambos os casos, por

[431] EDPB-EDPS. "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", 11.

exemplo, as autoridades poderiam buscar identificar participantes de um protesto político público sem qualquer suspeita ou evidência de que os manifestantes tenham violado alguma lei." [432]

Perante tais contestações, o Parlamento parece ter acolhido tais preocupações na nova redação do AIA, não banindo os SIBD em diferido completamente, mas restringindo bastante o seu uso, limitando-o apenas para a criminalidade grave prevista no TFUE, e através de autorização com base em legislação europeia. Tal solução parece ser coerente com o fundamento da salvaguarda dos DH e DF, mas poderia ainda ser complementada com a necessidade de uma autorização por parte da autoridade nacional de proteção de dados do respetivo país, para garantir que nenhum tipo de abuso fosse cometido no procedimento em causa. Também poderia ser determinado os limites temporais e geográficos que as autoridades competentes poderiam utilizar para a prossecução de tais crimes. A esperança final é que as negociações realizadas no Parlamento tenham em conta tais salvaguardas.

No que diz respeito aos SIBD que não tenham lugar em espaços de acesso público, estes são permitidos, mas enquadrados como práticas de risco elevado[433] e, por isso, deverão respeitar os requisitos propostos para o uso destas.

Perante este fato, cabe expor o que o AIA entende como espaço de acesso público, pelo que no seu considerando 9 ele expõe que: "a noção de espaço de acesso público deve ser entendida como referindo-se a qualquer local físico que seja acessível ao público, independentemente de ser de propriedade privada ou pública, e independentemente das restrições de capacidade potenciais. Portanto, a noção não abrange lugares de natureza privada e normalmente não livremente acessíveis por terceiros, incluindo autoridades policiais, a menos que essas partes tenham sido especificamente convidadas ou autorizadas, como residências, clubes privados, escritórios, armazéns e fábricas. Espaços online também não estão abrangidos, uma vez que não são espaços físicos. No entanto, o mero fato de certas condições de acesso a um espaço específico se aplicarem, como bilhetes de admissão ou restrições de idade, não significa que o espaço não seja acessível ao público nos termos deste Regulamento.

[432] CDT Europe, "Facial recognition briefing Paper: The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act", 2.
[433] Conforme previsto no Anexo III, nº1, al. a).

Consequentemente, além de espaços públicos como ruas, partes relevantes de prédios governamentais e a maioria das infraestruturas de transporte, espaços como cinemas, teatros, estádios, escolas, universidades, partes relevantes de hospitais e bancos, parques de diversões, festivais, lojas e centros comerciais também são normalmente acessíveis ao público. No entanto, determinar se um determinado espaço é acessível ao público deve ser feito caso a caso, levando em consideração as especificidades da situação individual em questão."[434][435]

A própria letra do texto exemplifica que tipos de locais são considerados não públicos, como clubes privados, escritórios, armazéns e fábricas, no qual poderiam ser alvo de SIBD. Contudo, como estes sistemas realizam o processamento de dados biométricos, e, conforme já mencionamos previamente, para os atores desta prática poderem realizar a identificação biométrica, será necessário encontrar respaldo no artigo 10º da LED (autoridades policiais) e 9º da RGPD (demais entes).

No contexto de manutenção da ordem pública, é difícil encontrar justificativas para esse uso, pois o próprio considerando 9 do AIA estabelece que "a noção não abrange lugares de natureza privada e normalmente não livremente acessíveis por terceiros, incluindo autoridades policiais, a menos que essas partes tenham sido especificamente convidadas ou autorizadas". Isso significa que, para utilizar os SIBD, as autoridades precisam ser autorizadas e/ou convidadas para o local, além de terem uma base legal conforme estabelecido no artigo 10º da LED. Essa base legal requer, além da estrita necessidade, a autorização do direito da União Europeia ou do Estado-Membro, a proteção de interesses vitais do titular dos dados ou se esses dados se tornaram públicos pelo próprio titular.

No contexto do processamento de dados biométricos por entidades privadas através da tecnologia de reconhecimento facial, as exceções estabelecidas no artigo 9º do RGPD não

[434] Conforme o Considerando 9 do AIA.

[435] Cabe relevar que a ausência da inclusão de espaços online na definição de espaços de acesso público gerou preocupações anteriormente entre a comunidade acadêmica e os ativistas de direitos humanos, que temiam que a internet pudesse se tornar um local para a criação ou expansão de bases de dados biométricos. No entanto, o novo texto do AIA abordou essa preocupação no seu artigo 5º (d b), propondo a proibição da "colocação no mercado, a colocação em serviço ou o uso de sistemas de IA que criam ou ampliam bases de dados de reconhecimento facial por meio da coleta não direcionada de imagens faciais da internet ou de imagens de CCTV".

parecem ser adequadas para atividades de natureza privada, com exceção do consentimento[436] - contudo, mesmo esse apresenta requisitos exigentes que podem ser difíceis de atender.[437]

O consentimento como base legal para o uso de TRF por entes privados para a realização de identificação biométrica é rigoroso e impõe certos requisitos para ser aceito: deve ser inequívoco, livre e fornecido por meio de uma ação afirmativa clara; deve ser separado dos termos e condições do serviço e não pode ser uma condição para o acesso aquele serviço; há que haver um equilíbrio de poderes entre quem exige o consentimento e quem o dá; e, o provedor do consentimento deve possuir todas as informações perante aquilo que consente. Contudo, no caso das TRF para identificação biométrica, parece ser difícil atingir esses requisitos, pois: quando necessitarmos do consentimento de um grande número de pessoas, será difícil para o controlador de dados demonstrar que o consentimento foi dado por cada pessoa escaneada; se em um espaço, como um clube privado, houver pessoas que forneceram o consentimento e outras que não forneceram, o ator dos SIB terão problemas em conseguir realizar a identificação de apenas algumas pessoas quando esta tecnologia for realizada em tempo real; quando estivermos perante cenários em que o consentimento parece ser genuíno, mas na verdade o indivíduo não tem escolha real em não consentir, como no exemplo de uma empresa privada propor adotar um sistema de reconhecimento facial para verificar se os seus funcionários estão nos lugares que deveriam estar[438] – há aqui uma desequilíbrio de poderes entre o funcionário e a empresa, não revestindo em um consentimento considerado livre.

Por conseguinte, conseguimos analisar a dificuldade que será aplicar SIBD por atores privados que consigam respeitar todos os regulamentos vigentes, sendo que o uso das TRF que mais serão comuns e que menos levantarão problemas, hão de ser aquelas utilizadas para a autenticação – ou seja, para entrar em condomínios, em clubes, para o desbloqueio de smartphones, para realizar pagamentos virtuais, entre outros.

Por último, dentro do uso de TRF fora do escopo de SIB, há que falar da permissividade do AIA relativamente a utilização destes sistemas no âmbito da imigração, lembrando que as

[436] Previstos no artigo 9º, nº2º, al. a) do RGPD.
[437] RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", 12.
[438] *Ib.*, 12 – 14.

fronteiras não são consideradas espaços de acesso público, não estando proibidas pelo âmbito do artigo 5º d).

Desta forma, o considerando 39 do AIA propõe que "os sistemas de IA utilizados na gestão da migração, asilo e controle de fronteiras (...) são considerados de alto risco (...) mas podem ser utilizados para avaliação de riscos apresentados por pessoas físicas que adentram o território de um EM ou solicitam visto ou asilo; verificar a autenticidade dos documentos pertinentes de pessoas físicas; para auxiliar as autoridades públicas competentes na análise e avaliação da veracidade de evidências relacionadas a pedidos de asilo, vistos e autorizações de residência e queixas associadas em relação ao objetivo de estabelecer a elegibilidade das pessoas físicas solicitantes de um status; para monitorar, vigiar ou processar dados pessoais no contexto de atividades de gestão de fronteiras, com o propósito de detectar, reconhecer ou identificar pessoas físicas; e, para prever ou prever tendências relacionadas a movimentos migratórios e cruzamentos de fronteiras".

Perante o exposto, conseguimos concluir que o Parlamento falha em prever disposições que protegem os direitos dos migrantes em relação a regimes de vigilância discriminatória, dando azo para o rastreio, controle e monitoramento de migrante de forma altamente prejudicial, facilitando expulsões ilegais ou perfilhamento de pessoas em movimento de forma discriminatório, fortalecendo o panóptico nas fronteiras da UE.[439] Segundo MHER HAKOBYAN "é preocupante que o Parlamento não tenha conseguido garantir os direitos humanos quando os sistemas de IA afetam migrantes, refugiados e solicitantes de asilo (...). É vital que, à medida que o AIA avance para as negociações finais, os legisladores da UE não ignorem o direito destas pessoas."[440] SARAH CHANDER completa expondo que "infelizmente, o apoio do Parlamento aos direitos das pessoas não vai além da proteção aos migrantes contra danos causados pela IA, inclusive quando a IA é utilizada para facilitar pushbacks (expulsões ilegais). A UE está criando uma regulamentação de IA em dois níveis, em que os migrantes recebem proteções inferiores em relação ao restante da sociedade."[441]

[439] EUROPEAN DIGITAL RIGHTS, EDRI. "EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act".
[440] AMNISTIA INTERNACIONAL. "EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk".
[441] EUROPEAN DIGITAL RIGHTS, EDRI. "EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act".

É extremamente preocupante o fato de o AIA não proibir práticas como a avaliação de riscos apresentados por pessoas físicas que entram no território de um EM ou solicitam visto ou asilo, assim como a verificação da autenticidade de documentos pertinentes. Além disso, a utilização de IA para auxiliar as autoridades públicas na análise e avaliação da veracidade de evidências relacionadas a pedidos de asilo, vistos e autorizações de residência e em reclamações associadas, a fim de estabelecer a elegibilidade dos solicitantes, e para monitorar, vigiar ou processar dados pessoais no contexto de atividades de gestão de fronteiras, com o propósito de detectar, reconhecer ou identificar pessoas físicas, bem como prever tendências migratórias e cruzamentos de fronteiras, revela uma lacuna grave na proteção dos direitos dos migrantes, refugiados e solicitantes de asilo na UE. Essas práticas podem levar a discriminação, violações dos direitos humanos, falta de transparência e danos significativos às pessoas mais vulneráveis, negando-lhes o devido respeito aos seus direitos fundamentais. É essencial que sejam estabelecidas regulamentações mais abrangentes e rigorosas para evitar abusos e garantir a proteção dos direitos humanos de todas as pessoas, independentemente de seu status migratório.

Conforme propõe DANIEL LEUFER "a equipe de negociação do Parlamento deve exigir que essas proteções não se mantenham enfraquecidas durantes as negociações trilaterais, mantendo a posição contra o lobby da indústria e o excesso de poder estatal para garantir a segurança dessas vitórias e ampliá-las para as pessoas nas fronteiras da UE, além de tentar fechar as lacunas e brechas que ainda existem."[442]

## 3. A LACUNA DA DISCRIMINAÇÃO ALGORITMICA

Conforme abordado ao longo deste texto, um dos grandes problemas associado ao uso das tecnologias de reconhecimento facial prende-se com possibilidade desta apresentar aquilo que agora consideramos o racismo algorítmico. Este é definido por TARCÍZIO SILVA como "o modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em detrimento de grupos minorizados, sendo que essa ordenação pode ser

[442] ACCESS NOW. "Historic vote in the European Parliament: dangerous AI surveillance banned, but not for migrant people at the borders", 2023.

vista como uma camada adicional do racismos estrutural, que, além do mais, molda o futuro e os horizontes de relações de poder, adicionando mais opacidade sobre a exploração e a opressão global que já ocorriam desde o projeto colonial do século XVI"[443] Ou seja, podemos afirmar que este novo tipo de discriminação tem lugar quando os sistemas de inteligência artificial e algoritmos utilizados em processos automatizados tomam decisões que resultam em tratamento desigual ou injusto com base em características pessoais, como raça, gênero, idade, orientação sexual ou origem étnica, sendo que essa forma de discriminação pode ser sutil, muitas vezes invisível aos olhos dos usuários e das próprias empresas que desenvolvem esses sistemas.

Esta prática danosa não se cinge apenas às TRF, sendo que podemos encontrar o racismo algorítmico em outras técnicas da IA, como: hiper-sexualização de crianças e mulheres negras como resultado de buscas não pornográficos; plataforma que entregam anúncios sobre crime especificamente afro-americano; aplicativos de "embelezamento" ou "envelhecimento" de selfies que embranquece os rostos dos usuários; análise facial de emoções relaciona categorias de emoções negativas à pessoas negras; *chatbots* questionam a existência do holocausto judaico; vídeos com desinformação baseada em racismo recebem mais engajamento pelo tom extremistas; entre diversos outros exemplos que existem atualmente.[444] Muitos destes exemplos elucidativos se dão devido a dados de treinamento não representativos, viés em esquemas de rotulagem de dados e funções matemáticas defeituosas/inadequadas.[445]

No entanto, como observado por TARCÍZIO SILVA, a atribuição de autoridade à tecnologia em decisões relacionadas a abordagem, identificação, tipificação ou condenação, por meio de dispositivos de reconhecimento facial, policiamento preditivo e escores de risco, representa um dos maiores perigos do racismo algorítmico.[446] Essas tecnologias tendem a apresentar viés discriminatório, afetando principalmente as pessoas não brancas, de diferentes raças e etnias, bem como aquelas que não se enquadram nos padrões cisgênero, com destaque especial para as mulheres transexuais. Infelizmente, no século XXI, a imagem idealizada ainda remete à figura de um homem branco, o que contribui para a perpetuação dessas disparidades.

[443] SILVA, Tarcízio. "Racismo Algorítmico: Inteligência Artificial e discriminação nas redes digitais",2022, 66.
[444] *Ib.,* 33-34.
[445] EPRS, "Regulating facial recognition in the EU", 17.
[446] *Ib.,* 66.

O quadro europeu que rege a proteção da não discriminação, num contexto prévio ao AIA, é composto por uma legislação primária e outra legislação secundária que pode ser aplicada à tomada de decisões algorítmicas. Relativamente a legislação primária temos consagrado o direito e regras de não discriminação no artigo 2º do TUE, 10º do TFUE, 20º e 21º da Carta e como um princípio geral na jurisprudência. Considera-se que o artigo 21º da Carta pareça ser aquele que conceitualmente é adequado para lidar com casos de discriminação algorítmica.[447]

Em termos de legislação secundária, as leis antidiscriminação mais pertinentes incluem a Diretiva da Igualdade Racial 2000/43/CE, a Diretiva da Igualdade no Emprego 2000/78/CE, a Diretiva dos Bens e Serviços com Base no Gênero 2004/113/CE e a Diretiva da Igualdade de Gênero (reformulada) 2006/54/CE. Esta legislação abrange o âmbito de emprego, sistema de bem-estar e acesso a bens e serviços e possui uma lógica homogênea que distingue entre discriminação direta e indireta.

A discriminação direta ocorre quando há uma distinção explícita com base no "fundamento protegido" ou em um fator inseparável deste, e só pode ser justificada sob condições estritas. Por outro lado, a "discriminação indireta" refere-se a um tratamento aparentemente neutro (regra, critério ou prática neutra) que coloca um grupo em desvantagem significativa. No caso de discriminação algorítmica, a discriminação indireta parece ser aquela adequada para abranger um amplo espectro de resultados algorítmicos aparente neutros, mas na verdade discriminatórios.[448] Contudo, muitos pesquisadores consideram que este quadro apresentado de antidiscriminação da UE não oferece uma proteção suficiente contra a discriminação algorítmica, tendo em vista que este problema é relativamente novo e pode sujeitar novos segmentos da população a tratamento diferencial que não se enquadram nestas bases pré-existentes.[449] Por mais que o DF à não discriminação apresentar uma solução que pareça plausível a problemática em causa, ele apenas se aplica quando as instituições, órgãos, escritórios e agências da União estão atuando ou quando o direito da UE está sendo implementado pelos EM (segundo o artigo 51º da Carta).[450]

---

[447] EPRS, "Regulating facial recognition in the EU", 18.
[448] *Ib.,* 19.
[449] WATCHER, Sandra / MITTELSTADT, Brent / RUSSEL, Chris. "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI", 2020, 11-12.
[450] GERARDS, Janneke / BORGESIUS, Frederik Zuiderveen. "Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence", 2021, 12-13.

O AIA engenhado pela União veio, de diversas maneiras, contribuir com a diminuição da discriminação que é operada pelo uso da IA ao relevar a absoluta proteção dos direitos humanos e fundamentais e por prever, explicitamente a proibição, o controle e a verificação de práticas discriminatórias.

Relativamente as técnicas de reconhecimento facial, conseguimos perceber o quanto a UE levou a sério a possibilidade desta ter efeitos discriminatórios, proibindo o seu uso em sistemas de identificação biométricos em espaços acessíveis ao público, quando tais sistemas sejam utilizados em tempo real. Como comprovado e demonstrado ao longo deste a partir de inúmeros exemplos, essa nova tecnologia já foi alvo de exemplos concretos de discriminação perante pessoas não brancas, concretizando a prisão ilegal de pessoas por erros da máquina.

Ao tratarmos de SIBD que não sejam implementados em tempo real, o regulamento propõe que tais sistemas devam ser considerados de risco elevado, pelo que devem seguir uma série de requisitos para a sua utilização. Um desses requisitos diz respeito a práticas adequadas de governação e gestão dos dados de modelos que utilizem técnicas que envolvam o treino de modelos de dados[451] (como é o caso das TRF). Para tal, o artigo f) impõe que para esses sistemas possam ser utilizados tem de haver um "exame em vista de possíveis viéses que provavelmente afetam a saúde e segurança das pessoas, impactam negativamente os direitos fundamentais ou levam a discriminação proibida pelo direito da União, especialmente quando as saídas de dados influenciam as entradas para operações futuras ('loops de retroalimentação') e medidas apropriadas para detectar, prevenir e mitigar possíveis viéses.". Já o artigo f) a) sugerido pelo Parlamento ainda impõe que se tome medidas adequadas para detectar, prevenir e mitigar possíveis vieses.

Outro aspecto relevante, destacado por MICHAEL VEALE e FREDERICK ZUIDERVEEN BORGESIUS, é a permissão concedida pelo AIA aos provedores de sistemas de IA de alto risco para processarem categorias especiais de dados pessoais, visando à detecção e correção de vieses negativos. Essa permissão possibilita que os provedores tenham conhecimento das características protegidas das pessoas e comunidades afetadas, de maneira excepcional, sendo

[451] Conforme impõe o Aritgo 10º do AIA.

que esta exceção não é permitida pelo RGPD, por exemplo.[452] Esta provisão está enquadrada no artigo 10º nº5 do regulamento e impõe as garantias apropriadas para os direitos e liberdades fundamentais das pessoas naturais, incluindo limitações técnicas sobre a reutilização e uso de segurança e privacidade de ponta, sendo que os provedores que recorrerem a essa disposição devem elaborar documentação explicando por que o processamento de categorias especiais de dados pessoais foi necessário para detectar e corrigir viéses.

Por fim, o regulamento ainda contém obrigações relacionadas à precisão, robustez e cibersegurança dos sistemas de IA, com uma especial atenção à discriminação à medida que os sistemas aprendam e ao uso de *machine learning* como impõe o artigo 15º, nº3.

Por conseguinte, ficou claro que o AIA proporcionou um arcabouço legal mais abrangente e rigoroso para mitigar a discriminação causada por sistemas de IA, com um enfoque na proteção dos DH e DF, proibindo certas práticas comprovadas como discriminatórias e estabelecendo requisitos importantes na governança e gestão de dados, que impõe uma maior qualidade e diversidade na base de dados a serem utilizadas por tais sistemas. A partir disso conseguimos verificar que a UE conseguiu, em certa parte, demonstrar seu compromisso em lidar de forma eficaz e proativa com este desafio decorrente do uso da IA. Contudo, algumas preocupações relativas à possibilidade da preservação do racismo algorítmico permanecem.

Primeiramente podemos citar o fato de que as vítimas de discriminação de inteligência artificial enfrentariam desafios profundos para detectar e comprovar (*prima facie*) a discriminação. Sem pontos de referência (comparativos) e devido à "velocidade, escala e níveis de complexidade que desafiam a compreensão humana", as decisões algorítmicas podem parecer legítimas e a vítima pode nem mesmo perceber a discriminação em primeiro lugar,[453] sendo que mesmo que a vítima suspeitasse de discriminação, as evidências das decisões algorítmicas ficam sob posse do operador ou fornecedor e, portanto, provavelmente inacessíveis à vítima.

Também elucidamos o fato de que algoritmos são pouco inteligíveis para não especialistas, como vítimas, juízes e legisladores. Alguns sistemas de inteligência artificial são até mesmo

[452] VEALE, Michael / BORGESIUS, Frederik Zuiderveen. “Demystifying the Draft EU Artificial Intelligence Act”, 2022, 7.
[453] WATCHER, Sandra / MITTELSTADT, Brent / RUSSEL, Chris. “Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI”, 6 e 10.

"não decomponíveis" (fenômeno da "caixa preta") e desafiam o raciocínio do senso comum, impossibilitando a detecção de decisões discriminatórias ou a compreensão da funcionalidade técnica.[454]

Além disso, os requisitos que possam impedir os sistemas de IA de operarem uma discriminação algorítmica estão, majoritariamente, reservados para os sistemas de alto risco, pelo que aqueles que não se enquadrem neste parâmetro não dispõem destas condições. Este é o exemplo das TRF para autenticação, ou seja, aquelas utilizadas para acederem a certos locais, para realizarem check in e controle de passaportes em aeroportos, para utilização de filtros faciais, desbloqueio de smartphones, autorizações em serviços financeiros, verificação de identidade em serviços governamentais, entre outros. Por mais que a consequência destes erros não seja tão gravosa como um falso positivo que dê voz de prisão a uma pessoa que não cometeu nenhum crime pelo erro de um sistema de reconhecimento facial, esta prática ainda consiste em um tipo de discriminação, através de microagressões que constrangem , oprimem e violentam as pessoas de diferentes raças, etnias, sexualidade e gênero.  Esta prática pode levar àquilo que TARCÍZIO SILVA propõe como exclusão ou isolamento, ou seja, é um tipo de racismo que impõe que determinado grupo não se sinta pertencente nas relações interpessoais, educacionais ou laborais, e em outros âmbitos também.[455]

Para a superação destes desafios expostos, diferentes abordagens foram esquematizadas por académicos ao redor do globo. Alguns académicos recomendam que "os legisladores nacionais devem manter ou introduzir disposições gerais de não discriminação que possam atuar como rede de segurança", para casos em que o tratamento diferencial não é abrangido por leis gerais (Artigo 21º da Carta) ou específicas de antidiscriminação, mas parece injusto e problemático.[456] Outra solução passaria pelos órgãos nacionais de igualdade também podem desempenhar um papel importante no apoio a reivindicações individuais, na iniciativa de ações coletivas e na chamada de atenção do legislador para a questão.[457]

---

[454] *Ib.,* 12.
[455] SILVA, Tarcízio. "Racismo Algorítmico: Inteligência Artificial e discriminação nas redes digitais", 36.
[456] GERARDS, Janneke / BORGESIUS, Frederik Zuiderveen. "Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence", 67.
[457] XENIDIS, Raphaele / SENDEN, Linda. "EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination", 2020, 27.

Tendo em vista que a IA já é realidade e está a minar todos os campos da nossa sociedade, revelando-se num cenário inevitável, a criação de uma legislação europeia de caráter vinculativo que aborde a problemática do racismo algorítmico poderia ser uma medida efetiva para fortalecer ainda mais a proteção das pessoas contra os impactos discriminatórios dos sistemas de IA. Embora o AIA já tenha como objetivo prevenir a discriminação e garantir a conformidade ética dos sistemas de IA, uma legislação específica voltada para o combate ao racismo algorítmico poderia trazer benefícios adicionais. Uma legislação europeia nesse sentido poderia estabelecer diretrizes claras e vinculativas para a detecção, prevenção e mitigação do racismo algorítmico. Isso poderia incluir requisitos mais rigorosos de transparência e responsabilidade para os provedores de sistemas de IA, bem como a definição de salvaguardas específicas para mitigar o risco de viés racial nos algoritmos.

Foram realizados avanços significativos, porém, há obstáculos pendentes que demandam uma abordagem séria e comprometida, a fim de evitar que a discriminação presente em nossa sociedade se propague para o ambiente digital. A conscientização e ação contínua são essenciais para enfrentar esses desafios e garantir um espaço virtual mais inclusivo e igualitário.

## *4.* DA UNIÃO EUROPEIA PARA O MUNDO: A ESPERANÇA DO "EFEITO CASCATA" DO *ARTIFICIAL INTELLIGENCE ACT*

A UE e o CoE têm sido pioneiros na promoção e proteção dos direitos humanos, liberdades fundamentais e preservação ambiental. Seu compromisso com esses valores tem tido um impacto significativo não apenas no continente europeu, mas também globalmente. A adoção e implementação de legislações que abranjam essas perspectivas são cruciais para garantir uma sociedade justa e sustentável, além do reforço dos importantes valores democráticos.

A UE desempenhou um papel fundamental no avanço dos direitos humanos e liberdades fundamentais por meio de seu abrangente arcabouço jurídico. A Carta dos Direitos Fundamentais da União Europeia destaca-se como um farol de proteção, consagrando uma ampla gama de direitos civis, políticos, econômicos e sociais. Suas disposições servem como

uma força orientadora na elaboração de legislação e políticas nos EM da UE, promovendo uma abordagem consistente e harmonizada para a proteção dos direitos fundamentais.

Uma legislação exemplar que ilustra o compromisso da UE com os direitos humanos é o RGPD, já citado previamente neste texto. Este regulamento, que entrou em vigor em 2018, estabelece princípios sólidos de proteção de dados e direitos para os indivíduos. Ele estabelece padrões elevados para o processamento de dados pessoais, garantindo transparência, consentimento e responsabilidade por parte dos controladores e processadores de dados. Essa legislação não apenas teve um impacto transformador na privacidade e proteção de dados dentro da UE, mas também inspirou outras nações a adotarem legislações semelhantes, reconhecendo a importância de salvaguardar as informações pessoais das pessoas na era digital.

Um exemplo concreto da relevância do RGPD em outros países, é do caso brasileiro na concretização da LGPD. Como pontuam MANUEL DAVID MASSENO, GUILHERME MAGALHÃES MARTINS E JOSÉ LUIZ DE MOURO FALEIROS JÚNIOR "a LGPD tem sido reiteradamente exposta como sendo uma "espécie de projeção" do RGPD na terra de Vera Cruz (...) sendo que até a própria *occasio legis* seria suscetível de o demonstrar, pela coincidência da entrada em vigor do RGPD, no final de maio de 2018, com a aceleração do processo legislativo no Congresso brasileiro, depois de anos de hesitações na opção entre o "modelo norte-americano", de fragmentação legislativa vertical e aplicação judiciária a posteriori, e o "modelo europeu", prevalecente."[458]

Além disso, o CoE, tem sido uma força motriz na proteção dos direitos humanos e liberdades fundamentais em seus Estados-membros. A CEDH, supervisionada pelo CoE, é um pilar do direito dos direitos humanos. Sua proteção abrangente dos direitos civis e políticos, incluindo a proibição de tortura, liberdade de expressão e direito a um julgamento justo, influenciou sistemas jurídicos em todo o mundo. A CEDH serve como um instrumento vital para que os indivíduos afirmem seus direitos e busquem reparação por violações, promovendo o desenvolvimento da jurisprudência dos direitos humanos em seu próprio tribunal, o TEDH.

[458] MASSENO, Manuel David / MARTINS, Guilherme Magalhães / FALEIROS JÚNIOR, José Luiz de Moura. " A segurança na proteção de dados: entre o RGPD Europeu e a LGPD brasileira" , 2020, 3.

Perante estes exemplos, podemos afirmar que o compromisso da UE com a proteção dos direitos humanos, liberdades fundamentais estabeleceu um precedente para nações ao redor do mundo. A adoção de legislações alinhadas com esses princípios não apenas protege a dignidade e os direitos inerentes dos indivíduos, mas também contribui para o desenvolvimento de uma sociedade global justa, sustentável e inclusiva.

Desta forma, podemos afirmar com facilidade, que a par do AIA, a UE desempenha um papel pioneiro e crucial ao implementar este regulamento sobre IA, adotando abordagens centradas na preservação dos direitos humanos e buscando a participação ativa da sociedade civil na construção de legislações relacionadas. À medida que a UE assume a liderança nessa área, é fundamental que este regulamento seja amplamente reconhecido como um modelo a ser seguido por outras nações ao redor do mundo.

No que toca a relevante proibição do uso de TRFs para SIBD em tempo real em locais de acesso público, bem como a restrição rigorosa do uso desses sistemas em situações *ex post*, enfatiza-se a importância da preservação da privacidade e da não discriminação. Países como o Brasil e os Estados Unidos, onde o uso excessivo desses sistemas é observado, devem prestar especial atenção a essa proibição, reconhecendo os danos efetivos que eles causam à sua população, tanto em termos de vigilância em massa quanto em casos concretos de prisões injustas decorrentes de erros cometidos pela "neutralidade" das máquinas.

A influência da UE na regulamentação da IA pode contribuir para um ambiente global mais ético e responsável, promovendo a harmonização das práticas e garantindo que os direitos humanos sejam preservados em face do rápido avanço tecnológico. Ao adotar uma abordagem que busca o equilíbrio entre inovação e proteção dos direitos fundamentais e humanos, a UE estabelece um importante precedente que pode inspirar e guiar outras nações na criação de suas próprias legislações sobre a IA

## CONSIDERAÇÕES FINAIS

Diante do exposto, é inegável a magnitude dos avanços tecnológicos e a relevância da IA na moldagem do comportamento da sociedade contemporânea. A ascensão de tecnologias

de reconhecimento facial no âmbito da identificação biométrica em espaços públicos tem suscitado debates acalorados, trazendo à tona questões fundamentais relacionadas à privacidade, proteção de dados e não discriminação.

Para compreender plenamente os impactos dessas tecnologias, torna-se imperativo compreender o funcionamento peculiar e distinto da IA. Através da análise de grandes volumes de dados, a IA é capaz de aprender padrões e comportamentos humanos, sendo assim capaz de tomar decisões autônomas. Esse avanço técnico proporciona às máquinas uma sofisticação que, em muitos aspectos, supera a capacidade humana. Contudo, a aplicação desse conhecimento exige cautela, especialmente quando se trata de vigilância em massa baseada em reconhecimento facial.

Nesse contexto, é inevitável fazer uma reflexão sobre o mundo distópico apresentado por George Orwell em sua obra "1984". As tecnologias de reconhecimento facial impõem à sociedade uma sensação de vigilância constante, estabelecendo um ambiente permeado pelo medo e promovendo uma política de controle exacerbado. Regimes autoritários ao redor do mundo já fazem uso dessa tecnologia, exacerbando as preocupações com relação aos direitos fundamentais dos cidadãos.

É importante destacar que essas tecnologias têm um efeito altamente negativo no direito à privacidade, à proteção de dados e à não discriminação. Ao coletar e analisar dados biométricos de forma indiscriminada, as ferramentas de reconhecimento facial violam a intimidade e a esfera pessoal de cada indivíduo. Além disso, a falta de regulamentação adequada possibilita o uso discriminatório dessas tecnologias, exacerbando desigualdades sociais já existentes.

A ausência de instrumentos legislativos "*hard law*" voltados especificamente para essa problemática é preocupante, tal lacuna expõe os cidadãos a um cenário de incerteza e vulnerabilidade, já que não há um quadro legal claro que proteja efetivamente seus direitos. Embora diretrizes e recomendações tenham sido estabelecidas, principalmente na Europa, elas não têm sido suficientes para conter o uso indiscriminado das tecnologias de reconhecimento facial, especialmente por parte das autoridades policiais. Nesse sentido, é válido ressaltar o papel desempenhado pelo RGPD e pela LED, que solucionam algumas questões sobre o processamento de dados pessoais, com ênfase nos dados biométricos.

Ao examinar a aplicação dessas tecnologias em diferentes países, notamos abordagens distintas. O Brasil, a China e os Estados Unidos têm utilizado amplamente essas tecnologias, enquanto a Europa tem adotado uma postura mais restritiva. No entanto, mesmo com legislações mais avançadas, o problema persiste, exigindo ações mais contundentes e abrangentes.

Nesse contexto, destaca-se o marco legislativo representado pelo AIA da UE Essa legislação propõe soluções para as preocupações suscitadas, como a proibição de sistemas de identificação biométrica à distância em tempo real e a imposição de restrições significativas a esses sistemas em casos *ex post.* Embora promissor, é importante salientar que esse documento ainda não está em vigor, deixando-nos vulneráveis à possibilidade de um controle estatal e privado indiscriminado de nossos rostos até lá.

Por fim, é fundamental reconhecer e saudar o papel desempenhado pela sociedade civil, representada por iniciativas como a Amnistia Internacional, a EDRI e, principalmente, a Reclaim your Face. Essas organizações desempenharam um papel determinante na proibição de sistemas de identificação biométrica à distância em tempo real, evidenciando que o poder emana do povo e que este deve ser sempre consultado em decisões que afetem diretamente suas vidas.

Diante do exposto, é inegável a necessidade de um debate jurídico abrangente e a adoção de medidas efetivas para garantir o respeito aos direitos fundamentais dos indivíduos no contexto do novo estado de vigilância baseado em tecnologias de reconhecimento facial. Somente com a participação ativa da sociedade e a implementação de regulamentações adequadas poderemos mitigar os riscos e preservar os valores democráticos que sustentam nossas sociedades.

No entanto, a simples compreensão dos avanços tecnológicos e dos riscos inerentes não é suficiente. É necessário estabelecer um equilíbrio entre a utilização dessas tecnologias e a proteção dos direitos individuais. Para isso, é essencial que as legislações acompanhem o ritmo acelerado da evolução tecnológica, proporcionando uma base sólida para a regulamentação dessas práticas, sendo que o desafio reside em encontrar soluções que permitam o uso responsável e ético das tecnologias, garantindo a proteção dos direitos fundamentais dos cidadãos.

É imprescindível, portanto, que os legisladores atuem de forma proativa e desenvolvam marcos regulatórios sólidos e atualizados, que abordem de maneira específica as questões

relacionadas ao uso de tecnologias, em específico àquelas que utilizem do reconhecimento facial. Essas legislações devem ser pautadas pelos princípios fundamentais de privacidade, proteção de dados e não discriminação, garantindo que os direitos dos cidadãos sejam respeitados e preservados.

Em suma, o novo estado de vigilância baseado em tecnologias de reconhecimento facial representa um desafio significativo para o sistema jurídico. A evolução tecnológica acelerada demanda uma resposta efetiva e equilibrada, que proteja os direitos fundamentais dos indivíduos sem comprometer o progresso e os benefícios trazidos pela inovação. Somente por meio do engajamento ativo de todos os atores envolvidos, desde os legisladores até a sociedade civil, poderemos alcançar um equilíbrio adequado e garantir um futuro em que a tecnologia seja utilizada para o bem comum, respeitando os valores democráticos, os direitos humanos e fundamentais.

## BIBLIOGRAFIA


ABIKO, Kenya Araújo et al., "Urbanismo: História e Desenvolvimento" in *disciplinas USP*, 1995, disponível em: <https://edisciplinas.usp.br/pluginfile.php/4405055/mod_resource/content/2/urbanismo-historiaedesenvolvimento.pdf> consultado em 13 de novembro de 2022.

ACCESS NOW. "Historic vote in the European Parliament: dangerous AI surveillance banned, but not for migrant people at the borders" in *Press Releases Access Now*, 2023. Disponível em https://www.accessnow.org/press-release/historic-vote-in-the-european-parliament-dangerous-ai-surveillance-banned-but-not-for-migrant-people-at-the-borders/ Acessado em 16 de junho de 2023.

AGENCIA ESPAÑOLA PROTECCÍON DATOS - AEDP. "Procedimiento No: PS/00120/2021", 2021. Disponível em https://www.aepd.es/es/documento/ps-00120-2021.pdf Acessado em 01 de maio de 2023.

ALMEIDA, Eduarda Costa. "Reconhecimento facial e segurança pública: como garantir a proteção de dados pessoais e evitar os riscos da tecnologia" Brasília: ANPR, 2020.

AMAZON WEB SERVICES "What is Amazon Recognition", 2021. Disponível em: https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html acessado em 18 de fevereiro de 2023.

AMNISTIA INTERNACIONAL. "Amnesty International response to the EU's proposal for an Artificial Intelligence Act ("AIA")", 2021. Disponível em https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665634_en Acessado em 22 de maio de 2023.

AMNISTIA INTERNACIONAL. "EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk" in *Amnesty International News*, 2023. Disponível em https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/ Acessado em 15 de junho de 2023.

AMNISTIA INTERNACIONAL. "EUA: Tecnologia de reconhecimento facial reforça policiamento discriminatório" in *Amnistia Internacional Notícias*, 2022. Disponível em https://www.amnistia.pt/eua-reconhecimento-facial-policiamento-discriminatorio/ Acessado em 4 de março de 2023.

ANTUNES, Henrique Sousa. "Direito e Inteligência Artificial", Porto: Universidade Católica Editora, 2020.

ARAÚJO FARIAS, James Magno, "Direito, Tecnologia e Justiça Digital: O uso de ferramentas digitais em busca da razoável duração do processo em Portugal e no Brasil" in *DDIR - Teses de Doutoramento,* 2022, disponível em: <http://hdl.handle.net/11144/5395> consultado em 13 de novembro de 2022.

ARISTÓTELES. “Política de Aristóteles”, São Paulo: Martin Claret, 2003.

ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 03/2012 on developments in biometric technologies” adotado em 27 de abril de 2012 disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf Acessado em 05 de dezembro de 2023.

ARTICLE 29 DATA PROTECTION WORKING PARTY. “Opinion 02/2012 on facial recognition in online and mobile services” adotado em 22 de março de 2012 disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf Acessado em 05 de dezembro de 2023.

AVAAZ THE WORLD IN ACTION. “Avaaz Feedback on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts”, 2021. Disponível em https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665625_en Acessado em 22 de maio de 2023.

BBC NEWS STAFF. “2,000 wrongly matched with possible criminals at Champions League” in *BBC News*, 2018. Disponível em https://www.bbc.com/news/uk-wales-south-west-wales-44007872 Acessado em 26 de abril de 2023.

BELCHIOR, Wilson Sales. “Artificial Intelligence, OECD principles and recommendations (Part I)” in *Blog Rocha Marinho e Sales*, 2021. Disponível em https://rms.adv.br/en/rms-noticias/direito-digital/inteligencia-artificial-principios-e-recomendacoes-da-ocde-parte-i/ Acessado em 13 de março de 2023.

BENEDEK, Wolfgang. “Compreender os Direitos Humanos - Manual de educação para os direitos humanos” (trad. por Vital Moreira e Carla de Marcelino Gomes), Coimbra: Coimbra Editora, 2012.

BERTUZZI, Luca. “AI regulation filled with thousands of amendments in the European Parliament” in *Euractiv*, 2022. Disponível em https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/ Acessado em 06 de junho de 2023.

BERTUZZI, Luca. “EU Council presidency pitches significant changes to AI Act proposal” in *EURACTIV*, 2021. Disponível em https://www.euractiv.com/section/digital/news/eu-council-presidency-pitches-significant-changes-to-ai-act-proposal/ Acessado em 23 de maio de 2023.

BERTUZZI, Luca. “US obtains exclusion of NGOs from drafting AI treaty” in *EURACTIV,* 2023. Disponível em: https://www.euractiv.com/section/digital/news/us-obtains-exclusion-of-ngos-from-drafting-ai-treaty/ Acessado em 21 de março de 2023.

BETÂMIO DE ALMEIDA, Alfredo. “A Privacidade: Um enquadramento geral do conceito e levantamento de questões” in *Política do medo ou o mundo de hoje entre a privacidade e a segurança*, Porto: Universidade Católica Editora, 2021.

BILLINGTON, James. “Panasonic facial recognition in use at Brøndby Stadium” in *Stadia Magazine*, 2019. Disponível em https://www.stadia-magazine.com/news/security-ticketing-access-control/panasonic-facial-recognition-in-use-at-brondby-stadium.html Acessado em 24 de abril de 2023.

BORAL, Masha. “EU Parliament approves AI Act amid heated biometrics debates” in *Biometric Update*, 2023. Disponível em https://www.biometricupdate.com/202306/eu-parliament-approves-ai-act-amid-heated-biometrics-debates Acessado em 16 de junho de 2023.

BRAJKOVIC, Jelena. “Council of Europe’s useful guidance concerning facial recognition” in *Lexology,* 2021. Disponível em https://www.lexology.com/library/detail.aspx?g=c068fce0-e8fa-45fa-b90a-5296a78e2fc8 Acessado em 20 de março de 2023.

BRANDÃO, Hemerson. “As cidades mais vigiadas por câmeras no mundo; poucas são do Brasil” in *Giz Brasil, UOL,* 2022. Disponível em https://gizmodo.uol.com.br/as-cidades-mais-vigiadas-por-cameras-no-mundo-poucas-sao-do-brasil/ Acessado em 14 de maio de 2023.

BUOLAMWINI, Joy. ““Artificial Intelligence Has a Problem With Gender and Racial Bias. Here’s How to Solve It” in *Time*, 2019. Disponível em: https://time.com/5520558/artificial-intelligence-racial-gender-bias/ Acessado em 18 de fevereiro de 2023.

BUYERS, John. “Artificial Intelligence – the practical legal issues”, 2ª edição, Law Brief Publishing*,* 2021.

CAIXETA, Izabella. “Foto de Michael B. Jordan aparece entre suspeitos de chacina” in *Estado de Minas*, 2022. Disponível em https://www.em.com.br/app/noticia/diversidade/2022/01/07/noticia-diversidade,1336086/foto-de-michael-b-jordan-aparece-entre-suspeitos-de-chacina.shtml Acessado em 24 de fevereiro de 2023.

CÂMARA DE DEPUTADOS. “PROJETO DE LEI N.º 3.069, DE 2022 (Do Sr. Subtenente Gonzaga)” in *DESPACHO: ÀS COMISSÕES DE: SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO E CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (MÉRITO E ART. 54, RICD)*, 2022. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2244098 Acessado em 03 de maio de 2023.

CANOTILHO, Mariana. “O princípio constitucional da proporcionalidade e o seu lugar na metódica constitucional: breves apontamentos a propósito da metáfora da balança” in O Princípio da Proporcionalidade, XIII Encontro de professores de Direito Público (org. Dulce Lopes, Francisco Pereira Coutinho, Catarina Santos Botelho), Coimbra: Instituto Jurídico, 2021.

CASTELLS, Manuel. “A Sociedade em rede”, Volume I, 8ª edição, São Paulo: Paz e Terra, 1999.

CDT Europe. “Facial recognition briefing Paper: The Human Rights Risks of Facial Recognition AI Tech in Policing and Immigration Must be Properly Recognised in the EU AI Act”, 2023.

CISCO. “A empresa que simbolizou a primeira grande onda da internet aponta para uma nova revolução de negócios baseada nas comunidades e na colaboração online” in *Revista Exame,* 2008. Disponível em https://www.cisco.com/web/BR/solucoes/tele_noticias.html?sid=167400_1 Acessado em 01 de dezembro de 2023.

COMISSÃO EUROPEIA. “Artificial intelligence act in a Europe Fit for the Digital Age”, 2023. Disponível em https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence?sid=7001 Acessado em 06 de junho de 2023.

COMISSÃO EUROPEIA. “Comunicação da Comissão: Inteligência artificial para a Europa {SWD(2018) 137 final}”, Bruxelas, 2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A52018DC0237 Acessado em 07 de abril de 2023.

COMISSÃO EUROPEIA. “LIVRO BRANCO sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança”, 19 de fevereiro de 2020.Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0065 Acessado em 05 de dezembro de 2023.

COMISSÃO EUROPEIA. “O que são dados abertos?” in *data.europa academy*, 2020. Disponível em https://data.europa.eu/pt/dataeuropa-academy/what-open-data Acessado em 02 de dezembro de 2022.

COMISSÃO EUROPEIA. “O que são dados pessoais?” in *Reforma das regras de proteção de dados da UE*, 2019. Disponível em https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_pt acessado em 06 de dezembro de 2022.

COMISSÃO EUROPEIA. “Orientações éticas para uma IA de confiança” in *Publications Office*, 2019. Disponível em https://data.europa.eu/doi/10.2759/2686 Acessado em 08 de abril de 2023.

COMISSÃO EUROPEIA. “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS - Draft AI Act”, 2021. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 Acessado em 13 de novembro de 2022.

COMISSÃO EUROPEIA. “Regulatory framework proposal on artificial intelligence”, 2021. Disponível em https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai Acessado em 18 de maio de 2023.

COSTA, Ramon Silva / OLIVEIRA, Samuel Rodrigues de, "O uso de Tecnologias de Reconhecimento Facial em Sistemas de Vigilância e Suas Implicações no Direito à Privacidade" in *Revisto de Direito, Governança e Novas Tecnologias*, 2020.

COULDRY, Nick, CAMPANELLA, Bruno. "Nick Couldry: Do mito do centro mediado ao esvaziamento do mundo social - as mídias e o processo de ratificação da sociedade" in *Matrizes,* volume 13, número 2, Universidade de São Paulo, 2019, disponível em: https://doi.org/10.11606/issn.1982-8160.v13i2p77-87 consultado em 14 de maio de 2023.

COUNCIL OF EUROPE - CoE. "Convenção 108+ Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal", 2018. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2 Acessado em 19 de março de 2023.

COUNCIL OF EUROPE - CoE. "Guidelines on facial recognition", 2021. Disponível em https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html# Acessado em 20 de março de 2023.

COUNCIL OF EUROPE - CoE. "Guidelines on Facial Recognition", 2021. Disponível em https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 Acessado em 09 de abril de 2023.

COUNCIL OF EUROPE - CoE. "Recommendation 2102 (2017): Technological convergence, artificial intelligence and human rights", 2017. Disponível em: https://ccdcoe.org/uploads/2019/09/CoE-171017-Reply-to-Recommendation-on-technological-convergence-AI-and-human-rights.pdf Acessado em 18 de março de 2023.

COUNCIL OF EUROPE - CoE. "Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling", 2021. Disponível em https://rm.coe.int/0900001680a46147 Acessado em 21 de março de 2023.

COUNCIL OF EUROPE - CoE. "Resolution 2045(2015) Mass surveillance", 2015. Disponível em http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en Acessada em 18 de março de 2023.

COUNCIL OF EUROPE - CoE. "REVISED ZERO DRAFT [FRAMEWORK] CONVENTION ON ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW", 2023. Disponível em https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f Acessado em 22 de março de 2023.

COUNCIL OF EUROPE. "Facial recognition: strict regulation is needed to prevent human rights violations" in *Full News Council of Europe*, 2021. Disponível em https://www.coe.int/en/web/portal/-/facial-recognition-strict-regulation-is-needed-to-prevent-human-rights-violations- Acessado em 20 de março de 2023.

COUNCIL OF THE EUROPEAN UNION, "Council Directive 2000/43/ EC" divulgada em 29 de junho de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0043 Acessada em 21 de fevereiro de 2023

COUNCIL OF THE EUROPEAN UNION. “Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights” in Council of the EU *Press releases*, 2022. Disponível em https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ Acessado em 07 de junho de 2023.

COUNCIL OF THE EUROPEAN UNION. “Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text”, 2021. Disponível em https://www.kaizenner.eu/post/aiact-part3 Acessado em 23 de maio de 2023.

COUNCIL OF THE EUROPEAN UNION. “Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach”, 2022. Disponível em https://www.kaizenner.eu/post/aiact-part3 Acessado em 02 de Janeiro de 2023.

COUTINHO, Clara. “Sociedade da informação, do conhecimento e da aprendizagem: Desafios para a educação no século XXI”, in *Revista da Educação* Volume XVIII, nº1, 2011.

CREEMERS, Rogier. “China’s Social Credit System: An Evolving Practice of Control”, Leiden: Leiden University - Leiden Institute for Area Studies, 2018. Disponível em: https://deliverypdf.ssrn.com/delivery.php?ID=207103102008007121085024004094084077015002001000090086121025079112086090029102095091030096049125038001052021086099029097119003046002046043009067000119072102120117111068050057068083111091112101105109101113120123125121089110071004091102104115117105007065&EXT=pdf&INDEX=TRUE

DARWIN, Charles “A Origem das Espécies”, Londres, 1859.

DATTA, Asit Kumar et. al. "Face Detection and Recognition - Theory and Practice". Kolkata, India: Future Institute of Engineering and Management. Boca Raton, London, New York: CRC Press, 2015.

DE SOUZA, Alexandre Magno Antunes. “Administração Pública 4.0 - A mudança por meio da Blockchain e da Inteligência Artificial” in *Inteligência Artificial e Direito Administrativo (Coordenado por André Saddy),* Rio de Janeiro: Editora CEEJ, 2022.

DELEUZE, Gilles. “Post-Scriptum sobre as sociedades de controle”, *Conversações: 1972-1990,* Rio de Janeiro: Editora 34, 1992.

DRAKE, Nadia, “A Evolução Humana” in *National Geographic,* 2021*, d*isponível em: < https://www.natgeo.pt/historia/a-evolucao-humana > consultada em 12 de Novembro de 2020

EBERS, Martin e GAMITO, Marta Cantero. “Algorithmic Governance and Governance of Algorithms - Legal and Ethical Challenges”, Inglaterra: Springer, 2021

EBERS, Martin. “Algorithms and Law”, Inglaterra: Cambridge University Press, 2020.

EBERS, Martins. “Regulating AI and Robotics - Ethical and Legal Challenges” in EBERS, Martin. “Algorithms and Law”, Inglaterra: Cambridge University Press, 2020.

EDPB-EDPS. “Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”, 2021. Disponível em https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf Acessado em 18 de dezembro de 2022.

EPRS - EUROPEAN PARLIAMENTARY RESEARCH SERVICE. “Regulating facial recognition in the EU”, Bruxelas, 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf acessado em 2 de março de 2023.

ESCOLA DE DADOS. “Para iniciantes: O que são dados?”, 2022. Disponível em https://escoladedados.org/tutoriais/o-que-sao-dados/ Acessado em 01 de dezembro de 2022.

EUR-LEX. “O direito primário da União Europeia”, 2016. Disponível em https://eur-lex.europa.eu/PT/legal-content/summary/the-european-union-s-primary-law.html Acessado em 15 de abril de 2023.

EUROPEAN AI FORUM. “Feedback to the European Commission’s regulation proposal on the Artificial Intelligence Act”, 2021. Disponível em https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665603_en Acessado em 22 de maio de 2023.

EUROPEAN DATA PROTECTION BOARD - EDPB. “Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement”, 2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en Acessado em 21 de abril de 2023.

EUROPEAN DIGITAL RIGHTS, EDRI. “EU Parliament calls for ban of public facial recognition, but leaves human rights gaps in final position on AI Act” in *EDRI News*, 2023. Disponível em https://edri.org/our-work/eu-parliament-plenary-ban-of-public-facial-recognition-human-rights-gaps-ai-act/ Acessado em 15 de junho de 2023.

EUROPEAN PARLIAMENT. “Artificial Intelligence Act: Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))”, 2023. Disponível em https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf Acessado em 15 de junho de 2023.

EUROPEAN PARLIAMENT. “Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces” in *European Parliament's Committee on Legal Affairs and Petitions Committee*, 2021. Disponível em

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf Acessado em 05 de junho de 2023.

European Protection Data Board, EPDB. "Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo" adotada em 29 de janeiro de 2020, disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf Acessado em 05 de dezembro de 2023.

European Protection Data Board, EDPB. "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default", 2019. Disponível em https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en Acessado em 09 de abril de 2023.

EXPRESSO STAFF. "Polícia do País de Gales criticada por recorrer a reconhecimento facial em concerto de Beyoncé" in *Expresso, Blitz*, 2023. Disponível em https://expresso.pt/blitz/2023-05-19-Policia-do-Pais-de-Gales-criticada-por-recorrer-a-reconhecimento-facial-em-concerto-de-Beyonce-d799e729 Acessado em 04 de junho de 2023.

FACHINETTI, Aline Fuke / CAMARGO, Guilherme. "Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil" in *Conjur*, 2021. Disponível em: https://www.conjur.com.br/2021-jul-04/opiniao-convencao-108-relevancia-protecao-dados Acessado em 19 de março de 2023.

FARIAS, James Magno Araújo. "DIREITO, TECNOLOGIA E JUSTIÇA DIGITAL: O USO DE FERRAMENTAS DIGITAIS EM BUSCA DA RAZOÁVEL DURAÇÃO DO PROCESSO EM PORTUGAL E NO BRASIL", DDIR- Tese de Doutoramento, Lisboa: Universidade Autónoma de Lisboa, 2022.

FRA - European Union Agency for Fundamental Rights. "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 2020.

FRAZÃO, Ana. "Big data e impactos sobre a análise concorrencial." Parte I, *Jota.* Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/big-data- e-impactos-sobre-a-analise-concorrencial-29112017 Acessado em 30 outubro 2022.

G1 RIO. "Homem preso por reconhecimento fotográfico em foto 3x4 antiga deixa a cadeia no Rio" in *G1 Rio,* 2021. Disponível em https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/09/13/homem-preso-por-reconhecimento-fotografico-em-foto-3x4-antiga-deixa-a-cadeia-no-rio.ghtml Acessado em 22 de fevereiro de 2023.

GABINETE NACIONAL DE SEGURANÇA. "Despacho n.º 2705/2021" in *Diário da República nº49/2021, 2ª série*, 2021. Disponível em https://diariodarepublica.pt/dr/detalhe/despacho/2705-2021-159088948 Acessado em 24 de abril de 2023.

GASPAR, João Pedro, "O Milénio de Gutenberg: do desenvolvimento da imprensa à popularização da Ciência" in *Cultura e ciência,* 2004, disponível em: <https://iconline.ipleiria.pt/bitstream/10400.8/112/1/O%20Milénio%20de%20Gutenberg

%20-do%20desenvolvimento%20da%20Imprensa%20à.pdf> consultado em 15 de novembro de 2022.

GATES, Kelly. "Our biometric future: facial recognition technology and the culture of surveillance", New York: New York University Press, 2011.

GATES, Kelly. "The Past Perfect Promise of Facial Recognition Technology", in *Institute of Communications Research,* University of Illinois at Urbana-Champaign, 2004.

GERARDS, Janneke / BORGESIUS, Frederik Zuiderveen. "Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence" in *Colorado Technology Law Journal, forthcoming*, 2021. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3723873 Acessado em 18 de Junho de 2023.

GILLESPIE, Tarleton. "The relevance of Algorithms" in *"Media technologies: Essays on communication, materiality, and society"* Cambridge, MA: MIT Press: Virtual Books, 2014.

GODINHO, Renato Domith. "Como foi inventado o automóvel?", 2020, artigo disponível em: https://super.abril.com.br/mundo-estranho/como-foi-inventado-o-automovel/ consultado em 21 de novembro 2022.

GOODWIN, Gretta. "Facial Recognition Technology: Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees" in *Us. Government Accountability Office*, 2021. Disponível em https://www.gao.gov/products/gao-21-105309 Acessado em 03 de maio de 2023.

GOUVEIA, Luis Borges. "O Contexto do digital, a informação e a Inteligência Artificial" in *VII Jornadas Ciências Jurídicas e Tecnologias da informação: IA, desafios à ética e ao Direito*, 2022.

GRUPO DE DE TRABALHO DO ARTIGO 29º PARA A PROTEÇÃO DE DADOS - GT29. "Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)" adotada em 29 de novembro de 2017.

GUIMARÃES, Leandro. "Qual a diferença entre dado e informação? Entenda agora!" In *Know Solutions,* 2022. Disponível em https://www.knowsolution.com.br/diferenca-dado-e-informacao/ Acessado em 02 de dezembro de 2022.

HADDADIN Sami e KNOBBE Dennis. "Robotics and Artificial Intelligence - The Present and Future Vision in *Algorithms and Law,* Martin Ebers, Inglaterra: Cambridge University Press, 2020.

INSTITUTO GARAPÉ. "Reconhecimento facial no Brasil: Desde 2011 vem sendo utilizado o Reconhecimento Facial no Brasil" in *Instituto Garapé Website*, 2022. Disponível em https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ Acessado em 02 de maio de 2023.

INTERPOL, et. al. "A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations", World Economic Forum, 2022. Disponível em:

https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf Acessado em 13 de março de 2023.

JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", Bruxelas: European Digital Rights, 2020.

JAKUBOWSKA, Ella / NARANJO, Diego. "Ban Biometric Mass Surveillance - A set of fundamental rights for the European Commission and EU Member States on the use of technology for the untargeted mass processing of special categories of personal data in public spaces", Bruxelas: European Digital Rights, 2020.

KAUFMAN, Dora. "A inteligência artificial irá suplantar a inteligência humana?", São Paulo: Estação das Letras e Cores, 2018.

KISSINGER, Henry et. al. "A era da inteligência artificial e o nosso futuro humano" (traduzido por José Mendonça da Cruz) Alfragide: Dom Quixote, 2021.

KNONDE, Mutale, "Automated Anti-Blackness Facial Recognition in Brooklyn, New York" in *Harvard Kennedy School Journal of African American Policy*, 2020.

KOKOTT, Juliane / SOBOTTA, Christoph. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" in *International Privacy Law*, v. 3, issue 4, 2013. Disponível em: https://doi.org/10.1093/idpl/ipt017 Acessado em 3 de março de 2022.

KORONAIOS, Aimilios. "CCTV in public spaces: What changes does the new Presidential Decree bring?" in *Publications, TaxHeaven, Websites"*, 2020. Disponível em https://akoronaios.gr/en/cctv-in-public-spaces-what-changes-does-the-new-presidential-decree-bring/ Acessado em 02 de maio de 2023.

KORTLI, Y.; JRID, M.; AL FALOU, A.; ATRI, M. "Face Recognition Systems: A Survey." Sensors, vol. 20, no. 2, 2020. Disponível em: [https://doi.org/10.3390/s20020342].

KOUROUPIS, Konstantinos. "Facial Recognition: a challenge for Europe or a threat to human rights?" In *European Journal of Privacy Law & Technologies*, 2021.

LA QUADRATURE DU NET. "Projet de loi relatif aux Jeux Olympiques et Paralympiques de 2024 : dossier d'analyse de la vidéosurveillance automatisée", 2023. Disponível em https://www.laquadrature.net/wp-content/uploads/sites/8/2023/02/Dossier-VSA-2-LQDN.pdf Acessado em 02 de maio de 2023.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET - LAPIN. "Relatório: Vigilância automatizada: uso de reconhecimento facial pela Administração Pública no Brasil", 2021. Disponível em https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/ Acessado em 02 de maio de 2023.

LEÃO, Anabela Costa. "A Carta dos Direitos Fundamentais da União Europeia: Protegendo os Direitos a um nível Multidimensional" in *Revista da Faculdade de Direito do Porto*, 2006.

LI, Stan Z.; JAIN, Anil K. "Handbook of Face Recognition". London: Springer, 2011.

LIBERTY HUMAN RIGHTS. “Legal Challenge: Ed Bridges v. South Wales Police, 2020. Disponível em https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/ Acessado em 21 de abril de 2023.

LIBERTY HUMAN RIGHTS. “Liberty wins ground-breaking victory against facial recognition tech”, 2020. Disponível em https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/ Acessado em 21 de abril de 2023.

LYDICK, Neil. “A Brief Overview of Facial Recognition”, University of Michigan, 2007 Disponível em: http://www.eecs.umich.edu/courses/eecs487/w07/sa/pdf/nlydick-facial-recognition.pdf Acessado em 3 de dezembro de 2022.

MACCIONI, Elvira. “Italy outlaws facial recognition tech, except to fight crime” in *Reuters*, 2022. Disponível em https://www.reuters.com/technology/italy-outlaws-facial-recognition-tech-except-fight-crime-2022-11-14/ Acessado em 01 de maio de 2023.

MANN, Monique; SMITH, Marcus. “Automated facial recognition technology: Recent developments and approaches to oversight” in *University of New South Wales Law Journal,* 2017.

MANNING, Jake. “The Story of CCTV in Europe, from resistance to adoption” in *Blog Calipsa*, 2021. Disponível em https://www.calipsa.io/blog/the-story-of-cctv-in-europe-from-resistance-to-adoption Acessado em 21 de abril de 2023.

MARKETS AND MARKETS. “Facial recognition Market by Component (Software Tools (3D Facial Recognition) and Services), Application (Law Enforcement, Access Control, Emotion Recognition), Vertical (BFSI, Government and Defense, Automotive), and Region . Global Forecast to 2025”, 2020. Disponível em https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html Acessado em 07 de dezembro de 2022.

MARKHIJA, Yashoda e SHARMA, Rama Shankar. “Face recognition: novel comparison of various feature extraction techniques. Harmony Search and Nature Inspired Optimization Algorithms: Theory and Applications”, in *Harmony Search and Nature Inspired Optimization Algorithms,* ICHSA, 2018.

MARQUES FARIAS, Leonel. “Uso da energia ao longo da história: evolução e perspectivas históricas”, 2011, artigo disponível em: <10.31514/rliberato.2011v12n17.p07> consultado em 18 de novembro de 2022.

Martins, L. M.*“*O direito civil à privacidade e à intimidade*.” I*n *Martins-Costa, Judith (Org.). “A reconstrução do Direito Privado”*. São Paulo: Revista dos Tribunais, 2002.

MASSENO, Manuel David / MARTINS, Guilherme Magalhães / FALEIROS JÚNIOR, José Luiz de Moura. “ A segurança na proteção de dados: entre o RGPD Europeu e a LGPD brasileira” in *Revista do CEJUR | TJSC: Prestação Jurisicional*, v.8, nº1, 2020. Disponível em https://revistadocejur.tjsc.jus.br/cejur/article/view/346/181 Acessado em 20 de junho de 2023.

MELLO, Daniel. “Justiça libera edital de câmeras com reconhecimento facial em SP” in *Agência Brasil*, 2023. Disponível em https://agenciabrasil.ebc.com.br/justica/noticia/2023-05/justica-libera-edital-de-cameras-com-reconhecimento-facial-em-sp Acessado em 05 de junho de 2023.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA/GABINETE DO MINISTRO. “Portaria nº793: Regulamenta o incentivo financeiro das ações do Eixo Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com os recursos do Fundo Nacional de Segurança Pública, previstos no inciso I do art. 7º da Lei nº 13.756, de 12 de dezembro de 2018” in *Diário Oficial da União,* ed.208, Secção 1, 2019. Disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575 Acessado em 02 de maio de 2023.

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRATICA. “Resolución de 16 de julio de 2020, de la Subsecretaría, por la que se publica el Convenio entre el Centro para el Desarrollo Tecnológico Industrial, E.P.E., y el Ministerio del Interior, relativo a la contratación precomercial de servicios de I+D en materia de seguridad en el medio rural” in *Boletín Oficial del Estado* nº198, 2020. Disponível em https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-8276 Acessado em 02 de maio de 2023.

MOBILIO, Giuseppe. “Your face is not new to me - Regulating the surveillance power of facial recognition” in *Internet Policy Review*, v.12, Issue 1, 2023. Disponível em https://policyreview.info/pdf/policyreview-2023-1-1699.pdf Acessado em 22 de abril de 2023.

MODERN DIPLOMACY. “Proposed Law Enforcement Principles on the Responsible Use of Facial Recognition Technology” in *Newsroom ModernDiplomacy*, 2022. Disponível em https://moderndiplomacy.eu/2022/11/06/proposed-law-enforcement-principles-on-the-responsible-use-of-facial-recognition-technology/ Acessado em 13 de março de 2023.

MOROZOV, Evgeny. “Big Tech: A Ascensão dos dados e a morte política”, São Paulo: UBU Editora, 2018.

MOZUR, Paul / FU, Claire / CHIEN, Amy Chang. “China usa reconhecimento facial para rastrear manifestantes contra Covid zero” in *Folha de São Paulo*, 2022. Disponível em: https://www1.folha.uol.com.br/mundo/2022/12/china-usa-reconhecimento-facial-para-rastrear-manifestantes-contra-covid-zero.shtml Acessad em 4 de março de 2023.

NICOLÁS, Elena Sánchez. “Pandemic speeds calls for ban on facial recognition” in *euobserver*, 2020. Disponível em https://euobserver.com/health-and-society/148387 Acessado em 04 de março de 2023.

Norvig, quoted by Scott Cleland, Google’s “Infringenovation” Secrets, Forbes, October 3, 2011, https://www.forbes.com/sites/scottcleland/2011/10/03/googles-infringenovation-secrets/#78a3795430a6. Acessado em 16 de novembro de 2022.

O'NEIL, Cathy. "Weapons of Math Destruction: how big data increases inequality and threatens democracy". New York: Crown Publishers, 2016.

OECD, “Recommendation of the Council on Artificial Intelligence”, OECD/LEGAL/0449, 2019. Disponível em https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 acessado em 17 de março de 2023.

OLIVEIRA, Samuel R. "Sorria, você está sendo filmado! Repensando direitos na era do reconhecimento facial". São Paulo: Thomson Reuters, 2021.

ORWELL, George. 1984. São Paulo: IBEP, 2003.

PACHTENBEKE, Andy Van. “UNESCO Recommendation on the Ethics of Artificial Intelligence Human Rights-based & Future oriented” in *Human Rights Context*, 2022. Disponível em: https://www.humanrightsincontext.be/post/unesco-recommendation-on-the-ethics-of-artificial-intelligence-human-rights-based-future-oriented Acessado em 17 de março de 2023.

PARLAMENTO EUROPEU. “Artificial Intelligence Act: lead committees to launch joint work on 25 January” in *Press room - News European Parliament,* 2022. Disponível em https://www.europarl.europa.eu/news/en/press-room/20220119IPR21312/artificial-intelligence-act-lead-committees-to-launch-joint-work-on-25-january Acessado em 06 de junho de 2023.

PARTIDO COMUNISTA PORTUGUÊS. “Declaração de voto sobre a Proposta de Lei n.º 111/XIV sobre videovigilância”, 2021. Disponível em https://www.pcp.pt/declaracao-de-voto-sobre-proposta-de-lei-no-111xiv-sobre-videovigilancia Acessado em 24 de abril de 2023.

PASCU, Luana. “Football club Ajax Amsterdam deploys Mitek biometrics to improve online experience, privacy” in *Biometric Update,* 2019. Disponível em https://www.biometricupdate.com/201910/football-club-ajax-amsterdam-deploys-mitek-biometrics-to-improve-online-experience-privacy Acessado em 26 de abril de 2023.

PATRÃO NEVES, Maria. “Política do medo: Amigos ou inimigos? Privacidade e segurança em tempos de medo global” in *Política do medo ou o mundo de hoje entre a privacidade e a segurança*, Porto: Universidade Católica Editora, 2021.

PAUL, Kari. “'Ban this technology': students protest US universities' use of facial recognition” in *The Guardian*, 2020. Disponível em https://www.theguardian.com/us-news/2020/mar/02/facial-recognition-us-colleges-ucla-ban Acessado em 04 de março de 2023.

PENATTI, Giovana “25 anos de World Wide Web: as primeiras aparições de tudo que forma a internet hoje”, 2014, artigo disponível em: https://tecnoblog.net/especiais/25-anos-world-wide-web/“ consultado em 21 de novembro de 2022.

PIRES, Maria José Morais. “Carta Africana dos Direitos Humanos e dos Povos” in *Documentação e Direito Comparado*, nº 79/80, 1999. Disponível em http://www.dhnet.org.br/direitos/sip/africa/ua_pires_carta_africana_direitos_povos.pdf Acessado em 20 de junho de 2023.

PORTAL DE DADOS ABERTOS DA ADMINISTRAÇÃO PÚBLICA. "Sobre dados abertos" in *dados.gov*, 2020. Disponível em https://dados.gov.pt/pt/docs/about_opendata/ Acessado em 04 de dezembro de 2022.

PRIVACY INTERNATIONAL. "New UN High Commissioner report highlights the impact new technologies have on the right to protest", 2020. Disponível em https://privacyinternational.org/news-analysis/3980/new-un-high-commissioner-report-highlights-impact-new-technologies-have-right Acessado em 12 de março de 2023.

PRIVATE EQUITY WIRE. "AI Startups Raised USD734bn in Total Funding in 2020" in *Private Equity Wire*, 19 de novembro de 2020 disponível em: https://www.privateequitywire.co.uk/2020/11/19/292458/ai-startups-raised-usd734bn-total-funding-2020 acessado em 12 de novembro de 2022.

PROCURADORIA-GERAL DISTRITAL DE LISBOA. "Lei 59º/2019, de 08 de Agosto: DADOS PESSOAIS PARA PREVENÇÃO, DETEÇÃO, INVESTIGAÇÃO OU REPRESSÃO DE INFRAÇÕES PENAIS", 2019. Disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3123A0004&nid=3123&tabela=leis&pagina=1&ficha=1&so_miolo=?area=Identifica%E7%E3o%20civil%20e%20criminal&nversao=

Proposta de Lei 111/XIV/2 de 6 de novembro de 2021 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=121083 Acessado em 23 de abril de 2023.

RAINIE, Lee / FUNK, Cary / ANDERSON, Monica / TYSON, Alec. "Public more likely to see facial recognition use by police as good, rather than bad for society" in *Pew Research Center*, 2022. Disponível em https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/ Acessado em 03 de maio de 2023.

RAPOSO, Vera Lúcia. "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation" in *Information & Communications Technology Law*, 2022.

RAPOSO, Vera Lúcia. "The use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal" in *European Journal on Criminal Policy and Research*, 2022.

RECLAIMYOURFACE. *"*Football fans are being targeted by biometric mass surveillance" in *Reclaim your face News*, 2022. Disponível em https://reclaimyourface.eu/football-fans-are-being-targeted-by-biometric-mass-surveillance/ Acessado em 01 de maio de 2023.

RECLAIMYOURFACE. "No biometric surveillance for Italian students during exams" in *Reclaim your face News*, 2021. Disponível em https://reclaimyourface.eu/no-surveillance-during-exams/ Acessado em 01 de maio de 2023.

REIS, Paulo Victor Alfeo. "Algoritmos e direito", São Paulo: Almedina, 2020.

REUTERS STAFF. "French watchdog warns sports club about unlawful use of facial recognition technology" in *Reuters*, 2021. Disponível em

https://www.reuters.com/article/france-privacy-soccer-idUSL1N2KO2C6 Acessado em 26 de abril de 2023.

RODHEN, Valerio "O humano e racional na ética" in *Studio Kantiana* v.1 nº1, 1998.

RODRIGUES, Pedro Eurico, "Tecnologias na Pré História" in *Infoescola.* Artigo disponível em: https://www.infoescola.com/historia/tecnologias-na-pre-historia/ consultado em 29 de dez de 2022.

ROHE, Andersson. "O Ecossistema Chinês de vigilância e Reconhecimento Facial: ameaça ou solução tecnológica?", São Paulo: Dialética, 2022.

ROSE, Adam. "Are Face-Detection Cameras Racist?" in *Time,*2010. Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html. acessado em 20 de fevereiro de 2023.

ROXO BELTRAN, Maria Helena, et al. "A Imprensa, a Pólvora e a Bússola: ciência e técnica nas origens da ciência moderna" in *Temas: História da ciência,* Editora Livraria da Física, 2017.

RUDIGER, Francisco, "Tecnologia" em FILHO, Ciro, "Dicionário da comunicação" in *Revista e Ampliada* 2º Edição. São Paulo: Paulus, 2014.

SAITO, Vitória Hiromi. "Desafios Contemporâneos para a Tutela dos Direitos à Privacidade e aos Dados Pessoais" in *Res Severa Verum Gaudium. UFRGS*, v.5, nº2, 2021. Disponível em: https://www.seer.ufrgs.br/resseveraverumgaudium/article/viewFile/110379/61654. Acesso em: 2 de março 2022.

SANTOS, António Robalo. "Gestão estratégica: conceitos, modelos e instrumentos" Lisboa: Escolar. 2008,

SCHNEIDER, Shira. "Algorithmic Bias: A New Age of Racism" in , *Stern College for Women – Yeshiva University,* 2021. Disponível em: https://repository.yu.edu/bitstream/handle/20.500.12202/6887/Schneider%20Shira%20Algorithmic%20Bias_%20A%20New%20Age%20of%20Racism%20OA%202021April.pdf?sequence=1&isAllowed=y acessado em 24 de fevereiro de 2023.

SEGURTEC. "CCTV: tudo o que deve saber" in *Notícias Segurtec*, 2020. Disponível em https://segurtec.pt/cctv-tudo-o-que-deve-saber/ Acessado em 18 de fevereiro de 2023.

SEYLLER, Andrea D.M., "A concepção da Inteligência Artificial na administração Pública" in *Inteligência Artificial e Direito Administrativo (Coordenado por André Saddy),* Rio de Janeiro: Editora CEEJ, 2022.

SILVA, Tarcízio. "Racismo Algorítmico: Inteligência Artificial e discriminação nas redes digitais", São Paulo: Edições SESC, 2022.

SNOW, Jacob. "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots" in *American Civil Liberties Union,* 2018. Disponível em https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 Acessado em 20 de outubro de 2022.

SOUZA, Thiago. “História e Evolução dos Computadores”, artigo disponível em: https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/ consultado em 21 de novembro 2022.

STEINROOTTER, Bjorn. “The (Envisaged) Legal Framework for Commercialisation of Digital Data within the EU - Data Protection Law and Data Economic Law as a Conlficted Basis for Algorithm-Based Products and Services” in *Algorithms and Law,* Martin Ebers, Inglaterra: Cambridge University Press, 2020.

TACCA,Adriano e ROCHA Leonel. “Inteligência Artificial: Reflexos no Sistema do Direito”, in *Revista do Programa de Pós-Graduação em Direito da UFC*, Ceará, 2018.

TECMUNDO. “Reconhecimento facial erra e homem é preso injustamente nos EUA” in *Tecmundo*, 2020. Disponível em https://www.tecmundo.com.br/software/154511-reconhecimento-facial-erra-%20homem-preso-injustamente-eua.htm Acessada em 23 de fevereiro de 2023.

Texto Final e relatório da discussão e votação na especialidade da Proposta de Lei n.º 111/XIV/2ª (GOV). Disponível em: https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063484d364c793968636d356c6443397a6158526c6379395953565a4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396b4f574a6c4d6a67304d7930324e3245324c5451345a4751744f4751325969316c4d7a51355a6a4a694f44426d5a444d756347526d&fich=d9be2843-67a6-48dd-8d6b-e349f2b80fd3.pdf&Inline=true Acessado em 24 de abril de 2023.

THE GREENS/EFA. “Biometric & Behavioural Mass Surveillance in EU Member States” in *Report for the Greens/EFA in the European Parliament,* 2021. Disponível em http://extranet.greens-efa-service.eu/public/media/file/1/7297 Acessado em 01 de maio de 2023.

TURK, Matthew e PENTLAND, Alex. “Face Recognition Using Eigenfaces” in *Vision and Modeling Group, The Media Laboratory Massachusetts Institute of Technology*, 1991. Disponível em: https://sites.cs.ucsb.edu/~mturk/Papers/mturk-CVPR91.pdf Acessado em 05 de dezembro de 2022.

U.S.A. CONGRESS. “H.R.3907 - Facial Recognition and Biometric Technology Moratorium Act of 2021 (by Pramilla Jayapal)” in *117th Congress (2021,2022)*, 2021. Disponível em https://www.congress.gov/bill/117th-congress/house-bill/3907/text Acessado em 03 de maio de 2023.

UNESCO, “Recommendation on the ethics of artificial intelligence”, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000380455 Acessado em 17 de março de 2023.

UNITED NATIONS SYSTEM. “Principles for the Ethical Use of Artificial Intelligence in the United Nations System”, 2022.

UNITED NATIONS. “High Commissioner: the Human Rights Council Has Given a Disturbing Diagnosis of Human Rights Violations Occurring in the Context of Peaceful Protests” in *Press Releases Human Rights Council*, 2021. Disponível em

https://www.ohchr.org/en/press-releases/2021/09/high-commissioner-human-rights-council-has-given-disturbing-diagnosis-human?LangID=E&NewsID=27571 Acessado em 12 de março de 2023.

UNITED NATIONS. "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests: Report of the United Nations High Commissioner for Human Rights", divulgado em 24 de junho. 2020. Disponível em: https://undocs.org/A/HRC/44/24. Acessada em 12 de março 2023.

URBANO CALVÃO, Filipa. "Privacidade e segurança em tempos de medo global" in *Política do medo ou o mundo de hoje entre a privacidade e a segurança*, Porto: Universidade Católica Editora, 2021.

VALENTINA. "France becomes the first European country to legalise biometric surveillance" in *Reclaim your face News*, 2023. Disponível em https://reclaimyourface.eu/france-becomes-the-first-european-country-to-legalise-biometric-surveillance/ Acessado em 02 de maio de 2023.

VAN KOLFSCHOOTEN, Hannah. "The Council of Europe's Artificial Intelligence Convention: Implications for Health and Patients" in *Harvard Law Petrie-Flom Center*, 2023. Disponível em https://blog.petrieflom.law.harvard.edu/2023/04/18/council-of-europe-artificial-intelligence-convention/ Acessado em 02 de junho de 2023.

VEALE, Michael / BORGESIUS, Frederik Zuiderveen. "Demystifying the Draft EU Artificial Intelligence Act" in *Computer Law Review International: A Journal of Information Law and Technology,* 2022. Disponível em https://arxiv.org/abs/2107.03721 Acessado em 18 de junho de 2023.

VERASZTO, Estéfano Visconde et al. "Tecnologia: buscando uma definição para o conceito" in *Prisma* nº8, 2009, disponível em: < https://ojs.letras.up.pt/index.php/prismacom/article/view/2065/1901 > Consultado em: 09 de novembro de 2022.

VICENT, James. "NYPD used facial recognition to track down Black Lives Matter activist / Mayor Bill de Blasio says standards need to be "reassessed"" in *The Verge*, 2020. Disponível em https://reliefweb.int/report/world/high-commissioner-human-rights-council-has-given-disturbing-diagnosis-human-rights Acessado em 12 de março de 2023.

VIEIRA, Kauê. "Reconhecimento facial vira ameaça para negros: maioria entre presos" in *Hypeness,* 2021. Disponível em:https://www.hypeness.com.br/2019/11/reconhecimento-facial-vira-ameaca-para-negros-maioria-entre-presos/ acessado em 20 de fevereiro de 2023.

VON DER LEYEN, Ursula. "A Union that strives for more: My agenda for Europe" in *POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024,* 2019. Disponível em https://commission.europa.eu/system/files/2020-04/political-guidelines-next-commission_en_0.pdf Acessada em 07 de abril de 2023.

WALTER, Robert e NOVAK, Marko. "Cyber Security, Artificial Intelligence, Data Protection and the Law", Inglaterra: Springer, 2021.

WATCHER, Sandra / MITTELSTADT, Brent / RUSSEL, Chris. “Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI” in *Computer Law & Security Review,* nº 41, 2020. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922 Acessado e 18 de junho de 2023.

WESTIN, Alan Furman. “Privacy and Freedom”, Nova Iorque: Ig Publishing, 2015.

WHITMAN, James Q.. “The Two Western Cultures of Privacy: Dignity versus Liberty”, in *The Yale Law Journal*, v. 113, n. 6, 2004.

WIEWIÓROWSKI, Wojciech. “Facial recognition: A solution in search of a problem?” in *Blog European Data Protection Supervisor*, 2019. Disponível em https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en Acessado em 10 de abril de 2023.

WONG, K.L.X / DOBSON, Amy shields. “We’re Just Data: Exploring China’s Social Credit System in Relation to Digital Platform Rating Cultures in Westernised Democracies” Volume 4, Issue 2 in *SAGE Journals, 2019.* Disponível em: https://journals.sagepub.com/doi/epub/10.1177/2059436419856090

WOODWARD, John D., et al. "Biometrics: A Look at Facial Recognition". Santa Monica, CA: RAND Corporation, 2003.

WOOLACOTT, Emma. “Draft AI Act Passes, Banning Police Facial Recognition” in *Forbes*, 2023. Disponível em https://www.forbes.com/sites/emmawoollacott/2023/06/15/draft-ai-act-passes-banning-police-facial-recognition/?sh=395630c34965 Acessado em 16 de junho de 2023.

XENIDIS, Raphaele / SENDEN, Linda. “EU non-discrimination law in the era of artificial intelligence: Mapping the challenges of algorithmic discrimination” in Ulf Bernitz et al (eds), *General Principles of EU law and the EU Digital Order* (Kluwer Law International), 2020. Disponível em https://cadmus.eui.eu/bitstream/handle/1814/65845/Pre-print%2520version%2520Chapter%2520Xenidis_Senden.pdf?sequence=2&isAllowed=y Acessado em 18 de junho de 2023.

ZUBOFF, Shoshana. “A Era do Capitalismo da Vigilância - A disputa por um futuro humano na nova fronteira do poder”, Lisboa: Relógio D’Água, 2020.