UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

DANIEL DA SILVA MARQUES

O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA NO BRASIL: DESAFIOS ÉTICOS E JURÍDICOS

RIO DE JANEIRO
2021

DANIEL DA SILVA MARQUES

O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA NO BRASIL: DESAFIOS ÉTICOS E JURÍDICOS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação da Professora Dra. Kone Prieto Furtunato Cesário.

RIO DE JANEIRO

2021

CIP -Catalogação na Publicação

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a),
sob a responsabilidade de Miguel Romeu Amorim Neto – CRB - 7/6283.

DANIEL DA SILVA MARQUES

O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA NO BRASIL: DESAFIOS ÉTICOS E JURÍDICOS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob orientação da Professora Dra. Kone Prieto Furtunato Cesário.

Data da Aprovação: __/__/____.

Banca Examinadora:

_____

Orientador Profa. Dra. Kone Prieto Fortunato Cesário

_____

Prof. Carlos Augusto Thomas

Membro da Banca

_____

RIO DE JANEIRO

2021

Dedico este trabalho à minha esposa e minha pequena filha Maitê. Elas me motivam a cada dia ser uma pessoa melhor.

"A medida do amor é amar sem medida. Amor meus, pondus meum"

Santo Agostinho

RESUMO

O presente estudo pretende apresentar os desafios éticos e jurídicos no uso de algoritmos de reconhecimento facial na vigilância de massa a fim de evitar violações aos direitos humanos. O fenômeno da Cidade em sua dimensão multifacetária traz o desafio de criar políticas de segurança pública de combate ao crime sem segregar e discriminar indivíduos por motivo de raça, condição social e respeitando o devido processo legal. A segurança pública utiliza-se cada vez mais de ferramentas tecnológicas para sua atuação e observa-se ao redor do mundo uma crescente preocupação quanto à eficácia, segurança jurídica e respeito aos direitos humanos no uso do reconhecimento facial com inteligência artificial na segurança pública. Deseja-se explorar os principais desafios na utilização desta tecnologia mostrando exemplos concretos de ações contrárias aos direitos humanos e a legislação local vigente. Será considerada a hipótese de pensar em um instrumento jurídico, *Ética e Law by Design* que responda à transformação tecnológica e auxilie na criação de sistemas em que já venham inseridos com princípios que respeitem os direitos humanos e o ordenamento jurídico.

PALAVRAS-CHAVE: Inteligência Artificial. Algoritmo. Reconhecimento Facial. Direitos Humanos. Discriminação. *Law by Design.* Segurança Pública. Ética.

ABSTRACT

The present study aims to present the ethical and legal challenges in the use of facial recognition algorithms in mass surveillance in order to avoid human rights violations. The phenomenon of the City in its multifaceted dimension brings the challenge of creating public security policies to fight crime without segregating and discriminating individuals based on race, social status and respecting the due legal process. Public security is increasingly using technological tools for its performance and there is a growing concern around the world regarding efficiency, legal security and respect for human rights in the use of facial recognition with artificial intelligence in public security. The aim is to explore the main challenges in using this technology, showing concrete examples of actions contrary to human rights and current local legislation. It will be considered the hypothesis of thinking about a legal instrument, *Ethics and Law by Design* that responds to technological transformation and helps in the creation of systems in which they are already inserted with principles that respect human rights and the legal system.

KEYWORDS: Artificial Intelligence. Algorithm. Facial recognition. Human rights. Discrimination. Law by Design. Public security. Ethic

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

ABIS - Solução Automatizada de Identificação Biométrica

BBC – British Broadcasting Corporation

MIT – Massachussetts Institute of Technology

CPI – Comissão Parlamentar de Inquérito

DF – Distrito Federal

EUA – Estados Unidos da América

IBM – International Business Machines Corporation

INMETRO – Instituto Nacional de Metrologia, Qualidade e Tecnologia

LGPD – Lei Geral de Proteção de Dados

NIST - National Isntitute of Starndars and Tecnology

RF – Reconhecimento Facial

RFW - Racial Face in the Wild

STF – Supremo Tribunal Federal

UE – União Europeia

UK – United Kingdom

Sumário

INTRODUÇÃO

O uso do reconhecimento facial está em seu início e, atualmente, é uma das utilizações da Inteligência Artificial que mais pode impactar negativamente nos direitos humanos e exercício das liberdades. Apesar de algumas empresas de tecnologia terem interrompido suas pesquisas e desenvolvimento tecnológico e comercial dessa solução até uma manifestação legislativa sobre o uso delas, como mostra o caso da IBM nos EUA. Essa situação é temporária e exige uma reflexão e resposta jurídica imediata.[1]

Ainda não temos no Brasil um debate profundo, sério, interdisciplinar sobre o tema. A tecnologia está à disposição, outras empresas estão avançando em seu desenvolvimento. O momento é mais do que oportuno. É essencial que agora em seu início nos posicionemos enquanto sociedade sobre o tema a fim de proteger e promover os direitos humanos. Em breve, a inteligência artificial em suas diversas manifestações, como o reconhecimento facial, será uma das principais pautas regulatórias em nosso país e a academia deve estar preparada para oferecer estudos e pesquisas que fundamentem decisões que promovam os direitos humanos.

A tecnologia de reconhecimento traz em si diversos desafios e perigos como uso abusivo para fins de controle social, desrespeito aos direitos humanos, em especial a discriminação e preconceito social e racial.

Vivemos na Quarta Revolução Industrial, numa dimensão que o filósofo Luciano Floridi conceituará como Infoesfera, em que o valor da realidade é dado segundo o processamento das informações. Para o filósofo Floridi há um novo deslocamento do ser humano nessa nova sociedade. Na Revolução Copernicana, o ser humano não é mais centro do universo. Na Revolução Darwiniana, o ser humano não é mais o centro entre os seres vivos. Na Revolução Freudiana, o ser humano não é mais centro e motor de si mesmo.

Na Infoesfera, tudo indica que o ser humano não é mais o único agente no universo, ele é visto como um organismo feito de informação a semelhança das máquinas; essa seria a

[1] Disponível em: https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software. Acesso em: 10 de agosto de 2021.

Revolução de Turing.[2] Na Infoesfera, surge uma nova antropologia que exigirá uma nova ética e uma nova epistemologia que tenham em conta todos os entes como agentes informacionais e por consequência a criação de instrumentos jurídicos capazes de responder a essa nova configuração social.

Nessa sociedade entendida como informação, estaríamos caminhando para o que o historiador Yuval Harari chama de mundo pós-antropocêntrico. Nele a realidade é extraída a partir de um contínuo processamento de informação, realizado por agentes não humanos (Inteligência Artificial) e agentes humanos.[3]

A potencialidade da dissolução do ser humano em informação é tão grande, que Harari traz em seu livro *Homo Deus* o exemplo do Kindle. Atualmente ele já é capaz de identificar quantos livros você leu, quanto tempo demora em cada página, em que parágrafos há mais pausa. Agora imagine o seguinte cenário, onde o Kindle capta, com reconhecimento facial e sensores biométricos, a cada leitura de uma palavra, frase e parágrafo do livro suas emoções, reações biológicas, o que lhe deixou triste, o que lhe empolgou.

Nesse momento, não seria apenas você lendo o livro, mas o livro lendo você. E essas informações sendo armazenadas, utilizadas para o marketing gerar novos produtos. Mais importante ainda, o ser humano num simples ato de ler já não é o único agente.

Será que ao chegar nesse nível de interação teríamos a sensação de que nossas "almas" e identidades foram roubadas, reagindo como algumas culturas aborígines diante do primeiro contato com uma câmera de fotos ou o espelho?

---

[2] "ICTs are bringing about a fourth revolution, in the long process of reassessment of humanity's fundamental nature and role in the universe. We are not immobile, at the centre of the universe (Copernican revolution); we are not unnaturally distinct and different from the rest of the animal world (Darwinian revolution); and we are far from being entirely transparent to ourselves (Freudian revolution). ICTs are now making us realise that we are not disconnected agents, but informational organisms (inforgs), who share with other kinds of agents a global environment, ultimately made of information, the infosphere (Turing revolution)". Disponível em: http://governance40.com/wp-content/uploads/2018/12/Luciano-Floridi-The-Fourth-Revolution_-How-the-infosphere-is-reshaping-human-reality-2014-Oxford-University-Press.pdf. Acesso em 25 de julho 2020.

[3] HARARI, Yuval N. Homo Deus: uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

A lei de Moore preconiza que a cada 18 meses a capacidade de armazenamento e processamento de dados irá dobrar, enquanto o custo irá reduzir. Somando ao IOT (internet das coisas) produziremos e armazenaremos dados como nunca na história.[4]

Isso significa na prática que desde 2003, a cada dois dias armazenamos e produzimos a quantidade de dados de toda a história. Vivemos na abundância de dados e somente através de algoritmos iremos ser capazes de tratar, fazer a curadoria e extrair informações.

Para nossa sociedade a existência de algoritmos parece ser essencial. Um alerta que se dá diante dessa realidade exponencial é que podemos através de algoritmos também exponenciar preconceitos e violações aos direitos humanos. Por isso, é essencial uma reflexão jurídica profunda sobre os elementos necessários para uma utilização do reconhecimento facial que respeite, proteja e promova a dignidade da pessoa humana.

Refletir sobre ética, significa também pensar sobre os critérios que nortearão essa sociedade da informação moldada pela tecnologia para que permaneça fiel aos direitos humanos. É pensar na elaboração de mecanismos que permitam que a dignidade da pessoa humana seja protegida na mesma velocidade em que as novas tecnologias ganham escala. Se vivemos numa sociedade exponencial, como impedir que o preconceito algorítmico, o controle social e a perda da liberdade que possam advir do reconhecimento facial se perpetuem e ampliem as diferenças e injustiças sociais? Como a utilização ostensiva e sem critérios dessa tecnologia pelos órgãos de segurança pública irão impactar no ordenamento social das cidades? Teremos um aumento das diferenças sociais?

Refletir sobre ética é elaborar e possuir um arcabouço legal e jurídico que esteja em consonância com os anseios sociais e não seja sobreposto por uma sociedade da informação que coloque a dignidade humana de lado. Refletir sobre ética é também colocar os valores da dignidade humana como centro do diálogo atual e saber usufruir dos impactos positivos que as novas tecnologias também trazem.

Se o direito é um instrumento *sine qua non* para a justiça e se *ubis societas ibi jus*, é impossível que o universo jurídico não seja impactado por essa transformação, exigindo do

---

[4] MOORE, Gordon E. Cramming More Components Onto Integrated Circuits. Eletronics Magazine, n. 8, p. 33-35, abr. 1965.

direito uma nova forma de lidar com a tecnologia. Olhar e atuar juridicamente sem ter em conta que vivemos na Infoesfera conduzirá a interações jurídicas em dissonância com a realidade.

Deste modo o tema é relevante:

a) pelas manifestações crescentes e exemplos concretos em todo mundo sobre os perigos da má utilização dessa tecnologia ferindo os direitos humanos, gerando preconceitos e discriminações;

b) pois trata-se de um tema muito recente no diálogo público, no âmbito jurídico e acadêmico;

c) pois em diversas partes do mundo, no Brasil e no Rio de Janeiro o reconhecimento facial para identificação e prisão de criminosos já é utilizada sem uma base legal e uma profunda reflexão e análise jurídico-ética que fundamente seu uso dentro do contexto da segurança pública das cidades;

d) por ser necessário uma reflexão jurídica e regulatória sobre o tema;

e) pela sua relevância na defesa dos direitos humano;

f) pela importância da academia se manifestar em relação ao tema oferecendo reflexões, pareceres, propostas em prol do ser humano no uso dessa tecnologia.

1 PANORAMA DO USO DO RECONHECIMENTO FACIAL NO BRASIL E NO MUNDO

1.1 Panorama no Mundo

Em 2011, um algoritmo de reconhecimento facial do Registro de Motores de Masssachusetts classificou erroneamente um motorista como criminoso e o fez perder a carteira.[5]

Em junho de 2019, começaram vários protestos em Hong Kong e uma das grandes preocupações dos manifestantes era derrubar os postes com sistema de reconhecimento facial para evitar serem identificados pela polícia.[6]

Os protestos começaram pela insatisfação com a criação de uma lei que permite extraditar presos de Hong Kong para China. As manifestações foram crescendo em número e surgiram outras pautas, entre elas, frear o controle social do Governo Chinês através das tecnologias, por exemplo, o uso de reconhecimento facial. Estima-se que até final de 2020 a China terá implementado em lugares públicos mais de 300 milhões de dispositivos de reconhecimento facial.[7]

Um jornalista da BBC em Xangai lançou um desafio para a polícia a fim de descobrir a velocidade do sistema na identificação. Permitiu que sua foto fosse inserida no software e saiu para a rua, em 7 minutos a polícia conseguiu encontrá-lo.[8]

---

[5] Disponível em: https://www.wired.com/2014/11/algorithms-great-can-also-ruin-lives. Acesso em: 17 de julho de 2020.

[6] Disponível em: https://canaltech.com.br/inteligencia-artificial/protestantes-de-hong-kong-destroem-postes-com-sistemas-de-reconhecimento-facial-147861/. Acesso em: 20 de Julho de 2020.

[7] Disponível em: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html. Acesso em: 15 de Junho de 2020.

[8] Disponível em: https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/. Acesso em: 07 de Junho de 2020.

A Scotland Yard anunciou recentemente que usará o reconhecimento facial na segurança, indo na contramão de cidades que estão banindo seu uso pela força policial, como São Francisco e Cambridge, nos Estados Unidos.

A Universidade de Essex realizou um estudo sobre o grau de acurácia do sistema londrino e descobriu que ele é extremamente impreciso, levantando sérias preocupações em relação a eficácia da ferramenta e violações aos direitos humanos. Um de seus pesquisadores, Dr. Murray, afirma: "Este relatório levanta significativas preocupações em relação à conformidade dos julgamentos com os direitos humanos."[9]

Tudo indica que há diferentes critérios e parâmetros para identificar o grau de eficácia de um algoritmo. A polícia londrina considerou alguns em detrimento de outros. A controvérsia entre a Scotland Yard e a Universidade de Essex continua.

Uma das grandes preocupações está na possibilidade real dessas tecnologias serem usadas para controle social tanto por empresas privadas, como pelo Estado. Um dos alertas em relação ao uso dessa tecnologia foi dado por Luke Stark, pesquisador da Microsoft. Ele afirma em seu artigo que o reconhecimento facial é o plutônio da Inteligência Artificial e que sua regulação é necessária, pois ela é perigosa, facilmente conduzida a um viés discriminatório e tem poucas aplicações práticas. Para o pesquisador, ela deve ser regulada e ter um controle semelhante ao que foi aplicado no cuidado com o lixo nuclear.[10]

Recente estudo lançado nos Estados Unidos mostrou que cidadãos americanos asiáticos e negros possuem uma chance 100 vezes maior de serem equivocadamente identificados pelo reconhecimento facial que um homem branco.[11] Tal estudo mobilizou a sociedade e o congresso americano a iniciar a promoção de uma discussão ética e legislativa sobre o uso de reconhecimento facial nos Estados Unidos.

---

[9] Tradução nossa para: "This report raises significant concerns regarding the human rights law compliance of the trials." Disponível em: https://www.essex.ac.uk/news/2019/07/03/met-police-live-facial-recognition-trial-concerns. Acesso em: 12 de Julho de 2020.

[10] STARK, Luke. Facial Recognition is the plutonium of AI. Disponível em: https://www.researchgate.net/publication/332339918_Facial_recognition_is_the_plutonium_of_AI. Acesso em: 10 de Junho de 2020.

[11] Disponível em: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/. Acesso em: 21 de Julho de 2020.

A NIST (*The National Institute of Standards and Technology*), que cria os padrões para as novas tecnologias, testou mais 180 algoritmos de reconhecimento facial de 99 empresas, entre elas, gigantes como a Microsoft, Intel, Panasonic. E mostrou o quanto essa tecnologia é imperfeita gerando vieses preconceituosos.

Joy Boulamwini, pesquisadora pela MIT MEDIA LAB e ativista digital, tem manifestado constantemente o viés discriminatório dos algoritmos de reconhecimento facial, fazendo duras críticas a diversos sistemas como o da Amazon que tem um grau de assertividade muito menor para mulheres negras.[12]

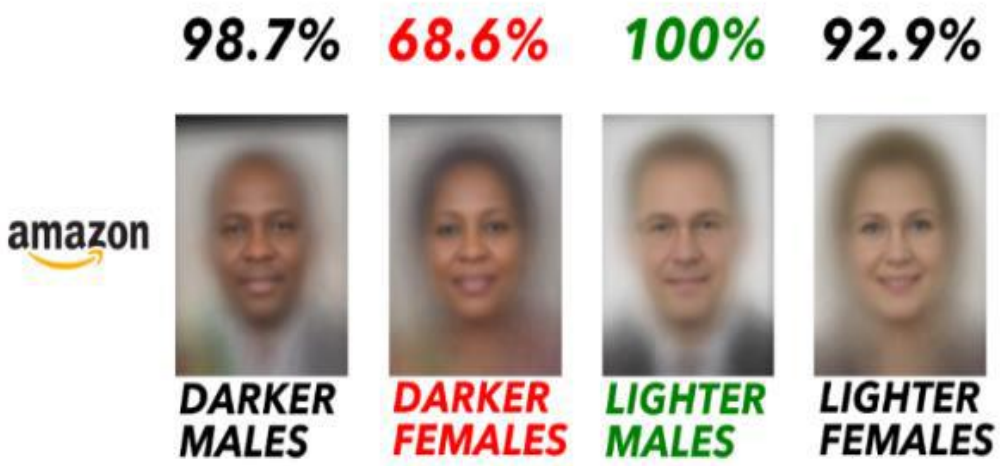

Figura 1: Grau de acurácia no reconhecimento facial da Amazon.

1.2 Panorama no Brasil

No Rio de Janeiro, desde 2018, são dezenas de câmaras de reconhecimento facial que estão espalhadas em bairros da Zona Sul, aeroporto Santos Dumont e Maracanã. Através de um banco de dados da Policia Civil do Rio de Janeiro em questão de segundos se escaneia o rosto

[12] Disponível em: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced. Acesso em: 15 de Junho de 2020.

das pessoas e comparam com os dos procurados pela justiça. Havendo uma combinação da foto escaneada com o banco de dados, um alerta é emitido com nível de risco e grau de acurácia.[13]

Em julho 2021, a Polícia Federal assinou contrato de aquisição e implementação de uma Solução Automatizada de Identificação Biométrica (ABIS), que funcionará já abastecida com cerca de 20 milhões de dados provenientes do banco de dados de impressões digitais, e está projetada para armazenar, em 48 meses, dados de 50 milhões de pessoas, com possibilidade para expansões posteriores que poderão conter dados de até 200 milhões de indivíduos.[14]

Uma decisão do Tribunal de Justiça de São Paulo sobre reconhecimento facial por câmeras com sensores instaladas nas plataformas da linha 4 (Amarela) do Metrô da Capital de São Paulo condenou a concessionária Via Quatro ao pagamento de multa no valor de R$ 100 mil pela coleta indevida de dados de passageiros. A coleta não tinha finalidade de segurança, mas sim de captar a reação de passageiros para fins de publicidade exibida na plataforma.[15]

Rio de Janeiro, Ceará, Bahia e São Paulo são alguns estados no Brasil que possuem monitoramento de reconhecimento facial para a segurança pública. A ferramenta utilizada em S. Paulo já está preparada para receber 90 milhões de registros.[16]

Nessa ano foi lançada pelo Ministério da Ciência, Tecnologia e Inovação uma estratégia nacional para o uso de Inteligência Artificial. No Congresso há um projeto de lei sobre a Inteligência Artificial e um Anteprojeto chamado LGPD Penal.

Em todo Brasil, o monitoramento por reconhecimento facial cresce sem termos uma lei efetiva possa regulamentar o uso da tecnologia. A diferença de outros paises, aqui não há manifestações públicas do cidadão mostrando insatisfação pela aplicação dessa tecnologia para vigilância de massa.

---

[13] Disponível em: https://oglobo.globo.com/rio/copacabana-maracana-ganham-sistema-de-cameras-de-reconhecimento-facial-23791025. Acesso em: 10 de Julho de 2021.

[14] Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biométrica Acesso em: 15 de agosto de 2015.

[15] Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2021/05/11/justica-multa-concessionaria-em-r-100-mil-por-coleta-de-dados-de-passageiros-na-linha-4-amarela-do-metro-de-sp.ghtml e https://www.jota.info/justica/tjsp-proibe-captura-de-dados-por-cameras-do-metro-de-sp-e-aplica-multa-de-r-100-mil-10052021 . Acesso em: 15 de agosto de 2021.

[16] Disponível em: https://tecnoblog.net/380749/por-que-o-uso-de-reconhecimento-facial-na-seguranca-e-controverso. Acesso em: 10 de agosto de 2015.

2 RECONHECIMENTO FACIAL E ASPECTOS TÉCNICO

2.1 O que é reconhecimento facial e riscos

O rosto é a parte do ser humano que está profundamente conectada com sua identidade pessoal, social e institucional. O domínio sobre tecnologias de reconhecimento facial significa um controle muito grande sobre a sociedade. Deste modo, discussões de cunho ético e jurídico estão crescendo em torno dessas tecnologias. Questionamentos importantes são feitos, quando se trata do uso de inteligência artificial para reconhecimento facial na vigilância pública. Como fica a privacidade e liberdades civis, quais as consequências políticas para a democracia, quais as fronteiras éticas para o uso da mesma?

Para Evan Selinger e Brenda Leong um dos primeiros passos para poder dialogar sobre o problema é definir os termos que são utilizados quando falamos de tecnologias de reconhecimento facial.[17] Algumas vezes são empregados de maneira indevida, aplicando o termo a tecnologias que analisam rostos, mas que não identificam individualmente as pessoas.

Para a construção de um diálogo que gere a elaboração comunitária razoável de soluções diante dos desafios éticos e jurídicos inerentes ao RF é muito importante colocar-se de acordo em relação aos significados dos conceitos, caso contrário, será uma torre de babel sem a possibilidade de consenso em ações concretas que beneficiem a sociedade e a justiça.

Existem 4 tipos principais de sistemas de escaneamentos faciais e cada um com graus de uso, benefícios e riscos diferentes.

O primeiro nível seria o uso para detecção facial. É um software que identifica o rosto da pessoa numa imagem ou vídeo. O rosto humano é encontrado para poder melhorar o foco, coletar a imagem para algum banco de dados, aplicar algum tipo de filtro como os usados em

---

[17] SELINGER, Evan; LEONG, Brenda. The Ethics of facial Recognition Tecnology. In The Oxford Handbook of Digital Ethics. Oxford: Ed. Carissa Veliz, 2021. Em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762185. Acesso em: 20 de setembro de 2021.

redes sociais, por exemplo, Instagram. Esse tipo de tecnologia não coleta dados pessoais identificáveis (*personally indetifiable information* ou PII).

Outra utilização de escaneamento facial é para a caracterização facial, análise facial ou detecção emocional. Extrai-se o rosto da pessoa e a partir dele estrutura-se os dados em informações sem ainda necessariamente identificá-lo. Agentes de marketing podem usar essa tecnologia para criar interação da pessoa com alguma propaganda no ponto de ônibus; pode descobrir e coletar o sexo e idade aproximada; indicar o tipo de emoção que a pessoa está sentindo.

Essa tecnologia elabora também uma descrição automatizada da imagem. Quando um usuário sobe (upload) uma imagem nas redes sociais, a inteligência artificial irá transformar essa imagem ou vídeo que são dados desestruturados em dados estruturados, identificáveis e tagueados. É deste modo que o Instagram pode descobrir os interesses de seus usuários simplesmente pelo modo como ele interage na plataforma e assim oferecer informações que façam sentido.

Apesar de não usar necessariamente dados individuais identificáveis, Selinger e Leong apresentam dois riscos no uso dessa tecnologia: (i) falta de acurácia na classificação e interpretação de rostos, caso da pesquisadora Buolamwini que foi a base para o documentário CODE BIAS da Netflix, onde relata os desafios no uso da Inteligência Artificial na sociedade. (ii) Uso desse sistema para fins controversos, como para saber se alguém é gay ou hétero.[18]

Em Dubai, estão construindo no aeroporto uma checagem e controle de fronteira 100% virtual e sem contato com o ser humano. Não terão mais as filas gigantescas e verificação manual dos passaportes pela imigração. Mas engana-se quem acha que a segurança diminuirá. Em substituição à fronteira física estão construindo um túnel com um aquário virtual que será passagem obrigatória para todos que estão no aeroporto. Nele, haverá milhares de microcâmeras que estarão lendo os rostos, expressões e a íris das pessoas para descobrir as emoções e prever possíveis ameaças. Além disso, será feita a leitura facial biométrica de cada pessoa para

[18] Disponível em https://www.bbc.com/news/technology-41188560. Acesso em: 18 de setembro de 2021.

checagem automática do passaporte. O que nos leva aos dois últimos tipos de escaneamentos faciais.[19]

Os próximos dois tipos de escaneamento facial são tecnologias voltadas mais especificamente para o reconhecimento facial, e são variações de sistemas biométricos que criam um modelo identificável e único de uma pessoa. Esse tipo de escaneamento tem uma dupla finalidade: verificação e identificação.

O que seria biometria? É qualquer medida de características pessoais únicas de um indivíduo e que pode ser usado para distinguir um ser humano de outro (IBIA, 2018). Com diferentes métodos, o que os softwares fazem? Eles escaneiam o rosto da pessoa, a partir de imagens de fotos ou vídeos, criam modelos para cada indivíduo, e armazenam essa informação com as medidas que são únicas para combinações futuras.

A verificação consiste no reconhecimento facial onde o sistema busca responder a seguinte pergunta: Essa pessoa é quem achamos que ela seja? O *output* é um simples sim ou não. Um exemplo de acesso por verificação são os telefones celulares, onde para desbloquear o aparelho a pessoa tem o rosto escaneado e identificado.[20]

Enquanto identificação é quando a partir da imagem de um rosto buscamos entre várias imagens armazenadas para saber quem é a pessoa (Selinger e Leong, 2021). Os sistemas de identificação buscam responder a seguinte pergunta: Pode o algoritmo determinar quem é essa pessoa desconhecida?

O escaneamento facial para identificação biométrica é usado na vigilância em aeroportos, metrôs, na rua e em lugares públicos como estádios de futebol. O sistema escaneia uma imagem (de um vídeo ou de uma câmera), cria um modelo único daquela pessoa e busca combinar com um banco de dados prévio. Pode ser usado também para criar um perfil dos

---

[19] Dubai airport's new virtual aquarium tunnel and what it means for the future of border security. ASPI, 2017. Disponível em: https://www.aspi.org.au/opinion/dubai-airports-new-virtual-aquarium-tunnel-and-what-it-means-future-border-security. Acesso em: 20 de setembro de 2021.

[20] Disponível em: https://olhardigital.com.br/2017/10/31/noticias/reconhecimento-facial-do-iphone-x-pode-ser-enganado-por-gemeos-identicos/.Acesso em: 20 de setembro de 2021.

consumidores para enviar sugestões de produtos e serviços, em hotéis, concertos, para o registro e check-in em aeroportos.

Além do uso para vigilância, a tecnologia de escaneamento de imagens tem outras aplicações como auxiliar os cegos na leitura do braile, ajudar autistas a identificarem emoções. Na medicina é usado para diagnósticos e tratamentos (Hallowel, e al, 2018). Deste modo, o simples banimento dessa tecnologia pode impedir o desenvolvimento e aplicações práticas benéficas e importantes que vão além da segurança pública.

2.2 Uso do reconhecimento facial e aspectos técnicos

O RF está ficando cada vez mais acessível economicamente e é uma tecnologia extremamente invasiva. A detecção facial já era possível sem um uso complexo de algoritmos, com ela poderíamos identificar, numa imagem ou vídeo, o rosto, mas sem correlacioná-lo com uma pessoa.

O reconhecimento facial, além de identificar que é um rosto humano, sabe afirmar de quem é o mesmo. Para isso, é necessário aplicar técnicas mais avançadas de inteligência artificial como *machine learning*, redes neurais e *deep learning.* Sem a compreensão da complexidade técnica desses campos da Inteligência Artificial será inútil qualquer tipo de tentativa de regulação da mesma. Como funciona um algoritmo? Como ele é treinado? Qual o impacto dos dados inseridos no sistema para a configuração do algoritmo? Existem l

qimites técnicos para a compreensibilidade das decisões algorítmicas?

Em geral, no reconhecimento facial, o algoritmo incialmente relaciona um número limitado de pontos do rosto na imagem ou vídeo de um ser humano, entre 6 a 8 pontos, e correlaciona o rosto com uma pessoa concreta.

Na medida em que se confirma como correta, vai ampliando até identificar aproximadamente 80 pontos. A partir dessa correlação, o algoritmo gera padrões das pessoas e as identifica com facilidade.

Numa imagem ou vídeo que não mostre de frente o rosto humano, se desenvolveu uma tecnologia para gerar uma imagem 3D e assim identificar a pessoa mesmo que ela não esteja de

frente. Uma das técnicas mais bem sucedidas é a do FACEBOOK, conhecida como *Deepface.*[21]

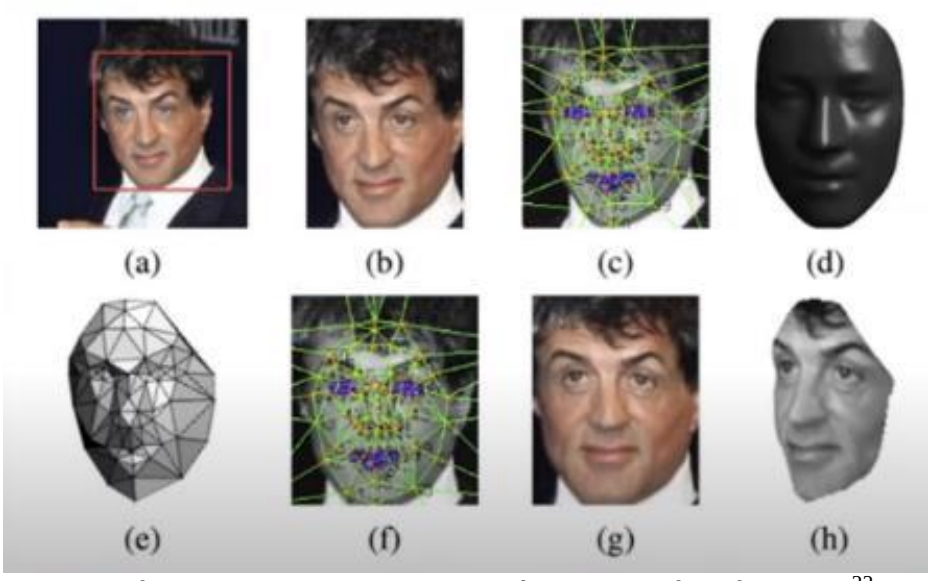

figura 2: Imagem de como a técnica Deepface funciona.[22]

O Iphone usa uma técnica de projeção de pontos chamada de *TrueDepth*. No momento de destravar o celular, é projetada uma luz de aproximadamente 50 mil pontos, por isso o iphone não desbloqueia com a foto da pessoa por não possuir a tridimensionalidade do rosto humano.[23] As técnicas estão evoluindo a ponto de identificar a pessoa pela textura da pele.

---

[21] TAIGMAN, Yaniv et al. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. Disponível em: https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf. Acesso em: 15 de Junho de 2020.

[22] Ib. página 2. Figure 1. Alignment pipeline. (a) The detected face, with 6 initial fiducial points. (b) The induced 2D-aligned crop. (c) 67 fiducial points on the 2D-aligned crop with their corresponding Delaunay triangulation, we added triangles on the contour to avoid discontinuities. (d) The reference 3D shape transformed to the 2D-aligned crop image-plane. (e) Triangle visibility w.r.t. to the fitted 3D-2D camera; darker triangles are less visible. (f) The 67 fiducial points induced by the 3D model that are used to direct the piece-wise affine warpping. (g) The final frontalized crop. (h) A new view generated by the 3D model.

[23] Disponível em: https://www.techtudo.com.br/noticias/2018/12/conheca-a-truedepth-tecnologia-por-tras-do-reconhecimento-facial-do-iphone.ghtml. Acesso em: 10 de Junho de 2020.

3 RECONHECIMENTO FACIAL E ASPECTOS JURÍDICOS

Estamos diante de um aumento significativo do uso de reconhecimento facial para vigilância de massa. Existe no Brasil e no Mundo um arcabouço legistivo que oriente o uso da mesma? Iremos analisar agora o que podemos extrair de alguma ações legislativas no mundo e da nova Lei Geral de Proteção de Dados e do Anteprojeto LGPD Penal em relação ao uso do RF.

3.1 Reconhecimento facial e panorama legislativo internacional

A falta de precisão e acurácia no uso do RF traz implicações gravíssimas, como por exemplo, em nome de uma suposta necessidade de aperfeiçoar a segurança através da tecnologia, discriminar minorias, gerando comportamentos abusivos por parte da força policial. Há também o perigo em relação ao viés de confirmação do algoritmo. Este viés ocorre quando a polícia utiliza Inteligência Artificial para decidir em que regiões haverá mais policiamento. Haverá mais vigilância onde os dados indicam para ter mais vigilância, e com o envio de mais força policial para os lugares indicados são gerados novos dados que serão inseridos no sistema retroalimentando o viés.[24]

Em 2017, o poder legislativo de Nova York aprovou uma regulamentação para garantir a transparência dos algoritmos usados pelos órgãos públicos da cidade como as decisões por algoritmos usados pela polícia. A lei municipal de Nova York *no.1696-A* possui poucos princípios, é temporária e limitada a órgãos públicos com o objetivo de garantir o uso seguro, transparente e democrático dos sistemas de decisão automatizada (*automated decision system*).[25] Essa lei foi uma das fontes para a criação do Anteprojeto LGPD Penal.

---

[24] Disponível em: https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology. Acesso em: 23 de julho de 2020.

[25] Disponível em: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0. Acesso em: 23 de julho de 2020.

A Inteligência Artificial é um algoritmo que segue um modelo matemático alimentado com dados para cumprir certas tarefas. Dependendo dos dados, o modelo matemático pode possuir um vieses que violem os direitos humanos. Algoritmos não são neutros. Eles aprendem através dos dados inseridos. É necessário criar estratégias de auditoria dos algoritmos que permitam replicar os valores éticos e direitos humanos fundamentais. Algoritmos podem ser matematicamente espetaculares, mas eticamente problemáticos.

Uma decisão simbólica que mostra a importância do tema é o caso da cidade de São Francisco, conhecido como o berço da inovação com o Vale do Silício. Em 2019, ela bane o uso da tecnologia para vigilância policial e pelos departamentos do Estado.[26]

Um passo ainda mais importante foi o anúncio quase que simultâneo da IBM, Microsoft e Amazon de parar ou pausar a venda e desenvolvimento de tecnologias de reconhecimento facial para a segurança pública. Em meio aos protestos causados pelo abuso policial que ocasionou a morte de George Floyd, algumas *big techs* decidiram interromper suas atividades nesse campo. O presidente da Microsoft em entrevista ao Washington Post afirmou que a empresa decidiu que:

> "nós não venderemos a tecnologia de reconhecimento facial para o departamento de polícia dos Estados Unidos até nós termos uma lei nacional bem enraizada nos direitos humanos que governarão essa tecnologia."[27]

3.2 Reconhecimento facial e LGPD

A Lei Geral de Proteção de Dados que entrou em vigor em setembro de 2020 não impede o uso de tecnologias de RF, pois há vedação expressa no art. 4 para aplicação da LGPD quando se refere ao uso de tecnologias que exigem o tratamento de dados para vigilância pública. [28]

---

[26] Disponível em: https://edition.cnn.com/2019/05/14/tech/san-francisco-facial-recognition-ban/index.html. Acessado em: 23 de julho de 2020.

[27] Tradução nossa para: "...decided that we will not sell facial recognition technology to police departments in the United States until we have a national law in place grounded in human rights that will govern this technology." Disponível em: https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons-face-recognition-bans-dont-go-far-enough. Acesso em: 23 de Julho de 2020.

[28] Lei federal 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 de Agosto de 2020.

No art. 4, inc. iv., § 1º, a LGPD estabelece que deverá ser criada legislação específica para as exceções previstas no inciso III, são elas: segurança pública, defesa nacional, segurança de Estado ou atividades de investigação e infrações penais.

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. (art. 4, inc. iv. § 1º da LGPD)

A lei deste modo deixou um vácuo em relação ao tratamento de dados de tecnologias de reconhecimento facial na segurança pública. Diante dessa lacuna, no Distrito Federal foi elaborada a lei 6.712/20 que regulamenta o uso de reconhecimento facial em áreas públicas.[29]

Nela se define que reconhecimento facial é uma tecnologia que analisa as características faciais usada para a identificação pessoal exclusiva de indivíduos em imagens estáticas ou em vídeos. Proíbe o uso da mesma para vigilância que ultrapasse 72h, restringe seu uso a espaços públicos e deve ter placas visíveis informando seu uso. Além disso, qualquer identificação realizada pelo sistema deve ser revisada por agente público antes de qualquer ação ou medida.

O art. 6º da mesma lei, se apresenta como um número problemático, pois se por um lado estabelece que as informações decorrentes do uso de tecnologia de reconhecimento facial são dados sensíveis e deve respeitar o estabelecido no tratamento de dados da Lei Geral de proteção de dados. Por outro lado, não indica a base legal para tratamento do mesmo. Afirma que o mesmo deve ser restrito a seu uso autorizado. Mas qual uso autorizado seria esse? Se seguir o estabelecido pela LGPD como a própria lei indica, dados biométricos são dados sensíveis e deve possuir uma base legal para o tratamento do mesmo. Seria o consentimento a base legal? O modo que foi redigido o número leva a um looping, é uma proposição tautológica.

Outra problemática em relação a LGPD: as vedações presentes no art. 4º. significariam uma falta de competência da Autoridade Nacional de Proteção de Dados em relação a esses

---

[29] Lei 6.712, de 10 de novembro de 2020, Distrito Federal. Disponível em: https://sintse.tse.jus.br/documentos/2020/Nov/11/para-conhecimento-institucional/lei-no-6-712-de-10-de-novembro-de-2020-dispoe-sobre-o-uso-de-tecnologia-de-reconhecimento-facial-trf. Acesso em: 10 de agosto de 2021.

temas? No Art.4º, § 3º, parece indicar que não, pois é função da ANPD emitir opiniões técnicas e recomendações referentes às exceções previstas no inciso III e que pode solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

3.3 Reconhecimento facial e LGPD Penal

No Congresso Federal encontramos o Anteprojeto LGPD Penal que versa sobre o tratamento de dados pessoais na segurança pública e persecução penal.[30] Foi criada uma comissão para elaborar o texto em novembro de 2019, em novembro de 2020 foi entregue ao Congresso o texto final.

Na exposição de motivos ressalta-se a importância de uma lei especifica sobre o tema, pois sua ausência obsta o Brasil de integrar órgãos de inteligência e de investigação de caráter internacional, não tendo acesso a banco de dados, informações relevantes e as técnicas mais modernas de investigação. Além disso, temos um grande déficit de proteção dos cidadãos ao não possuir uma regulação sobre o tratamento dos dados na esfera penal, no monitoramento e vigilância gerando uma assimetria de poder entre Estado e cidadão.

O anteprojeto está estruturado em 12 capítulos, com 68 artigos. É inspirado na LGPD; na Diretiva 680/2016, da União Europeia; e em leis dos Estados Unidos na parte específica sobre tecnologias de vigilância e tratamento de elevado risco. Estabelece que o Conselho Nacional de Justiça (CNJ) será a autoridade para a aplicação, supervisão e monitoramento da LGPD Penal.

No art. 42, observamos uma menção a utilização de tecnologias de monitoramento ou tratamento de dados pessoais que representem risco para direitos, liberdades e garantias dos titulares dos dados. Essas dependerão de previsão legal específica, que estabeleça garantias aos direitos dos titulares e deverão ter relatório de impacto.

---

[30] Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/wp-content/uploads/sites/41/2020/11/dadosanteprojetocomissaoprotecaodadossegurancapersecucaofinal_051120204929.pdf . Acessado em: 15 de Agosto de 2021.

No art. 43, veta a utilização de tecnologias de vigilância para identificar pessoas em tempo real e de forma contínua, a não ser que tenha conexão com atividade de persecução penal individualizada, autorizada por lei e decisão judicial. O anteprojeto não usa diretamente a palavra reconhecimento facial.

Tudo indica que ainda será necessário elaborar uma lei específica no que diz respeito ao uso de reconhecimento facial para a vigilância pública. Outro ponto interessante a ser estudado é sobre como esse anteprojeto pode comungar com o Decreto Federal 10.046/19 que trata sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro base do Cidadão e o Comitê Central de Governança de Dados.[31]

No art 18., inciso II do decreto, estabelece uma série de dados sensíveis que serão integrados numa base única, entre eles os dados biométricos. No art. 21, inciso I, afirma que Comitê Central de Governança de Dados deverá seguir a legislação referente à proteção de dados pessoais. Indica também no art. 3º., inciso I, que o compartilhamento dos dados entre órgãos e entidades também deverá seguir a LGPD.

Na prática estamos formando um grande repositório com todos os dados dos Brasileiros. Mais do que nunca a segurança da informação será essencial para gerar credibilidade ao sistema, especialmente diante de tantos vazamentos relatados no último ano.

Gilmar Mendes menciona o Anteprojeto de LGPD Penal na medida cautelar em mandado de segurança no. 38.187 impetrado pelo Brasil Paralelo contra aprovação dos Requerimentos 1362/20212 e 1364/2021 elaborados pela CPI do Senado concernente ao enfretamento da pandemia da Covid-19 no Brasil.[32]

Ele considerou o caso como um exemplo paradigmático de aplicação da LGPD para investigação penal. É uma lacuna normativa deixada intencionalmente tanto no Marco Civil da Internet, quanto na LGPD. Também menciona que essa lacuna é objeto do Anteprojeto de LGPD Penal. Cita o art. 2º da mesma, ressaltando a importância de defender a dignidade da

---

[31] Decreto Federal 10.046, de 9 de outubro de 2019. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm . Acessado em 20 de setembro de 2019.

[32] Medida Cautelar em Mandado de Segurança 28.187, Distrito Federal. Disponível em https://www.conjur.com.br/dl/gilmar-brasil-paralelo.pdf Acessado em 20 de setembro de 2021.

pessoa humana, a intimidade e vida privada do cidadão, e garantir o devido processo legal, a ampla defesa, do contraditório e a reserva legal.

Em referência ao Anteprojeto, ele afirma que dados de operações financeiras, registros e conteúdos de comunicação privadas e geolocalização são dados sigilosos requeridos pela CPI. Mesmo que o Anteprojeto não seja norma vigente e não possua caráter vinculativo, deve ser considerado por suas diretrizes interpretativas e por ter sido proposto e formulado em conjunto por especialistas sobre o tema.

Deste modo, o ministro Gilmar Mendes considera que não deve ser liberado registros de conexão, dados de comunicação e conteúdos de comunicações privadas dos usuários do Brasil Paralelo. Esse caso recente, escancara a importância peremptória de existir uma lei vigente sobre o tema, e sua urgência aumenta diante do uso real, atual e cada vez mais comum no Brasil do reconhecimento facial para a vigilância de massa.

4. RECONHECIMENTO FACIAL E DESAFIOS ÉTICOS

4.1 Desafios do reconhecimento facial

Com uso massivo do reconhecimento facial para a vigilância, quais são os principais riscos e desafios para a sociedade e para o exercício da justiça? (Selinger e Leong, 2021)

Um dos primeiros riscos está relacionado ao *dataset* (o conjunto de dados que será utilizado pela tecnologia). Quais bancos de dados podem ser usados? O governo pode utilizar os dados coletados para um finalidade em outra? Empresas privadas podem ter acesso a esses banco de dados para o treinamento de seu próprio software que depois serão utilizados para a viligância de massa? Qual seria o padrão minimo de qualidade e diversidade do *dataset* para que não se criem soluções com viés descriminatório?

São perguntas importantes e ainda em aberto. Alguma normativas surgem no mundo com objetivo de regular a finalidade e o modo em que os dados são tratados. Outros advogam pela necessidade de uma diversidade dos dados, afim de evitir descriminação das minorias. Algumas minorias que já se sentem excluidas afirmam que não irão favorecer o uso desses sistemas que permitirão uma escalada na descriminação (Samudzi, 2019).

Algumas soluções já estão sendo disponibilizadas pela própria tecnologia para ajudar em alguns problemas relacioanados ao *dataset*. Uma tecnologia que cria rostos humanos virtuais e únicos pode ajudar no treinamento de máquina sem precisar usar imagens de pessoas reais para melhorar o algoritmo.[33]

Na inglaterra, há uma proposta de que só armazenará as imagens por periodo limitado e o escaneamento para o reconhecimento biométrico só será utilizado na ocorrência de crimes na

[33] Disponível em https://mittechreview.com.br/a-inteligencia-artifical-da-openai-esta-aprendendo-a-gerar-imagens-ficticias/ . Acessado em 10 de setembro de 2021.

região que é monitorada, assim evitando a vigilância constante. Desde 2012, existe um guia de boas práticas e governança na Inglaterra para o uso dessa tecnologia.[34]

Outro desafio é o da acurácia, dependendo do grupo de pessoas, genêro ou sexo, a acurácia pode ser menor ou maior. O NIST (National Isntitute of Starndars and Tecnology), uma espécie de INMETRO dos Estados realizou uma pesquisa voluntária para medir o grau de acurácia das tecnologias existentes para RF. Os melhores sistemas (10 dos 15 mais usados) mostraram uma acurácia de 99%. No entanto, outras companhias (aproximadamente 100) não mostraram esse grau de acertividade. O maior agravante é que os erros aumentam consideralvemente quando se trata de categorias de gêneros e raças de minorias. No grupo de mulheres e negras as tecnologias de RF possuem menor acurácia (Samudzi, 2019).

Novamente, a tecnologia está ajudando a resolver o problema da acurácia para grupos minoritários. Uma startup carioca, a CyberLabs criou uma tecnologia chamada de *Racial Face in the Wild (RFW)* com uma acurácia de 99,84% para faces de pessoas negras.[35]

O terceiro desafio seria o legal e ético do chamado dano de distribuição desproporcional. Como o grau de acurácia é diferente dependendo do grupo social não todos estão igualmente vulneráveis aos prejuízos e danos advindos dos erros de identificação, falsas acusações e prisões equivocadas. Deste modo, as maiorias não assumem os riscos na mesma proporção que as minorias. No sistema de vigilância do Rio de Janeiro, uma mulher foi identificada equivocadamente e levada a delegacia onde se constatou o erro do sistema, sendo liberada em seguida.[36]

Um último risco que é pouco comentado é o do perigo da geração de efeitos sociais tóxicos (Selinger e Leong, 2021). Através da criação de modelos únicos de pessoas e o uso de inteligência artifical para reconhecimento facial com finalidade de vigilância em massa pode-se criar e fortalecer uma série de esteriótipos sobre raças e gêneros, além de impulsionar o

---

[34] Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf , Acesso em: 10 de setembro de 2021.

[35] Disponível em https://dicaappdodia.com/tecnologia-brasileira-reconhecimento-facial-pessoas-negras/ . Acessado em 10 de setembro de 2021.

[36] Disponível em https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml . Acessado em 20 de setembro de 2021.

surgimento de linhas de pesquisas baseadas em pseudo-ciências que conduzam a uma espécie de redução do ser humano a dados biológicos deterministas.

Lisa Feldman Barret, professora de psicologia da Northeastern University, afima que diversas tecnologias de escaneamento facial para detecção de emoções estão fundamentadas em paradigmas científicos ultrapassados. [37]

Com as novas tecnologias e o crescimento da neurociência estamos aos poucos revivendo o determismo científico que dominou o inicio da primeira revolução industrial e o iluminismo e que muitos pensadores apontaram como causa para o surgimentos das grandes guerras que assolaram o século 20 (Bauman, 1999).

No início do século 20, foi muito conhecido e utilizado no mundo inteiro os estudos e pesquisas do italiano Cesare Lombroso, um professor de medicina legal da Universidade de Turim. Em sua obra *L'Uomo delinquente* (1876) desenvolveu a teoria da origem atávica do comportamento antissocial e criou o termo o *criminoso nato,* que possui uma predisposição pessoal ao delito. A frenologia foi uma ciência médica determinista em que atribuía o formato e estrutura do cérebro a atos criminosos. Deste modo, o ser humano não era livre, mas seu agir era resultado de uma forma cerebral específica.[38]

Outra pseudociência que dominou o século XIX e XX foram as sociedades eugênicas em diversas partes do mundo. Elas tinham o objetivo de promover e desenvolver ideias de aprimoramento da composição genética por meio da reprodução controlada dos seres humanos. Em 1912, Leonard Darwin, filho de Charles Darwin realizou o primeiro Congresso Internacional de Eugenia em Londres. Alexander G. Bell, inventor do telefone, foi presidente honorário do segundo Congresso internacional realizado em Nova York. [39] Uma das razões de não estranharem algumas ideias eugênicas de Hitler quando o mesmo alcançou o poder foi o fato de que ideias eugênicas permeavam a sociedade naquele período (Bauman, 1999).

---

[37] Disponível em https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks . Acessado em 20 de setembro de 2021.

[38] Disponível em https://www.scielo.br/j/rh/a/LzvLWjsKMqRdNgZjNgJxWqh/?lang=pt. Acesso em: 15 de setembro de 2021.

[39] Disponível em https://embryo.asu.edu/pages/american-eugenics-society-1926-1972 . Acesso em: 15 de setembro de 2021.

Torna-se essencial acompanhar de perto o desenvolvimento de tecnologias que estejam fundamentadas numa visão antropológica determinista do ser humano. A preocupação é maior nesse momento, pois à diferença de tecnologias que surgiram em outros momentos históricos, o poder de escala global e exponencialidade das tecnologias atuais é maior, podendo se alastrar numa velocidade que uma vez implementada o dano possa ser irreversível.

4.2 Erosão da confiança entre as pessoas e nas instituições

Um estudo da *Georgetown Law Center on Privacy and Tecnology* levantou uma série de preocupações sobre a acurácia e impacto social do reconhecimento facial no contexto da aplicação da lei (Garvie, Bedoya, e Frankle, 2016; Rudolph, Moy, e Bedoya, 2017; Garvie e Moy, 2019; Garvie, 2019).

O modo em que essa tecnologia está sendo implementada e utilizada na sociedade começa a gerar uma série de fatos em que aumentam a desconfiança dos cidadãos entre si, e dos cidadãos em relação as instituições públicas.

Segundo a pesquisa, alguns elementos estão erosionando a confiança nas pessoas e instituções. (i) A falta de transparência da justiça com a população sobre como está sendo utilizado o reconhecimento facial no âmbito da vigilância. (ii) o uso indevido das imagens capturadas pelos agentes públicos sem seguir um padrão de qualidade e governança mínima dos dados que diminuam os viéses negativos. (iii) O uso de imagens de milhões de americanos com o nome da pessoa escrito na foto. (iv) A implementação legalmente duvidosa de reconhecimento facial nos aeroportos.

Essa erosão da confiança diante do abuso no uso dos dados gera problemas também entre consumidores e fornecedores. A percepação geral da população é que o uso dessas tecnologias produzem perdas de oportunidades, perdas econômicas, perdas de liberade e maior detrimento social (Selinger e Leong, 2021).

1. Perda de oportunidade: o uso indiscrimando e obscuro em processos seletivos, na aprovação de seguros, na elaboração e distribuição de beneficios sociais e na criação e implementação de políticas educacionais;

2. Perdas econômicas: politicas obscuras de liberação de crédito, precificação diferente dependendo do tipo de parâmetros imbutidos na inteligência da máquina, como o geopricing;
3. Perda da liberdade: maior percepção que estamos caminhando para uma sociedade da vigilância, da falta de privacidade e intimidade;
4. Detrimento social: criação de bolhas, viés da confirmação, estigmação de grupos e reforço de esteriótipos.

> "Se os indivíduos acreditarem que não têm como escapar da onipresença da vigilância, eles estarão mais propensos em perder a confiança nas garantias de que seus dados e escolhas privadas estão sendo respeitados." (Brandom, 2018).

Diante disso, diversos estudos estão sendo realizados sobre o tema estabelecendo a importância da transparência e do *accountability*. Estão emergindo paradigmas éticos centrados na razoabilidade e confiança no uso de RF.

A Inglaterra divulgou recentemente seu programa para o uso, promoção e governança da Inteligência Artificial para os próximos 10 anos.[40] A União Europeia também lançou seu programa para promover o desenvolvimento da Inteligência Artificial com o objetivo de impulsionar a pesquisa, a industria e garantir o respeito aos direitos fundamentais. Também será a base para uma legislação que impactará em toda a União Europeia.[41]

O Brasil também tenta no Congresso criar seu marco legal para a Inteligência Artificial, mas assim como seu programa estratégico para Inteligência Artificial divulgado pelo Ministério da Ciências, Tecnologia e Inovações, está sendo duramente criticado seja pela superficialidade, seja pela necessidade de uma maior amadurecimento em relação ao tema.[42]

---

[40] Disponível em https://www.gov.uk/government/news/new-ten-year-plan-to-make-britain-a-global-ai-superpower. Acesso em: 22 de setembro de 2021.
[41] Disponível em https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence. Acesso em: 22 de setembro de 2021.
[42] Disponível em https://www1.folha.uol.com.br/colunas/ronaldolemos/2021/04/estrategia-de-ia-brasileira-e-patetica.shtml. Acesso em: 22 de setembro de 2021.

4.3 Reconhecimento facial, virtude, livre arbítrio e desumanização

A vigilância constante modifica comportamentos, a percepação de si mesmo, e gerará um "chilling effect", efeito inibidor, efeito amendrontador, efeito desencorajador (Selinger e Leong, 2021).

Com o advento de uma sociedade da perfeita vigilância e com uma acurácia quase total no uso do reconhecimento facial existe a hipótese de que as pessoas possam se perceber limitadas em seu agir livre. Diante da vigilância constante, pessoas podem coibir suas manifestações espontâneas, livres e criativas conduzindo aos poucos a fragmentação dos fundamentos de uma sociedade democrática livre.

Para o filósofo Benjamim Hale, esse tipo de sociedade promove o fim do ideal Kantiano em relação ao livre árbitrio (HALE, 2005). "Isso erosionaria a motivação das pessoas para se engajarem em deliberações éticas sobre como eles deveriam agir e sobre quem elas deveriam ser" (Hale, 2005, p. 150). Cita o exemplo da impossibilidade de cometer um adultério ou de apenas realizar um ato virtuoso e bom não por convicção, mas porque existe um agente externo vigiando e punido.

Sem o espaço para a liberdade, o ser humano deixaria de exercitar as virtudes. Agiria não por convicção, mas por medo da punição diante da sociedade da vigilância. Sem espaço para exercer atos virtuosos e morais por convição haveria aos poucos a fragmentação da vontade e do livre arbítrio. Mais mecanismos de controle teriam que ser implementados para poder conter uma sociedade incapaz de ser virtuosa.

> "Nesse tipo de mundo, intensões éticas como carater moral ou virtudes pessoais que requerem o exercicio do livre árbitrio, como sinceridade ou integridade, seriam comprometidos porque eles seriam dificilmente desenvolvidos." (HALE, 2005, p.151)

Nessa sociedade hipotética da vigilância perfeita o ato individual de proclamar e agir pelo amor e entrega ao outro não teria a densidade da verdade, pois seria maculado pela eterna presença do vigilante que obriga a agir corretamente.

Para o filosofo Philip Brey (Brey, 2004), o reconhecimento facial aplicado a uma vigilância plena e perfeita levaria a uma profunda alienação do ser humano, levaria a humanidade para um processo de desumanização e perda de sua indentidade.

Através do reconhecimento facial aplicado em massa, o rosto humano, que é seu elemento mais caracteristico e distinto, a janela para seu eu e para sua personalidade seria reduzido a dados, a uma função instrumental de senha e controle social. Seria uma mudança essencial na percepção de si mesmo diante do mundo e do outro que advém do rosto humano. Há uma redução da nossa face a agente informacional. Não teriamos mais controle da nossa identidade e do nosso eu, separando o dono do rosto, do controle da sua propria identidade. Submeter-se ao consentimento para o uso do rosto transformado em dados gera uma alienação, onde o rosto já não é mais exclusivamente “seu”.

Alguns filosofos defendem que a relação cara a cara (entendido como viver na presença do outro) é a base para qualquer relação e de onde surge as responsabilidades éticas (Levinas, 1969). Sem essa relação, sem o dominio do “eu”, sem espaço para exercício livre da virtude a sociedade se destruiria.

4.4 Reconhecimento facial e banimento

Woodrom Hartzog e Evan Selinger defendem que “a tecnologia de reconhecimento facial é o mais perigoso mecanismo de vigilância inventado.” (Hartzog e Selinger, 2018). E recomendam que seja banida do uso público e privado.

Eles são defensores do *“Slipery Slope Argument”* razoável (argumento da ladeira escorregadia). É um tipo de argumento, onde se elabora uma sequências de pequenos passos que levam a uma cadeia de eventos que conduzem a um efeito significante e geralmente negativo.

Se é razoavel acreditar que a tecnologia de reconhecimento facial tem o potência de ser cada vez mais usada de modo a invadir a intimidade das pessoas e aumentar o controle, e se isso conduzirá a erosão da liberdade, da dignididade e da democracia, então tal tecnologia deve ser proibida ou controlada desde agora.

Adam Thierer defende que esse argumento não possui credibilidade, pois de maneira ilegitima considera os riscos do uso inapropriado e extrapola para uma distopia digna de ficção científica (Thierer, 2019). Esse tipo de argumento gera um tecnopânico totalmente infundado. Seriam os ludistas modernos.

Para Selinger e Hartzog, utillizando o argumento "slippery slope", aplicativos de tagueamento de fotos como o do facebook deveriam ter uma espécie de consentimento pleno e perfeito que eles chamam de "consentability", que vai além de um simples consentimento.

Esse tipo de consentimento pleno e perfeito implicaria em avisar a todos os usuários que taguear as fotos pode influenciar todos os usuários a serem receptivos ao surgimento de mais tecnologias ainda mais invasivas e que isso conduzirá a perigos contra direitos fundamentais (Selinger and Hartzog, 2019).

Nesse contexto, a prática comum onde as pessoas usam sua liberdade individual, mesmo que num pequeno ato de marcar uma foto, viola a "autonomia coletiva", uma espécie de principio ético que protege a democracia no âmbito das liberdades fundamentais.

Deste modo, mesmo que seja um ato livre de menor importância, esse ato replicado por milhões de usuários levará ao desenvolvimento e maior recepção de futuras tecnologias que serão mais invasivas. Assim, esse ato individual deveria ser proibido em nome de um possível dano a essa "autonomia coletiva" (Selinger e Hartzog, 2019)

> "Embora seja assustador pesar todos esses recursos, uma coisa é certa: quanto mais tempo levar para determinar as regulamentações apropriadas, mais difícil será reverter uma infraestrutura que implanta o poder de moldar a sociedade." (Selinger e Leong, 2021)

4.5 Reconhecimento facial e arte

O receio de uma surgimento de uma sociedade da vigilância penetrando todos os setores da sociedade, inclusive no mundo das artes. Ativistas usam o que é conhecido como *adversarial stickers* para impedir o reconhecimento facial. A artista polonesa Ewa Nowak criou uma linha

de joias que cobrem parte do rosto e impede a identificação. [43] A arte se colocando a serviço do ser humano e defendendo seus direitos.

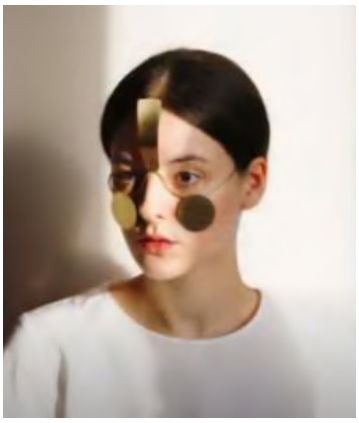

Figura 3: Exemplo de joias criada pela Ewa Nowak para despistar o reconhecimento facial.

Alguns ativistas e pesquisadores estão descobrindo modos de usar adesivos no rosto para atrapalhar o reconhecimento facial.[44]

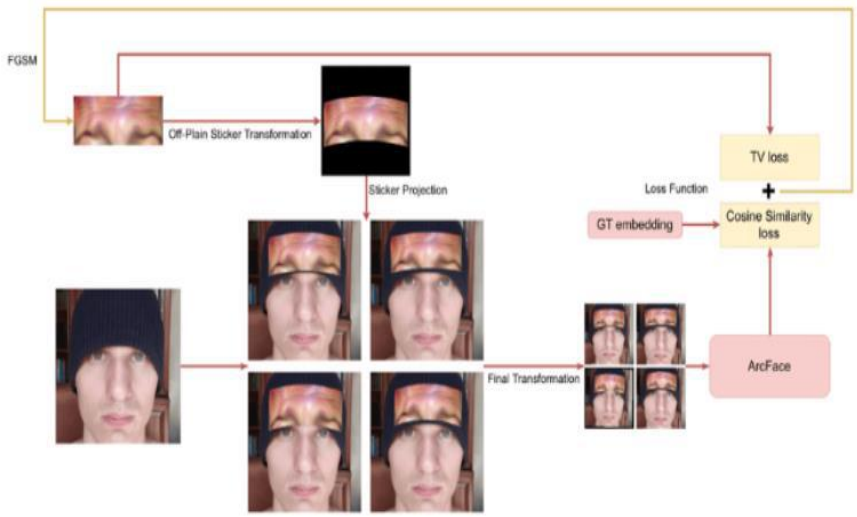

Figura 4: Exemplo de *adversarial stickers*

[43] Disponível em: https://www.dezeen.com/2019/07/30/ewa-nowak-anti-ai-mask-protects-wearers-from-mass-surveillance/. Acesso em: 20 de Julho de 2020.

[44] Disponível em: https://medium.com/syncedreview/adversarial-patch-on-hat-fools-sota-facial-recognition-82e8c4f83498. Acesso em: 20 de Julho de 2020.

Diante dos perigos e riscos no uso do RF cresce o posicionamento de proibir o desenvolvimento da tecnologia. No entanto, em vez de proibir não seria possível regular o uso? Barrar a tecnologia em si não poderia impedir o uso positivo em prol da própria sociedade? Não seria impedir o positivo potencial heurístico do reconhecimento facial? Um algoritmo para reconhecimento facial pode no futuro reconhecer um tumor, por exemplo? Como usar essa tecnologia respeitando os direitos humanos e as liberdades individuais? É possível no desenho dos próprios sistemas inserir princípios legais e éticos que impeçam um uso abusivo ou impeçam qualquer violação?

5. RECONHECIMENTO FACIAL E REGULAÇÃO

Durante muitos anos nossa sociedade foi pautada pelo princípio ético de raiz iluminista, mecanicista e materialista de que tudo que era tecnologicamente possível era automaticamente bom e deveria ser feito. Esse princípio ético está sendo questionado como nunca. Será que todas as transformações tecnológicas são boas em si? O fato de sermos capazes de desenvolvê-las significa que devemos colocá-las em ato?

O filósofo francês Bruno Latour defende que as tecnologias não são neutras, elas carregam em si uma finalidade e valores, que devem ser explicitados para colocar a luz seus possíveis vieses e preconceitos. Algo que o filósofo grego Aristóteles já assinalava ao falar das quatro causas do ente.

No entanto, questionar esse princípio ético de matriz mecanista não significa cair num ludismo contemporâneo ou um catastrofismo neofóbico que coloque freio à expressão da criatividade humana. O medo ao novo não pode ser um critério ético. Ir por esse caminho é fechar janelas para o futuro da sociedade.

Esse é o grande desafio da nossa geração. Seja do ponto de vista dos empreendedores da tecnologia, da população ou das autoridades de um país, todos estamos lidando com o desafio do equilíbrio, de estar aberto à experimentação de novos caminhos, respeitando o passado e tendo o ser humano como centro das decisões. É um caminho sem volta e de total importância seja na definição do plano de vida, da estratégia dos negócios ou na formulação de políticas públicas.

Independente do caminho que iremos seguir, uma coisa é certa: não podemos trilhar sozinhos. A colaboração, a transparência, a necessidade de criar estruturas inovadoras que resgatem a centralidade do ser humano é urgente. Tais valores devem permear as estruturas legislativas na criação de leis e ações que promovam um Brasil mais tecnológico, mais aberto à colaboração, mais equânime.

5.1 Reconhecimento facial e 4 vetores regulatórios

Lawrence Lessig, em sua obra *Free Culture* [45], afirma que 4 elementos devem estar em comunhão se queremos ter em conta uma estrutura de regulação em geral. Ela serve muito bem para compreender como se daria a relação jurídica numa sociedade hiperconectada e tecnológica. São eles: a lei, a norma, o mercado e a arquitetura.

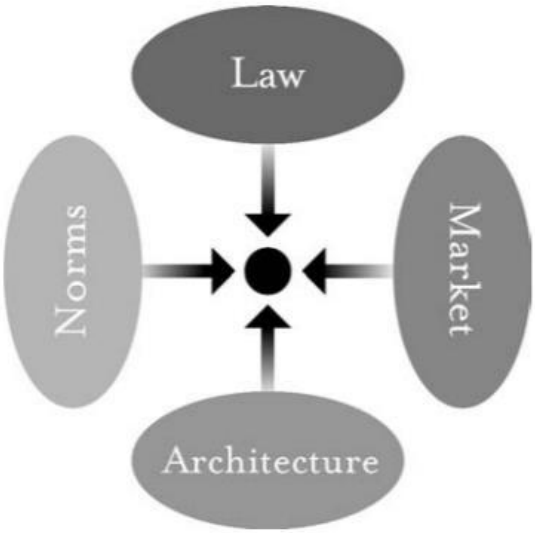

Figura 5: 4 fatores para regulação[46]

A lei é definida como aquilo que é imposto pelo Estado. A norma se enquadra num aspecto mais amplo, pois é o que nasce do seio social e é imposto pela sociedade e não apenas pelo Estado. A diferença entre as duas não está na força de quem pune, mas na fonte de punição: estado para a lei, norma para a sociedade.

O mercado traz também sua obrigação embutido nele. Você pode fazer ou ter X, se pagar Y. Gera uma obrigação, possui suas próprias regras. Assim como o mercado, a arquitetura não traz uma punição *ex post*, mas está lá, faz parte da estrutura da natureza. Se um bloco de

[45] LESSIG, Lawrence. Free Culture. Nova York: The Peguin Press. 2004.
[46] LESSIG, Lawrence. **Free Culture.** Nova York: The Penguin Press. 2004. Página 121.

500 quilos cai, é lei da física. Se uma passagem aérea no valor de US$ 500 impede você viajar, é a lei do mercado.

Não basta impor a lei sem ter em conta a nova arquitetura tecnológica própria da Infoesfera. Se o fizer, produzirá uma legislação ineficazes e sem sentido. Recentemente foi sugerido um Projeto de Lei[47] para regulação de Inteligência Artificial em que não houve participação de todos os setores da sociedade que poderiam ser impactados por essa PL e por isso, mesmo que aprovada e colocada em vigor, não será eficiente e efetiva como pede nosso Código de Processo Civil de 2015 em seus arts. 4º. e 8º. Ao desejar tutelar um bem, a lei não conseguiria alcançar seu fim por não levar em conta os limites da arquitetura dos sistemas. Além disso, pode até possuir eficácia jurídica, mas não terá eficácia social.

5.2 Reconhecimento facial, *ética e law by design*

O que seria *Ética e Law by Design?* Seria a elaboração de critérios e princípios éticos e jurídicos, alinhados às possibilidades técnicas, embutidos em todo o desenho e estrutura dos sistemas computacionais de inteligência artificial com o objetivo de evitar a violação aos direitos humanos e normas legais em seu uso e aplicação.

Richard Susskind em *Tomorrow Lawyers* explica sobre as tendências futuras no direito e afirma que num futuro próximo as regras legais já estarão inseridas nos sistemas e processos. Ele chama isso de *Embedded Legal Knowledge* (Conhecimento legal embutido).[48]

Por exemplo, um carro só poderia ligar após fazer um exame do grau de sobriedade do condutor. Ultrapassando os limites de velocidade permitidos o carro não funcionaria. A arquitetura do sistema, como diria Lessig, já estaria estruturada desde a lei. Isso conduz a um conjunto de resultados bem interessantes na sociedade como um todo. Um deles é que as normas regulatórias e respeito aos direitos humanos já estariam inseridos no sistema, diminuindo drasticamente as infrações.

---

[47] Projeto de Lei 21/2020.
[48] SUSSKIND, Richard. Tomorrow Lawyers. Oxford: Oxford University Press. 2017. Página 51.

Atualmente, agentes sociais devem conhecer a lei e respeitá-la. Em caso de descumprimento, sofrer a sanção necessária. Mas isso não respeita a lógica híbrida da vida *onlife*. E por outro lado, dependendo da área de atuação, a complexidade é tão grande que fica às vezes até difícil cumprir todas as exigências da lei; pense, por exemplo, em nosso sistema tributário.[49] Isso conduz a um conjunto de resultados bem interessantes na sociedade como um todo:

1) as pessoas não precisariam conhecer a lei para poder obedecê-las, o conhecimento estaria no próprio sistema;
2) seria mais fácil para as empresas seguirem as determinações da própria lei, pois o sistema já estaria de acordo com ela;
3) as normas regulatórias já estariam inseridas no sistema, diminuindo drasticamente as infrações;
4) os advogados já não necessitariam chamar a atenção dos clientes para circunstâncias legais;
5) haveria a autoexecução de contratos, o que podemos já presenciar com os *smarts contracts*;
6) execuções de processos e provisões poderiam ser feitos automaticamente sem a necessidade de advogados;
7) surgiria um novo nicho de atuação jurídica para os advogados: o "*legal knowledge engineer*". [50]

Os serviços jurídicos ficarão cada vez mais padronizados e computadorizados, advogados serão necessários para analisar, descartar e organizar uma quantidade gigante e complexa de materiais e processos legais. Serão cada vez mais necessários profissionais para criar procedimentos e replicar nos sistemas computadorizados todo o conhecimento legal. Eles ajudarão a desenhar sistemas que já contenham as normas legais do próprio negócio.

---

[49] Segundo Instituto Brasileiro de Planejamento e Tributação são editadas, no Brasil 2,14 normas tributárias por hora (dia útil). Disponível em: https://www.migalhas.com.br/quentes/313899/brasil-tem-mais-de-790-mil-normas-vigentes-foram-mais-de-6-mi-editadas-desde-a-cf-88. Acessado no dia: 10 de julho de 2020.
[50] The Legal Knowledge Engineer foi traduzido como Engenheiro de Conhecimento jurídico. (Tradução Livre do autor do artigo). Ibidem. Página 135.

Helena Haapio em seu artigo *Introduction to Proactive Law: a Businnes Lawyer View* faz uma distinção entre direito preventivo e direito proativo.[51] E para explicar melhor a distinção entre ambos, usa uma analogia médica. Enquanto a medicina preventiva trabalha para que a pessoa não fique doente, a medicina proativa trabalha para promover o bem-estar e a saúde do paciente. O direito preventivo atuaria mais nos efeitos e consequências, o direito proativo atuaria nas causas promovendo a saúde das relações jurídicas de tal modo a não gerar efeitos e consequências negativas.

Deste modo, através de uma *ética e law by desing* seria possível inserir nos sistemas de reconhecimento facial um conjunto de regras que permitiriam a promoção de um direito proativo? Já seria possível inserir nos sistemas um conjunto de regras computacionais capazes de um desenvolvimento da tecnologia que não fira os direitos humanos? Tudo indica que esse será um caminho a trilhar, pois para problemas tecnológicas, também são necessárias soluções tecnológicas.

[51] HAAPIO, Helena. Introduction to Proactive Law: A Businnes Lawyer View. In WAHLGREN, Peter. Scandinavian Studies in Law: A Proactive Approach. Stockholm: Stockholm Institute for Scandinavian Law. 2010. Volume 49, página 24.

CONCLUSÃO

O convite a uma reflexão ética no uso de tecnologias na segurança pública deve ser precedido também pelo debate público sobre o caráter ético da punição que vá além de considerações sociológicas, econômicas, antropológicas e jurídicas e que "tenha por objetivo estabelecer os fundamentos do sistema de segurança no estado democrático de direito", [52] como afirma o Prof. Vicente Barretto, deve abarcar tanto o conceito de responsabilidade moral, quanto jurídica. [53] Um reflexão sobre o conceito de direitos humanos se faz necessária, já que será o valor primordial muitas vezes violado no uso equivocado do reconhecimento facial.

O reconhecimento facial está em ritmo de desenvolvimento e implementação exponencial na sociedade. Citamos vários exemplos de abusos e desrespeito aos direitos humanos. A simples proibição da tecnologia sem compreender a atual realidade social parece indicar que não terá efeito numa nova sociedade da informação.

É possível corrigir essa tecnologia de tal modo a impedir que desrespeite os direitos humanos? É possível proibi-la? Devemos proibi-la? Ela trará mais malefícios que benefícios? É possível que uma *Ética* e *Law by Design* permitam que os algoritmos de reconhecimento facial respeitem os direitos humanos? Seria essa uma forma de regulação que já traga sistemas alinhados com os valores sociais? Estaríamos numa espécie de direito proativo digital? Quais os limites? Quais os impactos?

Além da apresentação dos riscos no uso de RF, e do arcabouço legal que está sendo elaborando no mundo e no Brasil devido a nossa sociedade de dados, percorremos o itinerário refletindo sobre a condição de possibilidade de inserir no próprio desenho e treinamento dos sistemas valores éticos e jurídicos necessários para promover os direitos humanos dentro do contexto de uma política de segurança pública da cidade.

Durante a pesquisa encontramos muitos artigos e literatura que ressaltam os aspectos negativos da tecnologia. Observamos no meio acadêmico um certo tecnopânico. Poucos autores

---

[52] Disponível em: https://www.institutomillenium.org.br/por-que-punir-por-um-debate-etico-transparente-e-democratico/. Acessado em: 18 de Julho de 2020.

[53] BARRETO, Vicente. Perspectivas Éticas da Responsabilidade Jurídica. In: Quaestio Iuris. 2013. Vol. 06, no. 02, p.257-278.

focam em promover os aspectos positivos da inteligência artificial em geral. Se por um lado, parece ser um contrapeso ao uso dela no mercado. Por outro lado, consideramos que seria importante abordar também o quanto a tecnologia já está contribuindo positivamente e como podemos promover e escalar o uso positivo da mesma.

Também são poucas as legislações no mundo que abordam o uso de reconhecimento facial para vigilância pública, bem como no Brasil, que possui uma lacuna jurídica nessa matéria.

Muito ainda tem que ser estudando. E esse trabalho apresenta alguns caminhos. Essa jornada só será trilhada corretamente com um profundo estudo técnico de como funciona a tecnologia de RF com suas limitações e potencialidades; com a união multidisciplinar de pensadores que atuam diretamente com a problemática; com a educação e engajamento de toda a sociedade em sua diversidade; com defesa da capacidade epistemológica do ser humano através do diálogo, da reflexão e da investigação de encontrar a verdade; com a busca de princípios axiológicos norteadores; e com o resgate de princípios e ferramentas jurídicas que permitam a busca e realização do bem comum.

REFERÊNCIAS

ASHLEY, Kevin D. **Artificial Intelligence and Legal Analytics**: New Tools for Law Practice in the Digital Era. New York: Cambridge University, 2017.

BARRETTO, V. P.. **O Fetiche dos Direitos Humanos e outros temas**. 2. ed. Porto Alegre: Livraria do Advogado, 2013. v. 1. 372p .

BARRETTO, V. P.. **Perspectivas Éticas da Responsabilidade Jurídica**. Quaestio Iuris (Impresso), v. 6, p. 257-278, 2013.

BARRETTO, V. P.; Narciso Leandro Xavier Baez . **Direitos Humanos em Evolução**. 1a.. ed. Joaçaba: Editora UNOESC, 2007. v. 1. 373p .

BARTON, Benjamin H.; BIBAS, Stephanos. **Rebooting Justice**: More Technology, Fewer Lawyers and the Future of Law. Nova York: Encounter Books, 2017. **Modernidade Líquida**. Rio de janeiro: Jorge Zahar, 2001.

BAUMAN, Zygmunt. Modernidade e Ambivalência. Rio de Janeiro. Zahar, 1991.

BOBBIO, Norberto. **A Era dos Direitos.** São Paulo: GEN LTC, 2004.

BRANDOM, R.(2018)'Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense.'The Verge. Disponível em https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy . Acessado em 10 de agosto de 2021.

BRASIL. **Projeto de Lei 21/2020**. Marco Legal do Desenvolvimento e Uso da Inteligência Artificial. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 10 de agosto de 2021.

_____. **Lei Federal 13.709,** de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 de Agosto de 2020.

_____. **Decreto-Lei 6.712**, de 10 de novembro de 2020, Distrito Federal. Sobre uso de Reconhecimento facial na Vigilância Pública. Disponível em:

https://sintse.tse.jus.br/documentos/2020/Nov/11/para-conhecimento-institucional/lei-no-6-712-de-10-de-novembro-de-2020-dispoe-sobre-o-uso-de-tecnologia-de-reconhecimento-facial-trf. Acesso em: 10 de agosto de 2021.

_____. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/wp-content/uploads/sites/41/2020/11/dadosanteprojetocomissaoprotecaodadossegurancapersecucaofinal_051120204929.pdf . Acessado em: 15 de Agosto de 2021.

_____. **Decreto Federal 10.046**, de 9 de outubro de 2019. Sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm . Acesso em: 20 de setembro de 2019.

BREY, P. **Ethical Aspects of Facial Recognition Systems in Public Places**.Journal of Information, Communication, and Ethics in Society vol.2: 97-109, 2004.

DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate machine learning will remake our world. Nova York: Basic Books, 2015.

FLORIDI, Luciano. **Scepticism and the Foundation of Epistemology - A Study in the Metalogical Fallacies**. Leiden: Brill, 1996.

FLORIDI, Luciano. **The Blackwell Guide to the Philosophy of Computing and Information**. Oxford : Blackwell Publishing, 2003.

GARVIE, C. **Garbage In, Garbage Out: Face Recognition on Flawed Data**. Georgetown Law Center on Privacy and Technology, 2019. Disponível em https://www.flawedfacedata.com/. Acessado em: 20 de agosto de 2021.

GARVIE, C., BEDOYA A., and FRANKLE J. **The Perpetual Line-Up: Unregulated Police Face Recognition in America.** Georgetown Law Center on Privacy and Technology, 2016. Disponível em: https://www.perpetuallineup.org/. Acesso em 20 de Agosto de 2021.

GARVIE, C.; MOY, L. **America Under Watch: Face Surveillance in the United States**. Georgetown Law Center on Privacy and Technology, 2019. Disponível em https://www.americaunderwatch.com. Acesso em: 20 de Agosto de 2021.

GILLESPIE, T. **The Relevance of Algorithms**, Media Technologies: Essays on Communication, Materiality, and Society, T. Gillespie, P. Boczkowski, and K. Foot, eds., MIT Press, 2014, pp. 167–194.

HALE, B. **Identity Crisis: Face Recognition Technology and Freedom of the Will'Ethics**, Place & Environment vol. 8(2): 141-158, 2005.

HALLOWELL, N.; PARKER, M. e NELLÅKER, C.. **Big data phenotyping in rare diseases: some ethical issues**. Genetics in Medicine vol. 21(2): 272-274. 2018.

International Biometrics and Identity Association. **Biometrics Explained: Answers to 13 Basic Biometrics Questions**. IBIA, 2018. Disponível em https://www.ibia.org/download/datasets/4346/IBIA-Biometrics-Explained-final-final-web.pdf. Acesso em: 15 de setembro de 2021.

KUHN, Thomas S. **A estrutura das revoluções científicas**. 5. ed. São Paulo: Editora Perspectiva S.A, 1997.

KURZWEIL, Ray. **The Age of Intelligent Machines**. Cambridge: MIT, 1990. LEGG, S.;

LATOUR, Bruno. **Como se orientar politicamente no Antropoceno: Volume 1.** São Paulo: Bazar do Tempo, 2020.

LATOUR, Bruno. **Investigação sobre os modos de existência: Uma antropologia dos modernos.** São Paulo: Vozes, 2019.

LÉVINAS, E. **Totality and Infinity: An essay on Exteriority**. Pittsburgh: Duquesne University Press, 1969.

MARTIJN, Van Otterlo. **A machine learning view on profiling**. HILDEBRANDT, Mireille; DE VRIES, Katja (eds.). Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology. Abingdon: Routledge, 2013.

MATA-MACHADO, Edgar G. **Contribuição ao Personalismo Jurídico.** São Paulo: Del Rey, 2000.

MITTELSTADT, Brent Daniel et al. **The ethics of algorithms**: Mapping the debate. Big Data & Society, 1-21, jul.- dez. 2016.

PASQUALE, F. **The Black Box Society**: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.

PERUZZOTTI, Enrique. **Accountability.** In: Corrupção: ensaios e críticas. Belo Horizonte: Editora UFMG, 2008, p.477-483.

SAMUDZI, Z.. **Bots Are Terrible at Recognizing Black Faces: Let's Keep It That Way**. DailyBeast, 2018. Disponível em: https://www.thedailybeast.com/bots-are-terrible-at-recognizing-black-faces-lets-keep-it-that-way. Acesso em 10 de setembro de 2021.

SELINGER, Evan; LEONG, Brenda. **The ethics of facial recognition technology**. Forthcoming in The Oxford Handbook of Digital Ethics. Carissa Véliz, 2021. Disponível em https://ssrn.com/abstract=3762185. Acesso em: 10 de agosto de 2021.

SUPREMO TRIBUNAL FEDERAL. **Medida Cautelar em Mandado de Segurança 28.187**, Distrito Federal, 2021. Disponível em https://www.conjur.com.br/dl/gilmar-brasil-paralelo.pdf. Acesso em: 20 de setembro de 2021.

SUSSKIND, Richard. **Tomorrow Lawyers: An Introduction to Your Future**. 2. ed. London: Oxford University, 2017.

SUSSKIND, Richard; SUSSKIND, Daniel. **The Future of Professions: How Technology Will Transnform the Work of Human Experts**. Oxford: Oxford University, 2015.

THIERER, A. **The Great Facial Recognition Technopanic of 2019**. The Bridge, 2019. Disponível em https://www.mercatus.org/bridge/commentary/great-facial-recognition-technopanic-2019. Acesso em: 10 de Julho de 2021.

TURING, Alan. **Computing Machinery and Intelligence.** Mind, New Series, v. 59, n. 236 p. 433-460, out. 1950.

VALENTINI, Rômulo Soares. **Julgamento por computadores? As novas possibilidades da juscibernética no século XXI e suas implicações para o futuro do direito e do trabalho dos juristas.** Tese (Doutorado em Direito do Trabalho) – Faculdade de Direito, Universidade Federal de Minas Gerais. Belo Horizonte, 2017.

VILLEY, Michel. **O direito e os direitos humanos.** São Paulo: WMF Martins, 2016.
XAVIER, José Roberto F.. **O sistema de direito criminal e a racionalidade penal moderna:**

ilustrações empíricas de dificuldades cognitivas em matéria de penas. Revista Brasileira de Ciências Criminais, v. 18, p. 271-311, 2010.

YEUNG, K. **An introduction to law and regulation**, Cambridge: Cambridge University Press, 2007.