XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

MAIQUEL ÂNGELO DEZORDI WERMUTH

Copyright © 2022 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Diretora Executiva - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - UNIVEM/FMU – São Paulo
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR – Ceará

Representante Discente: Prof. Dra. Sinara Lacerda Andrade – UNIMAR/FEPODI – São Paulo

Conselho Fiscal:
Prof. Dr. Caio Augusto Souza Lara – ESDHC – Minas Gerais
Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro
Prof. Dr. José Filomeno de Moraes Filho – Ceará
Prof. Dr. Lucas Gonçalves da Silva – UFS – Sergipe
Prof. Dr. Valter Moura do Carmo – UNIMAR – São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Daniela Marques De Moraes – UNB – Distrito Federal
Prof. Dr. Horácio Wanderlei Rodrigues - UNIVEM – São Paulo
Prof. Dr. Yuri Nathan da Costa Lannes - Mackenzie – São Paulo
Comunicação:
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul
Profa. Dra. Maria Creusa De Araújo Borges - UFPB – Paraíba
Prof. Dr. Matheus Felipe de Castro - UNOESC – Santa Catarina
Relações Internacionais para o Continente Americano:
Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM – Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão
Relações Internacionais para os demais Continentes:
Prof. Dr. José Barroso Filho – ENAJUM
Prof. Dr. Rubens Beçak - USP – São Paulo
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná
Eventos:
Prof. Dr. Antônio Carlos Diniz Murta - Fumec – Minas Gerais
Profa. Dra. Cinthia Obladen de Almendra Freitas - PUC – Paraná
Profa. Dra. Livia Gaigher Bosio Campello - UFMS – Mato Grosso do Sul

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UMICAP – Pernambuco

I61

Internet: dinâmicas da segurança pública e internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Maiquel Ângelo Dezordi Wermuth.

– Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-609-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXIX Congresso Nacional do CONPEDI Balneário Camboriu - SC (3: 2022: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXIX CONGRESSO NACIONAL DO CONPEDI BALNEÁRIO CAMBORIU - SC

INTERNET: DINÂMICAS DA SEGURANÇA PUBLICA E INTERNACIONAL

Apresentação

Apresentação

É com imensa satisfação que apresentamos a obra que reúne os artigos apresentados no Grupo de Trabalho "INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL I", durante o XXIX Encontro Nacional do CONPEDI, no dia 9 de dezembro de 2022, no Campus de Balneário Camboriú da UNIVALI.

O artigo de Danielle Jacon Ayres Pinto e Rafael Gonçalves Mota, intitulado "A GUERRA CIBERNÉTICA COMO A QUINTA DIMENSÃO DA GUERRA MODERNA E O SEU ENFRENTAMENTO CONSTITUCIONAL NO BRASIL" analisa a relação entre a evolução tecnológica, especialmente a importância que a rede mundial de computadores passou a ter na vida cotidiana dos indivíduos, instituições e estados e os conflitos bélicos, notadamente considerando que a guerra através de meios virtuais e cibernéticos passou a ser a quinta dimensão possível de desenvolvimento bélico, seguindo o mar, terra, ar e espaço.

Ezequiel De Sousa Sanches Oliveira e Greice Patricia Fuller, no artigo "A GUERRA CIBERNÉTICA NO CONTEXTO DAS CIDADES INTELIGENTES NO MUNDO PÓS-PANDÊMICO: PROVOCAÇÃO ANALÍTICA SOB O VIÉS DA CIBERSEGURANÇA /HACKING", abordam o uso da internet no contexto das "Smart Cities", salientando que a rede mundial de computadores é tomada como tecnologia da informação e comunicação, por impactar as ações humanas, razão pela qual deve passar por uma reflexão sob o viés da defesa cibernética no que toca à segurança da informação, notadamente no cenário descortinado pelo mundo pós-pandêmico, marcado pela profusão da cibercultura e da disseminação do universo hacker.

O artigo intitulado "A VIRADA TECNOLÓGICA E O PRINCÍPIO DA NECESSIDADE EM DAVID SCHMIDTZ: A QUESTÃO DA SEGURANÇA PÚBLICA NA ERA DO COVID19", de autoria de Feliciano Alcides Dias, Fabiel dos Santos Espíndola e Ubirajara Martins Flores, a partir da teoria pluralista da justiça de David Schmidtz, destaca que a transição da modernidade para a hipermodernidade é marcada por um descompasso imposto pela rapidez da evolução das ferramentas de tecnologia da informação e da comunicação e pelo desenvolvimento dessas atividades na Segurança Pública. Nesse sentido, a alternativa

encontrada na teoria de David Schmidtz propõe o respeito à individualidade das pessoas que, na sua concepção, significa justiça.

Em “ASPECTOS DIFERENCIADORES EM CURSOS DE FORMAÇÃO BÁSICA POLICIAL MILITAR”, Anderson Morais De Oliveira tematiza a formação policial no Brasil, apontando para a existência dos chamados currículos “ocultos” na formação de soldados da Polícia Militar. O estudo destaca as condições que fomentam o ingresso na carreira policial, alguns aspectos da cultura corporativa interna, bem como o aspecto influenciador nas relações de poder da atividade policial.

O artigo de Maiquel Ângelo Dezordi Wermuth e Fernando Antonio Sodre De Oliveira, sob o título “DA BIOPOLÍTICA DE MICHEL FOUCAULT À NECROPOLÍTICA DE ACHILLE MBEMBE: A FUNÇÃO DO RACISMO NA DIMENSÃO ESTRUTURANTE DA SEGURANÇA PÚBLICA NO BRASIL”, explora a possível conexão entre os conceitos de biopolítica (desenvolvido no percurso filosófico de Michel Foucault) e de necropolítica (que ocupa lugar de centralidade na filosofia de Achille Mbembe), perquirindo qual é a função que o racismo desempenha tanto no exercício do biopoder quanto do necropoder. Além disso, o texto busca-se analisar de que forma o racismo estrutura os Estados a partir da Modernidade, notadamente no que se refere à sua atuação no campo da segurança pública, ainda profundamente marcado pela seletividade étnico-racial.

No artigo “DESAFIOS À LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL: ENTRE O DIREITO À PRIVACIDADE E AS ROBOCALLS”, Matheus Adriano Paulo e Gilson Jacobsen analisam a oferta de produtos e serviços por meio de “Robocalls”, que são uma espécie de Inteligência Artificial desenvolvida para fazer ligações, emulando a ação humana e desafiando a melhor aplicação possível da Lei Geral de Proteção de Dados - LGPD, que pode e deve servir de freio a eventuais violações ao direito de privacidade dos cidadãos.

Em “DIREITO AO ESQUECIMENTO COMO FERRAMENTA TRANSNACIONAL PARA O ARMAZENAMENTO DE DADOS MAIS SUSTENTÁVEL”, Jaine Cristina Suzin, Jardel Anibal Casanova Daneli e Paulo Márcio da Cruz abordam a insustentabilidade do Armazenamento de Dados na Internet perante as dimensões ambiental, social e econômica, em um cenário que pode ser denominado de sociedade da informação transnacional. Nesse contexto, estudam a viabilidade do Direito ao Esquecimento enquanto ferramenta transnacional para a emergência da Sustentabilidade.

O artigo intitulado “ERA DA IA E O 5G: QUAL A VELOCIDADE DA (DES) INFORMAÇÃO?”, de Patrícia da Silva Almêda Sales e Debora Bonat, analisa a relação circunscrita entre a Inteligência Artificial (IA) e o Direito, especialmente no que diz respeito à desinformação na participação democrática com a expansão do 5G, enfocando as possíveis implicações na próxima fase de comunicação e compartilhamento de informações na 5ª geração de banda larga móvel, a exemplo da repressão digital, da vigilância em massa, do perfil de usuário aprimorado e microsegmentação etc.

No texto “FAKE NEWS E O PROCESSO ELEITORAL, A BUSCA PELO ENFRENTAMENTO E DIMINUIÇÃO DO FENÔMENO”, Rennan Gonçalves Silva, Lucas Gonçalves da Silva e Karla Thais Nascimento Santana discutem os impactos das fake news no processo eleitoral e analisam as medidas de enfrentamento a essas notícias durante o período eleitoral.

“O DILEMA DO SUJEITO MONITORADO NO PÓS-MUROS DO SISTEMA PRISIONAL” é o título do artigo e Joice Graciele Nielsson e Adriane Arriens Fraga Bitencourt, que analisa a posição do sujeito em monitoração eletrônica no sistema penal, ressaltando a necessidade de implementação de políticas públicas de apoio a esses sujeitos, com o efetivo acompanhamento de equipe multidisciplinar como condição mínima para a garantia da maior efetividade do sistema de liberdade monitorada.

Em “O DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS NA SEGURANÇA PÚBLICA E ÂMBITO PENAL: POSSIBILIDADES E DESAFIOS”, Joice Graciele Nielsson e Milena Cereser da Rosa abordam a proteção de dados pessoais enquanto direito fundamental e os desafios e possibilidades para a construção de uma Lei Geral de Proteção de Dados (LGPD) no âmbito da segurança pública e penal, como forma de garantir o direito fundamental a proteção de dados pessoais, diante da necessidade de equilibrar a privacidade e a efetividade da jurisdição penal, de modo a não prejudicar tanto o sistema jurisdicional quanto o titular do direito à proteção dos dados.

Mariana Chini e Maiquel Ângelo Dezordi Wermuth, no artigo “O “FUTURO” SOBRE CORPOS PENALIZADOS: TECONOLOGIA, SISTEMA PENAL E MONITORAÇÃO ELETRÔNICA DE PESSOAS” abordam os avanços da tecnologia no sistema penal, tendo por escopo central a monitoração eletrônica de pessoas, especialmente no contexto brasileiro, perspectivada a partir da estigmatização de pessoas eletronicamente monitoradas na esfera penal.

“RECONHECIMENTO FACIAL E (IN)SEGURANÇA PÚBLICA: VIOLAÇÃO A DIREITOS DA PERSONALIDADE IMPULSIONADA PELO EXCESSO DE VIGILÂNCIA” é o título do texto de Micaela Mayara Ribeiro, Vinícius Fachin e Zulmar Antonio Fachin, que analisa o uso da tecnologia de reconhecimento facial na segurança pública, aferindo os impactos que o excesso de vigilância pode ocasionar nos direitos da personalidade dos cidadãos

Por fim, Maite Neves Guerra e Thiago Santos Aguiar de Pádua, no artigo intitulado “VALIDADE JURÍDICA DO PRINT SCREEN DE WHATSAPP COMO PROVA NO PROCESSO PENAL”, discutem a necessidade de validação e autenticação de provas digitais, em especial as conversas do aplicativo WhatsApp, sugerindo o auxílio das novas tecnologias.

O(a) leitor(a), por certo, perceberá que os textos aqui reunidos, além de ecléticos, são críticos quanto à realidade a utilização das novas tecnologias na contemporaneidade – notadamente no campo da segurança pública e da segurança internacional–, o que reflete o compromisso dos(as) autores(as) na busca pela adequação do uso dessas tecnologias aos textos convencionais e constitucionais centrados na dignidade da pessoa humana.

Tenham todos(as) uma ótima leitura! É o que desejam os organizadores.

Danielle Jacon Ayres Pinto – UFSC

Maiquel Ângelo Dezordi Wermuth - UNIJUÍ

RECONHECIMENTO FACIAL E (IN)SEGURANÇA PÚBLICA: VIOLAÇÃO A DIREITOS DA PERSONALIDADE IMPULSIONADA PELO EXCESSO DE VIGILÂNCIA

FACIAL RECOGNITION AND PUBLIC INSECURITY: PERSONALITY RIGHTS VIOLATION DRIVEN BY EXCESS SURVEILLANCE

Micaela Mayara Ribeiro [1]
Vinícius Fachin [2]
Zulmar Antonio Fachin [3]

Resumo

Trata-se de um estudo sobre o uso da tecnologia de reconhecimento facial na segurança pública. O objetivo é estudar os impactos que o excesso de vigilância pode ocasionar nos direitos da personalidade dos cidadãos. Tais impactos podem ser positivos, no sentido de ampliar sua proteção aos direitos da personalidade, ou negativos, acarretando violações a tais direitos. Partindo da premissa de que o reconhecimento facial trata de dado biométrico, inclui-se no estudo os dispositivos previstos na Lei Geral de Proteção de Dados e indaga a possibilidade de sua aplicação. Utilizando-se do método dedutivo, foi realizada a busca de informações em livros, artigos científicos, legislações e demais documentos aptos ao desenvolvimento da pesquisa. Os resultados da pesquisa indicam que a implementação da tecnologia de reconhecimento facial pode ter mais impactos negativos do que positivos na segurança pública, vez que a tecnologia aplicada não pode ser considerada apta a lidar com certas peculiaridades do mesmo modo que a mente humana.

Palavras-chave: Tecnologia, Discriminação, Algoritmo, Direitos da personalidade, Dados pessoais

Abstract/Resumen/Résumé

This study treats about the use of facial recognition technology in public safety. The aim is to study the impacts that excessive surveillance can have on citizens' personality rights. Such impacts are positive, in the sense of expanding the protection of personality rights, or negative for violate such rights. Based on the premise that facial recognition deals with biometric data, the study includes the provisions of the General Data Protection Law. The

[1] Graduada em Direito pela UniCesumar. Especialista em Direito Digital e Proteção de Dados pela EBRADI. Mestranda em Ciências Jurídicas na UniCesumar. Bolsista CAPES. Advogada. E-mail: micaela-mayara@hotmail.com. ORCID - 0000-0002-6881-2748.

[2] Graduado em Direito e em Sistemas de Informação pela PUCPR. Especialista em Direito do Trabalho e Direito Previdenciário (IDCC/UENP). Mestrando em Direito, Sociedade e Tecnologias nas Faculdades Londrina. ORCID 0000-0001-5928-3744

[3] Doutor em Direito Constitucional (UFPR). Mestre em Direito (UEL). Mestre em Ciência Política (UEL). Bacharel em Direito (UEM). Bolsista Produtividade em Pesquisa do ICETI. ORCID 0000-0001-5514-5547.

deductive method was used, searching for information in books, scientific articles, legislation and other documents to research development. The research results indicate that the application of facial recognition technology may have more negative than positive impacts on public safety, since the technology hitherto applied cannot be considered able to deal with certain peculiarities in the same way as the human mind.

Keywords/Palabras-claves/Mots-clés: Technology, Discrimination, Algorithm, Personality rights, Personal data

1 INTRODUÇÃO

A presença de determinados mecanismos tecnológicos passa despercebida por grande parte das pessoas, mesmo que elas tenham se tornado parte do cotidiano, como no caso do desbloqueio de *smartphones* por meio da tecnologia de reconhecimento facial e da verificação de identidade em aplicativos que utilizam do mesmo mecanismo. A ascensão da tecnologia não aconteceu repentinamente e apenas nos últimos anos, sobretudo em razão da pandemia de covid-19. Na realidade, os passos sutis da revolução digital estão presentes há muito tempo.

Não só no cotidiano individual dos integrantes da sociedade, ferramentas digitais passaram a integrar também espaços públicos comuns, como as ruas, na busca de atingir o máximo de efetividade na segurança pública. Exemplo disso é a utilização da ferramenta de reconhecimento facial nas câmeras de videomonitoramento para identificar suspeitos de crimes e foragidos.

A pesquisa tem como objetivo estudar os impactos que a supervigilância pode ocasionar nos direitos da personalidade dos cidadãos. Já os objetivos específicos são averiguar se recorrer a tecnologia para garantir uma melhor segurança pública, acaba por gerar o efeito contrário, como a insegurança pública e logo na sequência, traçar uma correlação entre a Lei Geral de Proteção de Dados Pessoais e a aplicação da tecnologia de reconhecimento facial.

O problema da pesquisa gera o seguinte questionamento: o uso da tecnologia de reconhecimento facial para garantir a segurança pública se sobrepõe à proteção dos direitos da personalidade?

Para responder ao questionamento, o estudo considera a hipótese de que a implementação da tecnologia de reconhecimento facial para garantir a segurança pública sem nenhuma regulamentação específica acaba por violar direitos da personalidade.

A metodologia adotada foi a dedutiva, buscando informações em livros, artigos científicos, pesquisas desenvolvidas por centros de estudos, legislações, em especial no ordenamento jurídico brasileiro, e demais documentos aptos ao desenvolvimento da pesquisa.

O artigo está dividido em três partes, além da presente introdução e conclusão. A primeira trata sobre a Inteligência Artificial (IA) e a tecnologia de reconhecimento facial, correlacionando as similaridades entre as inteligências humana e artificial, bem como trazendo alguns aspectos do reconhecimento facial.

A segunda parte estuda a implementação da tecnologia de reconhecimento facial na segurança pública e os impactos que pode causar nos direitos da personalidade humana. Ao

mesmo tempo, traça pontos importantes sobre a discriminação algorítmica, levantando a indagação sobre os limites da sobreposição da aplicação de tecnologias que colocam em risco direitos fundamentais, como a proteção de dados pessoais.

Por fim, dispõe sobre a inexistência de regulamento específico no ordenamento jurídico brasileiro acerca do uso da tecnologia de reconhecimento facial, especialmente para a segurança pública e os prejuízos que a implementação da tecnologia de reconhecimento facial sem regulamentação específica pode ocasionar.

Ao final, a pesquisa identificou a existência de obscuridades, vez que, ao priorizar a otimização da segurança pública, ignoram-se outros direitos fundamentais como a proteção de dados pessoais.

2 INTELIGÊNCIA ARTIFICIAL E TECNOLOGIA DE RECONHECIMENTO FACIAL

Não causa surpresa o fato de que a tecnologia está mudando a rotina das pessoas em uma escala global e atos considerados impraticáveis por mãos humanas, até pouco tempo, tornaram-se possíveis graças à tecnologia. O que assombra, no entanto, é a longínqua ideia de que a tecnologia terá, em algum momento, autonomia capaz de se sobrepor a decisões humanas. De certa forma, pensar nessa possibilidade estremece até os mais vanguardistas. Há dez ou vinte anos atrás, era inimaginável o elevado patamar que a tecnologia alcançaria nos dias atuais e os impactos que essa progressão acarretaria nos mais variados cenários.

Atrelada ao desenvolvimento da tecnologia está o surgimento da Inteligência Artificial (IA), identificada como um conjunto de comandos informacionais estruturados para oferecer respostas, de acordo com um banco de dados fornecido. Esse sistema é chamado de algoritmo (VALENTINI, 2017, p. 42). A acepção do vocábulo foi realizada em 1956, por John McCarthy, conhecido como um dos pais fundadores da IA, em proposta apresentada na Conferência de Dartmouth, a qual tratava de temas sobre computação, redes neurais, aleatoriedade, criatividade e abstrações. A proposta era utilizar a linguagem complementada pela matemática, fazendo com que o computador fizesse mais do que cálculos.

No caso da IA, a palavra “inteligência” tem como parâmetro a inteligência humana e tem a pretensão de fazer com que uma ferramenta apresente um desempenho similar ou, até mesmo, mais eficiente que o homem. Isso não significa que 100% dos atos que antes eram realizados por mãos humanas passarão a ser praticados exclusivamente pela IA.

Com a automatização dos objetos, atos humanos como se deslocar até o interruptor para acender ou apagar a luz não serão mais necessários, pois há dispositivos acoplados à IA que podem controlar aparelhos eletrônicos de qualquer lugar por meio do comando de voz. Note-se que ainda não há autonomia, pois será necessária a intervenção humana para efetuar o comando da ação. Se fosse completamente independente, a IA acenderia e apagaria a luz da forma que lhe fosse conveniente, sem a necessidade de comando humano.

Apesar da semelhança entre eles, revela-se de grande importância distinguir a IA e o cérebro humano. O cérebro humano é composto por dois hemisférios que se conectam a partir de um feixe de fibras nervosas, o corpo caloso. O lado esquerdo processa principalmente material objetivo, como matemática e linguagem, enquanto o lado direito é responsável por habilidades mais subjetivas (PINTO et al, 2013). A capacidade cognitiva do ser humano permite que exista certa relação de confiança entre pessoas, na certeza de que a conversa é realizada entre sujeitos determinados. Em outras palavras, a mente humana tem a capacidade de reconhecer a face das pessoas e diferenciá-las, como parentes, amigos, conhecidos e rostos apenas familiares.

A IA não tem a mesma habilidade própria de cognição, visto que apenas replica os códigos registrados. Cada ser humano possui características distintas e personalíssimas que os tornam únicos e inconfundíveis entre si. Não só traços físicos, mas também emoções que se externalizam por meio de expressões faciais e que também são distintas em cada um. É possível saber quando alguém está triste, zangado ou feliz, sem exarar palavra alguma, apenas olhando para seu rosto. Pode-se dizer que o reconhecimento facial humano é a mais natural das técnicas biométricas (ZIMMERMANN, 2003, p. 19).

Com o passar do tempo e a evolução da tecnologia, pensou-se na possibilidade de que a máquina também exercesse a habilidade de reconhecimento e essa interação humano-computador foi bastante extensa. Isto porque, há diferença em treinar uma máquina para jogar xadrez, prever movimentos por meio de estatísticas e probabilidades e em reconhecer pessoas com particularidades físicas e emocionais. Pensar em uma computação afetiva é algo muito mais complexo.

Foi relativamente nesse sentido que se inventou a tecnologia de reconhecimento facial, com a pretensão de replicar a habilidade humana em identificar faces em cenários complexos com muito pouco esforço e mesmo sob as variações no estímulo visual (ZIMMERMANN, 2003):

> O reconhecimento se dá através da imagem adquirida da face, que basicamente pode ser do tipo bidimensional ou tridimensional.

> Medidas geométricas da face como distâncias entre olhos e nariz, curvatura da boca e outras ou como o uso de imagens da face como um todo são algumas das técnicas usadas na classificação de faces. É um sistema essencialmente inspirado na biologia visto ser esta a maneira com que os humanos reconhecem os seus semelhantes.

Em outras palavras, o reconhecimento facial funciona, a grosso modo, por meio da comparação e, para que esse reconhecimento seja possível por meio da tecnologia, é necessário que exista um vasto banco de dados. Assim, a estatística deixará de ser apenas uma fórmula e terá a função de comparar de modo automático uma imagem-alvo com cada uma das demais imagens que compõem o referido banco de dados (VIDAL, 2019, p. 222).

A utilização da técnica pode ser subdividida em três categorias em forma de questionamento e a resposta às indagações depende do fim almejado em seu uso: (i) há um rosto na imagem?; (ii) que tipo de rosto há na imagem?; e (iii) a quem pertence o rosto na imagem?" (BUOLAMWINI et al, 2020. p. 2). Essa abordagem híbrida pode ser considerada mais exata, mas ainda assim é passível de erros e pode ser considerada inferior ao reconhecimento de íris oculares e de impressões digitais (ORVALHO, 2019).

Não há dúvidas sobre o aprimoramento de câmeras ao ponto de capturar imagens tão nítidas que identificam imperfeições. Ainda que a evolução das câmeras seja notável e tenha permitido replicar um rosto com pontos nodais específicos de cada um, alguns aparelhos de videomonitoramento podem não conseguir captar a imagem exata em razão de influências externas como a posição da câmera que registrou a imagem, a expressão facial do indivíduo ou elementos como barba, bigode e óculos que podem modificar as características, iluminação, entre outros fatores.

Embora tenha se tornado popular em 2019, o reconhecimento facial vem sendo utilizado no Brasil desde 2011, com o projeto piloto realizado em Ilhéus, na Bahia, o qual tinha por objetivo inicial impedir fraudes no transporte público. Ao longo dos anos, a utilização da ferramenta tecnológica aumentou de modo significativo, principalmente no transporte e segurança pública. Todavia, muitos dos casos reportados publicamente se concentram na eficiência esperada e na implementação e pouco em informar os resultados (INSTITUTO IGARAPÉ, 2019).

Não se sabe até que ponto a sociedade está preparada para aceitar a implementação de uma tecnologia tão invasiva quanto a de reconhecimento facial. Embora não tenha alcançado a maturidade digital, pode-se dizer que o amadurecimento da coletividade para adaptação no contexto tecnológico está engatinhando. O que preocupa, no entanto, é a

maturidade com que aqueles que detém o poder para adquirir uma quantidade incalculável de tecnologias para o bem estar social acabam por utilizar da tecnologia para fins diversos.

3 SEGURANÇA PÚBLICA OU SUPERVIGILÂNCIA?

A pandemia de Covid-19 provocou consideráveis impactos na população em esfera global. O mundo se viu obrigado a cumprir quarentena em suas residências por tempo inestimável e isso fez com que o uso de tecnologia e acesso à Internet aumentasse de forma extraordinária. Uma adaptação tecnológica foi empurrada na sociedade que sequer pode notar o que de fato estava acontecendo.

Sabe-se que o Estado é responsável pela segurança pública (art. 144 da CF), serviço que tem como premissa a prevenção e repressão qualificada, nos limites inerentes à dignidade humana, aos Direitos Humanos e ao Estado democrático de Direito. Assim como os demais direitos fundamentais, a garantia da segurança pública deve ter maior atenção. Nas palavras de Schreiber (2014, p. 163) "Ao Estado compete não apenas zelar pela privacidade nas suas relações com o cidadão, mas também garantir a tutela da privacidade nas relações entre particulares, em especial naqueles setores em que o advento de novas tecnologias vem tomando sua violação particularmente frequente".

Diariamente, informações e dados são cedidos por usuários da Internet durante a navegação, alguns deles de forma consciente, porém outros não. Esse fluxo de dados obtidos com a participação da comunidade, sem dúvida alguma, foi crucial para situações como a contenção do Coronavírus durante a pandemia. No entanto, muitas informações e dados coletados com a justificativa de contenção da propagação do vírus tinham por fim, supostamente, algo muito maior: a vigilância constante.

Os riscos da sociedade da vigilância estão tradicionalmente ligados ao uso político de informações para controle dos integrantes da coletividade, de modo que a vigilância se torna constante nos momentos mínimos da vida, apresentando-se como um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações (COSTA; OLIVEIRA, 2019, p. 11).

Concomitantemente à procura pela imersão ao mundo digital, surgiu a possibilidade do monopólio de informações em larga escala, seja pelo Estado, seja pelo poder privado, transmutando o cotidiano da sociedade em estratégia de comercialização. Não muito longe, surgiu a ideia das cidades inteligentes que tinham por aparente objetivo melhorar o bem-estar

da coletividade e proporcionar o desenvolvimento econômico, em harmonia com o meio ambiente e à sustentabilidade. Esperava-se que as problemáticas antigas fossem resolvidas com o uso da tecnologia, como iluminação, transporte e segurança pública.

A mineração de dados para fins de tomada de decisão é, também, outro atributo das cidades inteligentes. Os dados seriam uma espécie de combustível para a integração entre os setores. É justamente essa integração entre governança e população que traz a efetividade das cidades inteligentes. Todavia, não se deve ignorar a hipótese de que uma cidade de vigilância esteja mascarada como cidade inteligente.

Em outras palavras, embora a tecnologia seja utilizada, em sua maioria, para otimizar a performance da convivência urbana e segurança pública, carrega dados e informações de extrema importância, os quais, usados para fins diversos daqueles para a organização da população, podem causar impactos desastrosos. Ou seja, falar em bem estar da coletividade não se limita a otimizar demandas rotineiras.

Do mesmo modo que arrecadar informações sobre o cotidiano das pessoas possa auxiliar a traçar um perfil de eventual risco para a população, também pode ocasionar um excesso de vigilância. Em outras palavras, a vida humana se torna datificada, não passando de números que circulam nas vias urbanas.

Redirecionando o enfoque para a segurança pública, nos mais variados locais, a tecnologia de reconhecimento facial foi implantada para identificar se as pessoas que por ali passavam faziam o uso de máscaras. De certa forma, isso facilitou a advertência das pessoas pelo descumprimento de decretos que tratavam sobre a necessidade do uso de máscaras em espaços públicos e privados e auxiliou na contenção da propagação do Coronavírus. Paira, no entanto, dúvidas sobre o tratamento das imagens e demais dados obtidos, se foram descartadas ou serviram para outros propósitos.

Antes mesmo da pandemia, o Estado da Bahia já era arquétipo para a implementação da tecnologia de reconhecimento facial. Em 2019, no carnaval de Salvador, um acusado de homicídio foi identificado pelo vídeo policiamento e preso logo em seguida. Na época, foram instaladas câmeras nas ruas que emitiam um alerta às autoridades policiais quando identificava 90% de similaridade entre o suspeito e o cidadão (FOLHA DE SÃO PAULO, 2019).

No entanto, a taxa de sucesso nem sempre é alta. Em paralelo aos pontos positivos da aplicação da tecnologia na segurança pública, surgiram questões alarmantes relacionadas às características únicas de cada ser humano, especialmente a cor da pele. Durante a fase de

testes de aplicação prática da tecnologia, foi possível observar uma "discriminação algorítmica" no uso dessas ferramentas na identificação de suspeitos por crimes.

A grande maioria dos alertas identificavam pessoas negras e inocentes como suspeitos, fazendo com que a polícia local abordasse pessoas de surpresa que não tinham relação com o suspeito, apenas a cor da pele. Uma ilustração impressionante sobre essa questão foi realizada no documentário "Codes Bias", disponível na plataforma de *streaming* Netflix (2020). No documentário, a pesquisadora do *MIT Media Lab*, Joy Buolamwini, revela o lado bárbaro da tecnologia, revelando que não há precisão em muitos *softwares* de reconhecimento facial, quando se trata de identificar rostos de pele escura e de mulheres.

Foram realizados testes como colocar uma máscara branca em pessoas negras para verificar a eficácia da tecnologia e o resultado evidencia muito claramente a discriminação algorítmica. E não se pode culpar a ferramenta por isso. Ficou evidente que a tecnologia apenas reproduz as fissuras sociais existentes na coletividade.

Também no ano de 2019, Governo do Estado do Rio de Janeiro, através da Secretaria de Estado de Polícia Militar (SEPM), implementou um projeto para uso da tecnologia de reconhecimento facial no sistema de videomonitoramento no bairro de Copacabana. Uma análise feita pelo Centro de Estudos de Segurança e Cidadania (CESeC) concluiu que não houve redução de crimes na região do bairro durante o uso das câmeras em 2019, relevando, ainda, certa despreocupação "com a transparência das ações, com o bom uso do dinheiro público e com a proteção dos dados da população" (NUNES, 2022).

O projeto denominado "O Panóptico", realizado pela equipe do CESeC, tem por finalidade monitorar a adesão da tecnologia de reconhecimento facial na segurança pública do Brasil, revelando alguns dos vieses que acompanham o uso da referida tecnologia e disponibilizando os resultados ao público geral. O nome do projeto é similar a arquimetáfora utilizada por Michel Foucault (1987) para descrever a vigilância constante. O Panóptico de Jeremy Bentham era uma torre localizada no centro de prisões em que os presos eram observados por alguém que se encontrava na torre, mas os presos não faziam ideia de quem os estava observando e se realmente estavam sendo observados.

É possível aplicar a intenção do Panóptico como uma analogia à vigilância atual ocasionada pela tecnologia. O mercado é como se fosse o vigilante e os presos seriam a população. A vigilância perpétua é necessária para a aplicação da disciplina, assim como o registro contínuo de cada indivíduo, de modo que essas informações sejam enviadas obedecendo a uma hierarquia.

Em uma escala global, a editora online Visual Capitalism (2020), focada em tópicos relacionados a mercados, tecnologia, energia e economia global, elaborou um mapa ilustrando quais países ao redor do mundo já fazem o uso da tecnologia de reconhecimento facial, quais aprovaram a utilização e ainda não a implementaram, quais não consideraram a tecnologia e quais baniram seu uso.

Em 2021, o órgão de vigilância da privacidade da União Europeia, Autoridade Europeia de Proteção de Dados (AEPD), proibiu o uso de reconhecimento facial na Europa, em razão de sua "intrusão profunda e não democrática" na vida privada das pessoas, sustentando a proibição no fundamento de que existe alto risco da implementação da tecnologia de reconhecimento facial aos direitos fundamentais (EDPB, 2021):

> Tendo em conta os riscos extremamente elevados colocados pela identificação biométrica à distância de pessoas em espaços acessíveis ao público, o CEPD e a AEPD apelam à proibição geral da utilização da IA para o reconhecimento automático de características humanas em espaços acessíveis ao público, tais como o reconhecimento de rostos, da maneira de andar, de impressões digitais, ADN, voz, digitação e outros sinais biométricos ou comportamentais, em qualquer contexto. Do mesmo modo, o CEPD e a AEPD recomendam a proibição de sistemas de IA que utilizem dados biométricos para classificar as pessoas em grupos com base na etnia, no género, na orientação política ou sexual ou outras razões pelas quais a discriminação seja proibida nos termos do artigo 21.º da Carta dos Direitos Fundamentais.

A China, por outro lado, carrega com mais leviandade a cultura da vigilância e expandiu o uso do reconhecimento facial na pandemia: nas casas, para vigiar se as pessoas cumprem a quarentena; ou nas ruas, para ver se estão com febre ou usando máscaras. No mesmo viés, a projeção da idade dos habitantes na China também está bastante avançada para o reconhecimento de desaparecidos quando crianças. Por meio de uma imagem antiga, é possível gerar uma suposição de como ela seria mais nova ou mais velha.

Sem segurança, não há confiança. No entanto, quando falta liberdade, a segurança pode ser comparada com uma prisão ou escravidão pior ainda quando perdura por muito tempo, inexistindo outra opção aos agentes senão se conformar com a privação e vigilância constante em nome de um bem “aparentemente” maior, ou seja, a segurança (BAUMAN, 2009, p. 51). Quer-se dizer que os habitantes foram reduzidos a objetos de testes, no sentido de que para viverem em uma sociedade supostamente segura, devem estar constantemente vigiados e, sob a vigilância, se comportarão conforme o esperado por quem detém o poder.

Se, por um lado, a implementação da tecnologia de reconhecimento facial é vista com bons olhos para um país, por outro, é reputada como viela para ofensa a direitos da personalidade. Algoritmos e tecnologia, embora tenham autonomia em alguns aspectos, não podem ser considerados entes completamente autônomos quando se trata de identificar essencialidades da pessoa humana. Para manter a higidez dos direitos da personalidade, a supervisão humana se torna peça crucial, fazendo com que eventuais falhas, envolvendo tais direitos durante o funcionamento de determinada tecnologia que inclui algoritmos, sejam cada vez mais raras.

4 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E RECONHECIMENTO FACIAL COMO DADO BIOMÉTRICO

A imagem facial também se tornou um dado biométrico capaz de diferenciar as pessoas umas das outras por traços específicos. Com a frequente utilização de câmeras de vídeo para segurança pública e privada, inclusive com reconhecimento facial, surgem questões sobre a necessidade de adequação na coleta das imagens e demais dados capturados, mantidos sob o poder de banco de informações.

As características afetivas e os traços de personalidade são anatomicamente definidos. Os dados biométricos são únicos e inerentes a cada indivíduo particular e, por essa razão, devem ser protegidos. Segundo denota Anderson Schreiber (2014, p. 139) “Toda pessoa tem direito a controlar a representação de si mesma que é construída a partir de seus dados pessoais. É direito de toda pessoa exigir que tal representação reflita a realidade, impedindo que seu uso assuma caráter discriminatório”.

Direitos da personalidade são aqueles reconhecidos à pessoa humana tomada em si mesma e em suas projeções sociais, previstos no ordenamento jurídico para a defesa de valores inatos ao homem, com a vida, a intimidade e a honra (BITTAR, 1995). Portanto, considera-se que os dados biométricos estão diretamente ligados à personalidade da pessoa humana e, por consectário, merecem maior proteção.

No tocante aos dados pessoais coletados pela ferramenta, vale ponderar a aplicação da Lei Geral de Proteção de Dados Pessoais, em vigor desde 2020 (BRASIL, 2018). É facultado ao titular dos dados solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os

aspectos de sua personalidade (art. 20). Ainda, caso não sejam oferecidas as informações, é permitido que a autoridade nacional realize auditoria para verificação de aspectos discriminatórios no tratamento automatizado de dados pessoais.

Muito embora a Lei Geral de Proteção de Dados Pessoais considere o dado biométrico como dado sensível (art. 5º, II), o inciso III, alínea "a" do artigo 4.º da referida Lei preceitua que esta não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, pois o tratamento de dados pessoais, nesse caso, será regido por lei 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.

No Brasil, inexiste, ao menos por ora, regulamento específico sobre o uso da tecnologia de reconhecimento facial para segurança pública. O mais próximo de regulação sobre o tema e que se tem conhecimento é das três proposições legislativas ainda em trâmite que versam sobre a Inteligência Artificial: o PL 5.051/2019, que define princípios para uso da Inteligência Artificial no Brasil; o PL 872/2021, que disciplina o uso desse tipo de recurso no país; e o PL 21/2020, que regulamenta o uso da Inteligência Artificial no âmbito nacional.

Considerando, portanto, a ausência de regulamento específico acerca do uso da tecnologia de reconhecimento facial na segurança pública e até mesmo em outros âmbitos, talvez seja válido considerar a implementação da tecnologia de reconhecimento facial sem regulamento específico positivado no ordenamento jurídico, o que seria uma atitude imprudente.

Dentre os deveres do Estado, identifica-se a função de promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV da CF). Melhor ênfase deve ser dada à assertiva de que o bem de todos deve ocorrer sem nenhuma forma de discriminação. Certo é que a tecnologia de reconhecimento facial ainda é imatura e, por esta razão, não deveria ser aplicada em território nacional, ainda que em fase de testes.

Ninguém deixa sua privacidade em casa quando sai à rua e estar em um local público não quer dizer que tudo o que ocorre nesse espaço aberto possa ser utilizado para qualquer fim que não seja previamente autorizado. Vale indagar até que ponto a segurança pública deve se sobrepor à proteção dos direitos da personalidade, como direito à imagem, direito à privacidade e direito à proteção de dados pessoais, especialmente quando se trata de dados pessoais sensíveis como a biometria facial.

No entanto, a supressão de informações referentes a dados sensíveis nos mecanismos de reconhecimento facial, de certa forma, não resolveria o problema de enviesamento. Na verdade, isso apenas dificultaria a identificação dos fenômenos discriminatórios e sua correção. Num olhar geral, identificam-se mais pontos negativos do que positivos em relação ao reconhecimento facial, sobretudo por se tratar de tecnologia invasiva que pode causar sérias violações a direitos fundamentais.

A privacidade, segundo Stefano Rodotá (2008) pode ser interpretada como o controle sobre os próprios dados, não se limitando à vaga definição de vida privada como o direito a estar sozinho. Assim, se esses dados e informações são explorados sem o devido consentimento do titular, podem violar a sua privacidade.

Torna-se nítido que, em relação aos mecanismos de controle ético, a amplitude de possibilidades de uso da IA cria novos nichos de mercado altamente rentáveis, como é o caso da segurança pública. No entanto, ainda não há como garantir o emprego de forma ética e responsável, por parte dos governos nem das empresas (ESTEVES NUNES CRIPPA, 2021, p. 167).

Não se discute o fato de que se o Brasil investir na tecnologia de reconhecimento facial, certamente, incorrerá em danos incalculáveis no que toca à violação de direitos da personalidade como a dignidade humana. Por outro lado, não investir significa abrir mão de ferramentas que poderiam, de certa forma, aprimorar questões pontuais da segurança pública. É bastante válido considerar que a realidade tecnológica é assustadora e pensar em algumas de suas consequências desarticula qualquer ser racional. Mas rememorando os primórdios do surgimento de aparelhos tecnológicos,

Se a norma jurídica que melhor abrange os direitos sobre o tratamento de dados pessoais não é aplicável à segurança pública, surge um impasse quanto à proteção dos direitos da personalidade. É como se o Estado se eximisse de proteger um direito para sobrepor a proteção de outro, o que leva a ponderar qual o critério adotado para medir a relevância de tais direitos. Em outras palavras, o uso da IA para fazer o reconhecimento facial pode ser útil à proteção dos direitos da personalidade, mas também pode acarretar violações a tais direitos. Tudo dependerá do uso que se fizer dessa moderna tecnologia.

5 CONCLUSÃO

A realidade é que o mundo e as pessoas nunca foram tão digitais quanto agora e a automatização dos afazeres mais simples do cotidiano torna o resultado muito mais imediato e talvez, mais satisfatório. As tecnologias como a Inteligência Artificial (IA) e o reconhecimento facial têm o poder de copiar e otimizar atitudes humanas de formas impressionantes.

Ainda que exista semelhanças entre a mente humana e a IA, não podem ser consideradas iguais, pois o cérebro humano tem a capacidade cognitiva de identificar peculiaridades externadas por outros seres humanos, como emoções e outros detalhes, enquanto que a IA tende a replicar comandos alimentados por algoritmos que nem sempre obtém sucesso, por ignorar particularidades relevantes, como a cor da pele humana.

Na verdade, o êxito da tecnologia de reconhecimento facial depende da qualidade do banco de dados utilizado para comparação, bem como dos algoritmos que alimentam sua IA. Se o banco de dados é alimentado com elementos insuficientes ou imprecisos, certamente os resultados não serão satisfatórios e muito provavelmente terão efeitos desastrosos, como a discriminação.

Não se ignora o avanço tecnológico dos últimos anos e os aspectos positivos que essa evolução trouxe para a sociedade. Atos que antes eram realizados apenas por mãos humanas e possuíam certa complexidade, hoje podem ser realizados quase integralmente ou com o auxílio de IA. Diversas mudanças extraordinárias são visíveis nesses pequenos atos do cotidiano, mas são ainda mais visíveis quando envolvem a sociedade como um todo.

Nesse sentido, o uso da tecnologia de reconhecimento facial para garantir direitos fundamentais como a segurança pública e o exercício pleno da cidadania, trouxe relevantes efeitos positivos e negativos. Dentre os pontos positivos, foi possível observar a agilidade para a adoção de algumas medidas relacionadas à segurança, como identificar um indivíduo procurado pela polícia ou encontrar pessoas desaparecidas como é feito na China.

Ao mesmo passo que o avanço carrega pontos positivos, há aspectos negativos que acabam por violar mais de um direito fundamental, provindo a necessidade de proteção de ambos ou ponderar qual deles deve se sobrepor. Para que a tecnologia funcione efetivamente e proteja direitos da personalidade, é necessário manter operante e muito bem alimentado um vasto banco de dados, com informações relativas à personalidade individual de cada um.

O reconhecimento facial é considerado um dado biométrico, ou seja, um dado pessoal sensível. No entanto, quando se fala em utilização desse dado para fins de segurança pública e considerando a não aplicabilidade da Lei Geral de Proteção de Dados Pessoais, sua proteção fica à mercê de regulamentação específica, o que não existe até o momento, ao

menos em território nacional. Nesse aspecto, se está diante de um impasse quanto a dois direitos fundamentais: a proteção de dados pessoais e a segurança pública.

Decidir qual deles deve prevalecer é uma tarefa complexa, o que leva a acreditar que existem mais pontos negativos do que positivos em relação ao uso de ferramentas de reconhecimento facial no âmbito da segurança pública, sobretudo por se tratar de tecnologia invasiva que pode causar sérias violações a direitos da personalidade.

Assim, acredita-se que a implementação de uma ferramenta com tantos vieses como a tecnologia de reconhecimento facial não seja a medida mais eficaz para o bem-estar da sociedade, uma vez que corrobora com a garantia da segurança pública enquanto função do Estado, mas viola outros (diversos) direitos da personalidade.

REFERÊNCIAS

BAUMAN, Z. **Vida Líquida**. Tradução Carlos Alberto Medeiros, 2ª ed. Rio de Janeiro: Zahar, 2009, p. 51.

BITTAR, C. A. **Os direitos da personalidade**. 2ª ed. Rio de Janeiro: Forense Universitária, 1995.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 out. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 15 out. 2022.

BUOLAMWINI, J. et al. **Facial Recognition Technologies**: A Primer. Algorithmic Justice League, 2020. Disponível em: https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf. Acesso em: 14 out. 2022.

CODED BIAS. Direção: Shalini Kantayya. Produção: Shalini Kantayya. **Documentário**, Netflix, 2020, 1h 25min.

COSTA, R. S.; OLIVEIRA, S. R. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. **Revista de Direito, Governança e Novas Tecnologias**. Belém. v. 5, n. 21, p. 01-21, jul/dez. 2019. DOI: http://dx.doi.org/10.26668/IndexLawJournals/2526-0049/2019.v5i2.5777. Acesso em 23 out. 2022.

EDPB. **O CEPD e a AEPD apelam à proibição da utilização da inteligência artificial (IA) para o reconhecimento automático de características humanas em espaços acessíveis ao público e de outras utilizações da IA que possam conduzir a uma discriminação injusta**.

2021. Disponível em: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_pt. Acesso em: 14 out. 2022.

ESTEVES NUNES CRIPPA, M. et al. Uso de reconocimiento facial aplicado a la seguridad pública en Brasil. **Controversias Y Concurrencias Latinoamericanas**, v. 12, n. 22, pp. 159-173, abr/set 2021. Disponível em: http://ojs.sociologia-alas.org/index.php/CyC/article/view/248. Acesso em 15 out. 2022.

FERRAZ VIDAL, I. **Poéticas e políticas do rosto na era das imagens inteligentes**. Significação, São Paulo, v. 46, n. 51, p. 209-228, jan-jun. 2019. Disponível em: https://www.redalyc.org/articulo.oa?id=609765275011. Acesso em 14 out. 2022.

FOUCAULT, M. **Vigiar e punir**: nascimento da prisão. Tradução: Raquel R. Petrópolis: Vozes, 1987.

INSTITUTO IGARAPÉ. **Reconhecimento facial no Brasil**. Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil. 2019. Site Instituto Igarapé, [s.l.], [entre 2019 e 2021]. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 14 out. 2022.

MCCARTHY, J., *et al.* A proposal for the dartmouth summer research project on artificial intelligence, August 31, 1955. **AI Magazine**, v. 27, n. 4, p. 12, 2006. Disponível em: https://doi.org/10.1609/aimag.v27i4.1904. Acesso em: 14 out. 2022.

NUNES, P. *et al*. **Um Rio de olhos seletivos: uso de reconhecimento facial pela polícia fluminense**. Rio de Janeiro: CESeC, 2022. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 23 out. 2022.

ORVALHO, V. Reconhecimento facial, **Revista de Ciência Elementar**, v. 7, n. 4, 2019. DOI: http://doi.org/10.24927/rce2019.073. Acesso em 20 out. 2022.

PINTO, B. M. C., *et al*. **Diferenças de gênero entre universitários no reconhecimento de expressões faciais emocionais**. Avances en Psicología Latinoamericana, 31, 2013, pp. 200-222.

PITOMBO, J. P. Vestido de mulher, homem é preso no Carnaval após reconhecimento facial na Bahia. **Folha de São Paulo**. São Paulo: Grupo Folha, 2019. Diário. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/03/vestido-de-mulher-homem-e-preso-no-carnaval-apos-reconhecimento-facial-na-bahia.shtml. Acesso em 18 out. 2022.

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

SCHREIBER, A. **Direitos da personalidade**. São Paulo: Atlas, 2014, pp. 139 e 163.

VALENTINI, R. S. **Julgamento por computadores?** As novas possibilidades da juscibernética no século XXI e suas implicações para o futuro do direito e do trabalho dos juristas. 2017.152 f. Tese (Doutorado em Direito do Trabalho) - Faculdade de Direito,

Universidade Federal de Minas Gerais, Belo Horizonte, 2017. Disponível em: http://hdl.handle.net/1843/BUOS-B5DPSA. Acesso em: 20 ago. 2022.

VISUAL CAPITALISM. **Smile, you're on câmera**. The facial recognition world map. 2020. Disponível em: https://www.visualcapitalist.com/wp-content/uploads/2020/05/Facial-Recognition-World-Map-Full-Size.html. Acesso em: 23 out. 2022.

ZIMMERMANN, A. C. **Reconhecimento de faces humanas através de técnicas de inteligência artificial aplicadas a formas 3D**. Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Engenharia Elétrica, 2003. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/85115. Acesso em: 14 out. 2022.