Sorria, você está sendo julgado

Brenda Cunha, André Boselli - Programa de Direitos Digitais e Acesso à Informação, Artigo 19

Data da publicação:

Janeiro 2024

Sistemas de reconhecimento de emoções e suas implicações em direitos humanos

Tecnologias de reconhecimento de emoções são sistemas eletrônicos e informáticos que pretensamente inferem o estado afetivo interno de uma pessoa. Para tanto, por meio do chamado *machine learning* (aprendizado de máquina), elas registram características pessoais – como expressões e microexpressões faciais, tom vocal, movimentos corporais e outros sinais biométricos e fisiológicos –, que são então classificadas em categorias como raiva, medo, surpresa, felicidade etc. Assim como outras tecnologias biométricas (como o reconhecimento facial), seu uso implica na coleta massiva de dados pessoais sensíveis; a inteligência artificial julga uma pessoa a partir da comparação entre os sinais capturados e um babilônico banco de dados. Isso é feito quase sempre de maneira imperceptível, sem o conhecimento ou consentimento do réu. Tampouco existe a possibilidade de controle externo sobre essa tecnologia e seu funcionamento é pouquíssimo transparente.

Mas o que nossas expressões corporais podem dizer sobre nós? A depender do *marketing* dos desenvolvedores de tecnologias de reconhecimento de emoções – e de Estados e empresas que compram esses dispositivos (e discursos) –, a resposta poderia ser muita coisa ou vários âmbitos da vida que os adquirentes desses sistemas queiram [tentar] controlar ou outras tantas situações que pretendam prever, normalmente gerando decisões opacas, unilaterais e irrecorríveis, tomadas por um algoritmo, sobre algum aspecto de nossas vidas.

Por exemplo, a aplicação real desses sistemas vai do comportamento e nível de atenção de estudantes na sala de aula à sinceridade de uma pessoa interrogada por policiais ou por agentes de imigração; da probabilidade de motoristas evadirem pedágios ou dormirem ao volante à confiabilidade de clientes que tentam contrair empréstimos bancários; do humor de consumidores em relação a produtos e conteúdos publicitários à detecção, em entrevistas de emprego, de futuros maus funcionários.

Consideradas acriticamente por muitos como a sequência natural e lógica dos sistemas de reconhecimento facial, os tentáculos das tecnologias de reconhecimento de emoções têm sorrateiramente se espraiado em vários lugares do mundo, como China, Índia, Europa, Estados Unidos e Brasil, com pouco ou nenhuma regulamentação ou discussões sobre seus riscos e impactos sobre os direitos humanos.

Se a identificação de pessoas por meio de câmeras e algoritmos já era algo bastante problemático, as tecnologias de reconhecimento de emoções levam os questionamentos e preocupações a outro patamar, pois a pergunta que norteia sua arquitetura tecnológica não é simplesmente quem é essa pessoa, mas também que tipo de pessoa é essa, o que ela diz com sua expressão ou o que ela está pensando, sentindo ou pretendendo fazer.

Esses sistemas pretensamente inferem os estados internos das pessoas avaliadas porque, na verdade, os julgamentos feitos por máquinas e algoritmos não passam de mera quimera tecnocrática: as premissas sobre as quais se funda sua arquitetura tecnológica foram geradas por uma teoria científica defasada, hoje considerada uma pseudociência. Trata-se da teoria da universalidade das emoções, derivada de um trabalho dos anos 1960 conduzido pelo psicólogo estadunidense Paul Ekman. Segundo essa teoria, existe uma relação direta e confiável entre as feições ou aparências externas de uma pessoa e seu estado emocional interior; esse estado interno pode

ser compreendido por meio de emoções básicas claramente identificáveis e exteriorizadas pelo corpo; e tais emoções são expressas de maneira uniforme por todos os seres humanos, independentemente de culturas ou construções sociais. No entanto, desde a primeira publicação sobre o assunto, cientistas têm investigado, contestado e amplamente rejeitado essas afirmações. O próprio Ekman chegou a questionar a aplicação dessa teoria por sistemas algorítmicos.1

Como se não bastassem esses graves vícios na própria concepção das tecnologias de reconhecimento de emoções, seu uso implica uma série de violações a direitos humanos. Em relação à liberdade de expressão, por exemplo, esses sistemas geram efeitos inibidores sobre as pessoas, que, sabendo ou imaginando que estão tendo suas expressões julgadas, passam a se autocensurar. Uma autocensura que envolve inclusive o sentido mais direto dessa liberdade: aquela relacionada não apenas à linguagem, mas também à expressão corporal e a outras características que compõem as individualidades. Privacidade e o direito de protestar e de se reunir também são atingidos em cheio, incluindo potenciais impactos desproporcionais e discriminatórios, principalmente se as tecnologias de reconhecimento de emoções forem usadas para fins de segurança pública no contexto de manifestações.

Além disso, o direito de não produzir provas contra si mesmo, ou de não se autoincriminar, também fenece quando essas tecnologias são implementadas, já que informações são extraídas forçosamente de pessoas interrogadas ou supervisionadas por autoridades ou sistemas de segurança. Tal situação se torna ainda mais grave se for considerado o caráter pseudocientífico desses sistemas e a possibilidade de serem usados de modo a discriminar grupos e pessoas historicamente vulnerabilizados.

Aliás, essas confissões forçadas ressaltam ainda outra característica dessas tecnologias: a existência de uma abissal assimetria de poder, pois a pessoa julgada não sabe o que exatamente está sendo avaliado e, pior, nada pode fazer contra a conclusão a que chegar a inteligência artificial – o que vale não apenas para contextos de aplicação da lei, mas para qualquer circunstância na qual esses sistemas sejam aplicados.

Também é importante ressaltar que pesquisas têm cada vez mais demonstrado que esses sistemas têm desempenho deficiente quando aplicados a rostos de mulheres negras, minorias étnicas, pessoas trans e crianças.2

É difícil afirmar com precisão a magnitude de inserção das tecnologias de reconhecimento de emoções pelo mundo. Um relatório sobre o mercado chinês feito pela Artigo 19 e publicado em 2021 indicou que em ao menos três setores esses sistemas estavam sendo testados e implementados no país asiático: segurança pública – para detectar previamente situações de perigo, fazer monitoramento após identificação de uma potencial ameaça e auxiliar em interrogatórios –, segurança de trânsito e educação.3 O trabalho se concentrou na China porque se trata de um grande mercado, em tese, com bastante demanda e motivação política para essas tecnologias, além de contar com mão de obra tecnicamente qualificada e investimentos abundantes. É possível que, desde então, o mercado chinês tenha se expandido ainda mais e que as empresas chinesas de tecnologia já estejam vendendo para outros países.

Em um artigo de 2023, Vidushi Marda, uma das autoras do relatório sobre o mercado chinês, revela como as tecnologias de reconhecimento de emoções estão sendo aplicadas na Índia.4 Destaque para o uso por departamentos de recursos humanos de empresas – como o inventário de personalidade sombria, concebido para tentar identificar certos traços de personalidade – e também por órgãos de segurança pública.5

Na Europa, uma das aplicações mais conhecidas desses sistemas é o desenvolvimento do programa iBorderCtrl, uma tecnologia que supostamente detecta mentiras contadas a agentes que trabalham em fronteiras controlando a entrada de imigrantes. Recentemente, uma decisão do Tribunal de Justiça da União Europeia negou acesso integral aos documentos referentes à iniciativa, o que ratifica a afirmação sobre a opacidade dessas tecnologias.6

A União Europeia está prestes a aprovar sua Lei de Inteligência Artificial (*Artificial Intelligence Act*). A proposta original considerava essas tecnologias como de risco baixo ou mínimo, o que significava que a única exigência para sua implementação era a obrigação de informar às pessoas que elas estariam interagindo com uma máquina.7 Após pressão de ativistas e organizações da sociedade civil (incluindo a Artigo 19), no entanto, o Parlamento Europeu alterou o texto. A nova redação bane a aplicação de sistemas de reconhecimento de emoções para situações de *law enforcement* (aplicação da lei penal), controle de fronteiras, educação e locais de trabalho. A versão final da lei será resultado da negociação entre os órgãos que compõem a União Europeia, o que é esperado para os próximos meses.9

Contexto brasileiro de vigilância

No Brasil, ao longo de mais de uma década, uma diversidade de tecnologias de vigilância e coleta de dados da população tem sido progressivamente adotada em diversos setores de atividades e serviços, com destaque para sistemas automatizados de inteligência artificial. Entre eles, sistemas de reconhecimento de padrão, como sistemas biométricos de reconhecimento facial, leitores de placas, reconhecimento de objetos, entre outros. Destaca-se também a crescente incorporação, nos setores público[9] e privado, de ferramentas para mineração e cruzamento de dados obtidos a partir de fontes públicas, como redes sociais e páginas na Internet, popularmente conhecidas como *Open Source Intelligence* - OSINTs (ou, em português, Inteligência de Fontes Abertas).

Nos últimos anos, especialmente a partir do governo Bolsonaro (2019-2023), observou-se também um aumento de investimento para a compra de softwares de espionagem e *hacking* estatal. O fenômeno de incorporação dessas tecnologias tem ocorrido tanto na esfera nacional como subnacional, sendo o governo federal um grande financiador e estimulador da expansão dessas tecnologias nos estados, seja por meio de verbas como pela celebração de convênios.[10] No âmbito do legislativo, a destinação de emendas parlamentares também contribuiu para o aumento dessas aquisições.[11] É importante também ressaltar o papel da pandemia de covid-19 a partir de 2020, dada sua contribuição para a aceleração de processos de aquisição de tecnologias e infraestruturas digitais, utilizadas para auxiliar medidas de prevenção e distanciamento social[12].

A implementação de projetos de Smart Cities também vem impulsionando a incorporação dessas tecnologias de vigilância, comumente associadas à integração de grandes bases de dados de posse do Estado. A prefeitura do Rio de Janeiro, a partir do Consórcio Smart Luz lançado no ano de 2021 para renovação do parque de iluminação da cidade, também prevê a implantação de cerca de 4 mil câmeras com reconhecimento facial.[13] O projeto Smart Sampa, lançado em 2022 pela Prefeitura de São Paulo, prevê a instalação de 20 mil câmeras de reconhecimento facial e integração de bases de diversas secretarias até 2024.[14] Além das grandes capitais citadas, iniciativas semelhantes são encontradas em municípios médios e pequenos.[15] O uso de reconhecimento facial na área da educação desponta como outro campo em ascensão no país,[16] tendo recebido um novo impulso para a incorporação dessas ferramentas após a nova onda de ataques em escolas, ocorrida no primeiro semestre de 2023.[17]

Observa-se, porém, que esse aumento tem se verificado sem a presença de regulamentação direcionada para o desenvolvimento, aquisição, utilização e impactos associados à incorporação desses sistemas. Apenas em 2020, a agenda de regulamentação de sistemas de inteligência artificial começou a avançar no Congresso Nacional. Atualmente, o Projeto de Lei (PL) 2.338/2023[18] tem se apresentado como a proposta mais sólida em discussão. O texto teve origem a partir do esforço de uma comissão de juristas, instalada no Senado Federal, em 2022, com a finalidade de aprofundar e conduzir os debates, visando ao estabelecimento de parâmetros e salvaguardas para mitigação de riscos e proteção aos direitos fundamentais.[19] No entanto, o texto ainda apresenta áreas de discordância e conflitos entre vários setores, incluindo a sociedade civil - focada em questões de direitos humanos[20] -, empresas, governo[21], forças de segurança, entre outros.

Outra característica distintiva do panorama brasileiro relacionado aos sistemas de inteligência artificial (IA) é a recorrente falta de transparência, tanto por parte do poder público quanto por agentes privados. A falta de regulamentação específica para as IAs acentua o problema, que também é intensificado por práticas como o descumprimento sistemático da legislação de proteção de dados pessoais por parte de gestores públicos[xxii] e empresas. Além disso, negativas de acesso à informação são frequentemente fundamentadas na aplicação inadequada dos dispositivos de proteção de dados presentes na Lei de Acesso à Informação (LAI) e na Lei Geral de Proteção de Dados (LGPD),[23] ou amparadas em exceções previstas nessas legislações quando aplicadas a atividades relacionadas à segurança.

Como consequência, observa-se também que o controle social sobre as diferentes etapas de incorporação dessas tecnologias tem sido prejudicado e, em alguns casos, inviabilizado. Denúncias recentes fornecem evidências de uso abusivo de tais tecnologias. Em 2020, o "Dossiê antifacista" veio à tona, revelando um documento contendo uma lista de opositores ao governo Bolsonaro, confeccionada com o auxílio de tecnologias de coleta de dados em fontes abertas. Em outubro de 2023, foi deflagrada operação da Polícia Federal após denúncias de irregularidades envolvendo a First Mile, sistema capaz de monitorar até 10 mil pessoas por ano utilizando informações de seus celulares. Dois servidores da Agência Brasileira de Inteligência (Abin) foram presos e cinco afastados, acusados de utilizar o sistema para monitorar ilegalmente cidadãos brasileiros, incluindo jornalistas, advogados e até

ministros do Supremo Tribunal Federal[24].

Reconhecimento de emoções: realidade brasileira

Dada a diversificação e interoperabilidade entre os recursos e funcionalidades, têm sido cada vez mais comum o desenvolvimento e a utilização integrada entre as tecnologias de vigilância e coleta de dados. No Brasil, a popularização de sistemas de reconhecimento facial, por exemplo, contribui para a incorporação de outros *softwares* analíticos, abrindo as portas para a integração de sistemas baseados em reconhecimento de emoções.

Dados de um levantamento[25] publicado em outubro de 2023 apontou que, desde o ano anterior, mil e setecentas escolas do Paraná passaram a implantar sistemas de reconhecimento facial em suas unidades. O sistema, chamado Educatron, foi instalado em um totem, equipado com televisão, computador, teclado, mouse, microfone e webcam. Posicionado em sala de aula ao lado do professor, o equipamento foi instalado oficialmente para exibir conteúdos multimídia e realização de video chamadas. O sistema também tem como finalidade identificar os alunos presentes na sala, além de estar habilitado para reconhecer expressões faciais dos alunos, funcionalidade que seria utilizada para medir o comportamento dos estudantes. Os professores que experimentaram o sistema apontaram várias falhas e erros, levando-os em alguns casos a executar tarefas sem o auxílio da tecnologia, como a realização de chamadas[26].

No início deste ano, no período quando o sistema operava em uma escola cívico-militar do estado, na fase piloto, o experimento teve como finalidade a geração de gráficos de atenção e dispersão, visando medir a qualidade das aulas por meio das emoções demonstradas pelos estudantes. Segundo a Companhia de Tecnologia da Informação e Computação do Paraná (Celepar), os dados de emoções dos alunos devem ser armazenados para a realização de análises estatísticas futuras. A Celepar também confirmou a realização de testes para medir comportamentos que representassem riscos à integridade dos alunos e servidores, com o apoio do software SecurOS, da empresa israelense Intelligent Security Systems (ISS). Contudo, de acordo com a Companhia, os testes não foram eficazes por limitações de captação das câmeras. Em 2021, um edital foi lançado em parceria entre a Celepar e Hotmilk, uma aceleradora de startups ligada à PUC-PR, para a selecionar soluções que oferecem monitoramento comportamental de alunos, por meio de vídeo e voz, utilizando inteligência artificial para coleta, processamento e classificação de emoções.

A experiência evidenciada no Paraná demonstra um preocupante avanço desses sistemas por iniciativa do poder público, com o agravante de submetê-los a crianças e adolescentes, cujos dados pessoais, de acordo com a Lei Geral de Proteção de Dados, devem ser tratados com grau maior de proteção. Até então, os casos de utilização de sistemas de reconhecimento de emoções que ganharam repercussão datavam de 2018 e 2019, ambos implementados por empresas e com fins comerciais. Nas duas situações, constatou-se que a utilização desses sistemas envolveu violação de direitos.

O primeiro caso reportado foi o da ViaQuatro, empresa concessionária da linha amarela do metrô de São Paulo. Em 2018, a empresa instalou câmeras nas portas de acesso ao veículo equipadas com a tecnologia. O sistema, que operou durante seis meses, de abril a outubro daquele ano, tinha como um de seus objetivos expor os usuários a conteúdo publicitário, captando dados, como visualizações, tempo de permanência, tempo de atenção, gênero, faixa etária, fator de visão e hora de pico de visualizações dos anúncios, além de medir emoções como raiva, alegria e neutralidade. A ação foi considerada ilegal, porque não havia consentimento dos passageiros, que foram expostos à coleta e tratamento de dados sem qualquer aviso, prévio ou posterior[27]. O caso foi judicializado e a empresa foi obrigada a interromper a coleta e imagens e uso do sistema, além de processada e condenada ao pagamento de multa no valor de R$500 mil.[28]

Outro caso, de 2019, que levou à condenação por utilização indevida desses sistemas envolveu a empresa Hering, denunciada por instalar, sem aviso prévio aos clientes, câmeras equipadas com reconhecimento de emoções em uma de suas lojas conceito, na cidade de São Paulo. O sistema captava as reações do consumidor às peças dispostas no local, para fins de publicidade direcionada.[29] A Secretaria Nacional do Consumidor (Senacon) condenou a Hering ao pagamento de multa no valor de R$58,7 mil, constatando-se ter havido a violação de direitos do consumidor, como direitos de informação e de personalidade, pois as imagens haviam sido utilizadas para fins comerciais sem consentimento[30].

Os exemplos anteriores ilustram a entrada facilitada e sem restrições desses sistemas no mercado brasileiro, o qual ainda carece de uma regulamentação específica. Sua adoção ocorre sem supervisão, tanto quando utilizadas

pelo setor público quanto por empresas, deixando a população suscetível a abusos e violações de direitos. Eventos desse tipo já ocorreram e a repercussão e medidas legais apenas se concretizaram após denúncias de setores da sociedade civil engajados nos direitos digitais. Entretanto, existe a perspectiva de uma disseminação mais ampla dos sistemas de reconhecimento de emoções no país, operando à margem da legalidade e apresentando ameaças aos direitos fundamentais.

Reconhecimento de emoções no debate regulatório de inteligência artificial (IA) no Brasil

Encontra-se em tramitação no Senado Federal o PL 2.338/2023 (Marco Geral da Inteligência Artificial), que dispõe sobre o uso de sistemas de IA no país. A proposta pretende estabelecer normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de IA no Brasil.

O texto aborda expressamente sistemas de reconhecimento de emoções ao tratar dos direitos associados à informação e compreensão das decisões tomadas por sistemas de inteligência artificial.31 Os legisladores propõem que pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição (Art. 7º, § 2º). A partir das definições descritas no texto como atividades classificadas de alto risco, sistemas de reconhecimento de emoções podem ser considerados nesta categoria. Considerando as possibilidades de aplicação prática desses sistemas, é possível identificá-las em atividades como a avaliação, por autoridades competentes, da possibilidade de alguém cometer infrações penais e, também na esfera criminal, a elaboração de estudos para identificar padrões de comportamento (Art. 17, incisos XI-XIII).

A proposta em discussão no Congresso tem ainda um longo caminho a ser percorrido para se tornar lei e inúmeros desafios pela frente, tanto a superação dos atuais impasses presentes no texto, decorrentes de disputas e barreiras de natureza política, como o desenvolvimento de soluções técnicas verdadeiramente voltadas para sistemas de inteligência artificial seguros, para o interesse público, inovadores e capazes responderem às complexidades que os envolvem. Até lá, é necessário que as autoridades brasileiras adotem um maior controle e fiscalização sobre o uso desses sistemas, especialmente quando utilizados pelo poder público no desenvolvimento de políticas públicas, garantindo que as outras normativas em vigor no país sejam cumpridas, como as legislações de proteção de dados pessoais, o Estatuto da Criança e do Adolescente, entre outras.

Recomendações

Tecnologias de reconhecimento de emoções, seja por violarem direitos humanos, seja por se basearem em pseudociência, ratificando e maximizando essas violações, pedem tratamento mais rigoroso que sua classificação como de alto risco. Em outras palavras, não se trata de estimar seu grau de risco e qual a disposição social para aceitá-lo, mas sim, proibir seu uso.

A Artigo 19 recomenda à comunidade internacional banir os projetos, concepção, desenvolvimento, implantação e venda (importação e exportação) de tecnologias de reconhecimento de emoções, com base na sua inconsistência fundamental com os padrões internacionais de direitos humanos. Da mesma forma, nós recomendamos a interrupção, por parte de empresas privadas, da concepção, desenvolvimento e implantação de tecnologias de reconhecimento de emoções, uma vez que possuem um enorme potencial para afetar negativamente a vida e a convivência das pessoas. Além disso, é necessário que haja divulgação aos indivíduos afetados por essas tecnologias e a garantia que mecanismos de reclamação e denúncia eficazes, acessíveis e equitativos estejam disponíveis por eventuais violações de seus direitos como resultado do reconhecimento emocional.

1 MURGIA, Madhumita. Emotion recognition: can AI detect human feelings from a face? **Financial Times**, 2021. Disponível em: https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. Acesso em: 10 de nov 2023.

2 Emotion Recognition Technology Report. **ARTICLE 19**, 2021. Disponível em: https://www.article19.org/emotion-recognition-technology-report/. Acesso em: 10 de nov de 2023.

3 ARTICLE 19. **Emotional Entanglement: China's emotion recognition market and its implications for human rights.** ARTICLE 19: Londres, 2021. Disponível em: https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Repor... . Acesso em: 10 de nov de 2023.

4 MARDA, Vidushi. Not Just Privacy: The Dangers of Emotion Recognition Technology. **India in Transition (InT)/CASI**, 2023. Disponível em: https://casi.sas.upenn.edu/iit/vidushimarda. Acesso em: 10 de nov de 2023.

5 KATHPALIA, Bhuvi. Dark Core Personality Tests: Assessing Dark Traits for a Productive Safe Workplace. **METTL**, 2021. Disponível em: https://blog.mettl.com/dark-core-personality-test/. Acesso em: 10 de nov de 2023.

6 ARTICLE 19. EU: Court denies full transparency about emotion recognition. **ARTICLE 19**, 2023. Disponível em: https://www.article19.org/resources/eu-court-denies-full-transparency-ab... . Acesso em: 10 de nov de 2023.

7 Marda, Vidushi; Jakubowska, Ella. Emotion (Mis)Recognition: is the EU missing the point? **ARTICLE 19**, 2023. Disponível em: https://www.article19.org/resources/eu-emotion-misrecognition/. Acesso em: 10 de nov de 2023.

8 LEUFER, Daniel. Historic vote in the European Parliament: dangerous AI surveillance banned, but not for migrant people at the borders. **Access Now**, 2023. Disponível em: https://www.accessnow.org/press-release/historic-vote-in-the-european-pa... . Acesso em: 10 de nov de 2023.

8 BOSELLI, André; GAGLIARDI, Marília Papaléo. **As práticas de Inteligência de Fontes Abertas (OSINT) são amigas ou inimigas dos direitos humanos?**. 1ª ed. São Paulo: Artigo 19, 2023. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2023/09/DIGITAL_OSINT... . Acesso em: 10 de nov de 2023.

10 Amaral, Pedro et al. **Mercadores da insegurança: conjuntura e riscos do hacking governamental no Brasil**. 1. ed. Recife: IP.rec, 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 10 de nov de 2023.

11 REBELO, Aiuri. O Mecenas. **Intercept Brasil**, 2023. Disponível em: https://www.intercept.com.br/2023/04/05/delegado-waldir-torrou-r-30-milh... . Acesso em: 10 de nov de 2023.

12 CUNHA, Brenda et al. O legado da Covid no Brasil: influência do setor privado nos serviços públicos. **Jota**, 2022. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-... . Acesso em: 10 de nov de 2023.

13 Presidente da Rioluz participa de audiência sobre modernização da iluminação do Rio. **Câmara Municipal do Rio de Janeiro**, 2021. Disponível em: http://www.camara.rio/comunicacao/noticias/230-presidente-da-rioluz-part... . Acesso em: 10 de nov de 2023.

14 SCHENDES, William. Smart Sampa: entenda a polêmica do edital de monitoramento facial em São Paulo. **Olhar Digital**, 2022. Disponível em: https://olhardigital.com.br/2022/11/30/pro/smart-sampa-entenda-a-polemic... . Acesso em: dia, 10 de nov de 2023.

15 REIA, J.; CRUZ, L. **Cidades inteligentes no Brasil: conexões entre poder corporativo, direitos e engajamento cívico.** Caderno das Metrópoles, São Paulo, v. 25, n. 57, pp. 467-490, maio/ago 2023. Disponível em: https://doi.org/10.1590/2236-9996.2023-5705. Acesso em: dia, 10 de nov de 2023.

16 TAVARES, C. et al. **Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras**. São Paulo: InternetLab, 2023. Disponível em: https://Internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-P.... Acesso em: 10 de nov de 2023.

17 PITOMBO, João P. Deputados querem 'big brother' nas escolas com câmeras, detectores e reconhecimento facial. **Folha de São Paulo**, 2023. Disponível em: https://www1.folha.uol.com.br/cotidiano/2023/04/deputados-querem-big-bro.... Acesso em: dia, 10 de nov de 2023.

18 A versão do Projeto de Lei (PL) 2338/2023 consultada para este artigoestá disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1698248.... Acesso em: 10 de nov de 2023.

19 Para maiores informações sobre a instalação da comissão de juristas, acesse: https://www.youtube.com/watch?v=nXnliBi3vKY.

20 AZEVEDO, Cynthia, P. G. et al. Nota Técnica Projeto de Lei Nº 2338/2023. **Coalizão Direitos na Rede**, **LAPIN**, 2023. Disponível em: https://lapin.org.br/wp-content/uploads/2023/08/Nota-tecnica-PL-que-regu.... Acesso em: 10 de nov de 2023.

21 BRASIL. ANPD. **Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-pre.... Acesso em: 10 de nov de 2023.

22 CUNHA, Brenda et al. **Dados Virais: Legado da COVID-19 nas aquisições de tecnologias pelo Poder Público.** Associação Data Privacy Brasil de Pesquisa: São Paulo, 2021. Disponível em: https://drive.google.com/file/d/1-PmjyYubF65W_8LuOiYR2pwFQiRWEyZ3/view. Acesso em: 10 de nov de 2023.

23 CUNHA, Brenda; ROCHA, Júlia. **Análise das negativas de acesso a informações públicas fundamentadas nas disposições referentes à proteção de dados pessoais constantes na Lei Geral de Proteção de Dados (LGPD) e na Lei de Acesso à Informação (LAI)**. Artigo 19: São Paulo, 2023. Disponível em: https://artigo19.org/wp-content/blogs.dir/24/files/2023/08/NOTA-TECNICA_.... Acesso em: 10 de nov de 2023.

24 DIAS, Tatiana; MOTORYN, Paulo .Como o Brasil virou o paraíso da espionagem ilegal. **Intercept Brasil**, 2023. Disponível em: https://www.intercept.com.br/2023/10/28/brasil-virou-paraiso-da-espionag.... Acesso em: Acesso em: 10 de nov de 2023.

25 AUDI, Amanda. Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas. **Pública**, 2023. Disponível em: https://apublica.org/2023/10/reconhecimento-facial-no-parana-impoe-monit.... Acesso em: 10 de nov de 2023.

26 ISRAEL, Carolina B. et al. **Reconhecimento facial nas escolas públicas do Paraná**. JararacaLab, Lavits, UFPR, Rede de Pesquisa em Governança da Internet, Observatório das Metrópoles: Curitiba, 2023. Disponível em: https://jararacalab.org/cms/wp-content/uploads/2023/10/Relatorio_RF_2023.... Acesso em: 10 de nov de 2023.

27 SOPRANA, Paula; AMÂNCIO, Thiago. ViaQuatro é condenada por reconhecimento facial sem autorização no Metrô de SP, 2021. **Folha de São Paulo**, 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/05/viaquatro-e-condenada-po.... Acesso em: 10 de nov de 2023.

28 MEDEIROS, Henrique. TJ-SP aumenta multa para ViaQuatro para R$ 500 mil por uso de reconhecimento facial indevido. **Mobile Time**, 2023. Disponível em: https://www.mobiletime.com.br/noticias/11/05/2023/tj-sp-aumenta-multa-pa.... Acesso em: 10 de nov de 2023.

29 Idec notifica Hering por coleta de dados faciais para publicidade. **IDEC**, 2019. Disponível em: https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-fac.... Acesso em: 10 de nov de 2023.

30 Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial. **IDEC**, 2020. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por.... Acesso em: 10 de nov de 2023.

31 Seção II (PL 2.338/2023). Para maiores informações, conferir nota 18.

Categoria:

- poliTICs 37