I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

Copyright © 2020 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

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto

Aires Jose Rover

Fabiano Hartmann Peixoto – Florianópolis: CONPEDI, 2020.

Inclui bibliografia

ISBN: 978-65-5648-086-2

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34

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

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O I ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 23 e 30 de junho de 2020, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação. Foi o maior sucesso nesses tempos de pandemia. Mais do que nunca se viu a tecnologia servindo como instrumento de ação no campo do conhecimento e da aprendizagem, o que este GT sempre defendeu e esteve atento discutindo os limites e vantagens dessa utilização. Os artigos apresentados, como não podia deixar de ser, mostraram que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas, em sua sequência de apresentação no sumário e apresentação no GT. No primeiro bloco temático temos:

• marco civil da internet no brasil

• proteção de dados pessoais do trabalhador

• governança de dados aplicada a big data analytics

• consentimento do titular dos dados

• princípios da lei geral de proteção de dados

• blockchain e LGPD

No segundo bloco:

• inteligência artificial, bots e sexismo

• inteligência artificial para melhoria do judiciário

• danos causados por veículos autônomos

• implicações éticas

• direitos da personalidade

• reconhecimento facial

No terceiro bloco:

• Peter Häberlee a democracia digital

• constitucionalismo digital

• inclusão digital e inclusão social

• democracia participativa

No quarto e último bloco:

• deepweb e a (in)segurança dos cidadãos

• criptoativos e soberania tradicional

• fakenews e direito à saúde

• intimações judiciais na internet

• aplicativo uber

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para a leitura na integra dos artigos.

Aires José Rover –UFSC

Fabiano Hartmann Peixoto - Universidade de Brasília

Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota técnica: O artigo intitulado “Marco civil da internet no Brasil: conquistas e desafios” foi indicado pelo PPGD/UNIVEM, nos termos do item 5.1 do edital do Evento.

Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias II apresentados no I Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 8.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

AS DIFICULDADES PRESENTES NA REGULAÇÃO DO RECONHECIMENTO FACIAL

THE DIFFICULTIES PRESENT IN THE REGULATION OF FACIAL RECOGNITION

Victor Costa Rodrigues

Resumo

Dentre as novas tecnologias utilizadas na atualidade, o reconhecimento facial certamente é uma das mais emblemáticas. Ao longo deste artigo, planeja-se verificar o marco regulatório do setor de dados que pode ser afetado ao reconhecimento facial, bem como evidenciar como a teoria da regulação se mostra adequada para enfrentar o problema de "como" regular esse poderoso instrumento de forma a compatibilizar seu uso pelo Estado e setor privado. Questões sobre limites desse uso também serão tratadas, visto que o reconhecimento facial lida com uma característica diferente que deve ser encarada com a máxima seriedade: possui característica de dado único.

Palavras-chave: Teoria da regulação, Tecnologia, Privacidade, Reconhecimento facial, Segurança pública

Abstract/Resumen/Résumé

Among the new technologies today's, facial recognition is certainly one of the most emblematic. Throughout the article, it aims to verify the regulatory framework of the data sector that can be affected to the facial recognition, as well to show how the theory of regulation proves it's adequacy to face "how" to regulate this powerful instrument in order to make compatible it's use by the State and private sector. Questions about the limits of its use will also be treated, since facial recognition deals with different characteristic that should be viewed with the maximum seriousness: it's characteristic of unique data.

Keywords/Palabras-claves/Mots-clés: Theory of regulation, Technology, Privacy, Facial recognition, Public security

Introdução

A normatização de novas tecnologias é um dos temas mais complexos para os reguladores, tanto pelo fato da dificuldade da ação técnica em si, quanto pela ausência de informações prévias, isto é, estudos que de alguma maneira tenham condão de guiar ou oferecer diretrizes para comportamentos posteriores do tomador de decisões (RANCHODAS, 2015). Trata-se de questão sensível que gira em torno da capacidade dos agentes públicos proverem respostas adequadas e úteis que sejam, ao mesmo tempo, assecuratórias de direitos e potencialmente protetoras da sociedade como um todo.

É baseado nesta dicotomia que o tema do reconhecimento facial se encontra em evidência atualmente. Chama a atenção inclusive por alguns comportamentos surpreendentes tal qual a abolição desta tecnologia justamente num dos locais mais propícios para o seu desenvolvimento: a cidade de São Francisco, nos Estados Unidos – EUA, muito próximo de onde se encontra o maior polo de tecnologia do mundo, o Vale do Silício (GOMES, 2019). A ação de São Francisco foi uma forma de limitar o uso do reconhecimento facial por parte da polícia e demais órgãos governamentais. Isto é, não houve qualquer ingerência restritiva da norma sobre as atividades de empresas privadas, o que abre espaço para ponderações.

Um estudo (BUOLAMWINI; GEBRU, 2018) teve êxito em verificar deficiências de vários sistemas usados hoje no mercado, revelando que o reconhecimento facial de diversas empresas como Facebook, IBM e Google provou ter diversos problemas nesse sistema entre mulheres e negros. Ressalte-se que são justamente essas empresas as mais avançadas do mercado no desenvolvimento desta ferramenta. Segundo as autoras, existiria uma espécie de viés nos algoritmos que impacta o uso da tecnologia, impedindo que pessoas nestas categorias fossem identificadas de forma satisfatória, como estava ocorrendo com homens caucasianos. Há outros estudos nessa direção que geraram análise de pesquisadores do Massachusetts Institute of Technology (AMINI, 2019), os quais construíram códigos numa tentativa de colaborar para reduzir os vieses e com isso evitar tratamento desigual.

Não obstante a gravidade do problema dos algoritmos, há ainda outras facetas do reconhecimento facial que precisam ser enfrentadas. Uma delas diz respeito ao controle por parte de entidades privadas do comportamento de terceiros. Em São Paulo, por exemplo, havia a utilização de reconhecimento facial na linha amarela do metrô pela concessionária ViaQuatro (AMIGO, 2018). Além de exibir anúncios, realizava monitoramento da reação dos usuários às propagandas. O algoritmo era capaz de mensurar o número de espectadores, sua idade e até

mesmo o sexo. Também conseguia classificar o comportamento emocional das pessoas em quatro tipos diferentes: felicidade, insatisfação, surpresa ou neutralidade. Isso ocorria sem qualquer tipo de informação ou permissão dos usuários do serviço público, colocando em xeque até onde pode ir o reconhecimento facial. Uma ação civil pública do Instituto de Defesa do Consumidor (IDEC) conseguiu no judiciário paulista uma medida liminar para desativar tal tecnologia[1].

Feito esse panorama fático, importa afirmar que o setor de reconhecimento facial vem crescendo em ritmo rápido no mundo. Segundo a consultoria MarketsandMarkets o mercado já movimentou mais de 4,05 bilhões de dólares no mundo em 2017 e poderia chegar a 7,76 bilhões de dólares em 2022. Dentre as empresas mais interessadas em consumir este tipo de tecnologia estão os bancos, companhias aéreas, telefônicas, fabricantes de computadores e celulares, dentre outros. O interesse das empresas pela tecnologia também vem acompanhada de uma série de preocupações. O próprio presidente da Microsoft, Brad Smith (SMITH, 2019), em anúncio oficial alertou para o perigo da má utilização dessa ferramenta e para as escolhas que a sociedade necessita fazer a fim de minimizar o risco para a iniciativa privada como um todo e garantir a proteção dos cidadãos em relação a seus direitos fundamentais. Em suma, a preocupação do presidente é que a tecnologia tenha um potencial tão poderoso e tão catastrófico que não haja possibilidade de voltar atrás depois do seu uso indiscriminado, justamente pelo fato da informação dos rostos dos indivíduos terem se espalhado.

Ainda, a informação presente no rosto das pessoas é um dado único que deve ser tratado com o máximo de cuidado possível. Apesar da impressão digital ter a mesma característica de singularidade, quando se fala de reconhecimento facial há um grave problema de incerteza sobre o uso desses dados em público. Ninguém consegue reconhecer o indivíduo pela digital a não ser que este forneça o dado em algum momento específico. No caso do reconhecimento facial, é possível que qualquer pessoa seja identificada, em qualquer lugar, com ou sem seu consentimento. Sobre isso, diferentes pontos podem ser destacados: de onde vieram as imagens que fazem com que as empresas ou o próprio governo sejam capazes de identificar o cidadão comum? O uso dessas imagens deve ser consentido?

Dessa forma, principal motivação para a elaboração deste artigo é a ausência de literatura sobre o tema no Brasil. Em que pese existirem algumas notas esparsas de juristas na imprensa nacional, ainda não houve um estudo sistematizado, de forma a mapear os principais riscos envolvidos na utilização desta inovação sob o ponto de vista legal. No exterior, há alguns

[1] Na justiça de São Paulo, o processo foi protocolado sob a seguinte numeração: 1090663-42.2018.8.26.0100.

estudos que tratam de diferentes problemas atrelados a esta tecnologia de modo geral, abordando dificuldades em suas próprias legislações. Aqui, o diferencial é a utilização da legislação brasileira como base das preocupações que são aventadas pela literatura internacional sobre a temática em um único artigo científico de caráter jurídico.

Objetiva-se, numa primeira parte, utilizar a teoria da regulação para demonstrar as dificuldades de se regular novas tecnologias e numa segunda, expor uma consolidação das principais preocupações ligadas ao reconhecimento facial. Essas preocupações são de enfrentamento obrigatório por parte do futuro regulador sob pena de criar-se insegurança jurídica, tanto para o mercado, quanto para o próprio Estado.

A hipótese aqui apresentada, é que o banimento completo da tecnologia talvez não seja necessária tal qual vem ocorrendo em algumas cidades Estados Unidos.

Em que pese o debate para tais soluções ser bastante amplo, com múltiplas formas, o presente artigo almeja ser um ponto de partida para discussões mais profundas sobre o tema, principalmente sob a ótica da recém-criada Autoridade Nacional de Proteção de Dados no Brasil que tem como uma das suas principais funções a regulação de dados sensíveis, como são os dados biométricos da face humana.

1. A dificuldade de regular novas tecnologias

A regulação é feita baseada em informações (COGLIANESE, 2004) de probabilidade e causa e efeito. As mais clássicas bases para regulação são: externalidades, ausência de competição (barreiras à entrada e monopólios) e assimetrias de informação. No caso da inovação em tecnologia, todos os itens básicos que os reguladores verificam estão ausentes. Primeiro porque, por vezes, ainda não há um mercado propriamente dito. Logo não há como existirem barreiras ou monopólios. Segundo, porque as externalidades não são conhecidas na sua totalidade, pois quando a tecnologia começa a despontar, pode provocar efeitos desconhecidos no médio e longo prazo que o regulador simplesmente não tem condição de prever. Por fim, as assimetrias de informação, quando não são desconhecidas pelo regulador, não possuem leis que imponham um *disclosure*, isto é, mesmo tendo ciência de que possui menos dados do que deveria, a ausência de normas específicas sobre a tecnologia faz com que o regulador continue ignorante àquilo que necessitaria saber.

Nesse sentido, Sofia Ranchordas (RANCHORDAS, 2015) afirma que, muitas das vezes, o governo tenta promover algumas tecnologias sem saber efetivamente os fins que deseja atingir

com a inovação. Tal autora trabalha com três atributos distintos neste caso, o de incerteza, complexidade e temporariedade/flexibilidade. A problemática da incerteza pode ser subdividida em interna (diferentes perspectivas em relação ao produto) e externas (comportamento dos agentes econômicos em face do regulador). O ponto de vista interno seria relacionado a própria característica de inovação em si, uma preocupação com a viabilidade mercadológica dos resultados obtidos no processo de inovação. O ponto de vista externo, por sua vez, teria relação com a incerteza do mercado em relação a uma determinada tecnologia. Em outras palavras, se as empresas não sabem se sua atividade ou produtos desenvolvidos serão autorizados ou, como serão regulados, os seus incentivos de investir acabam por ser reduzidos. Nesse sentido, o *regulatory lag* (BALDWIN, 2015, p. 113) é custoso, pois a indústria pode paralisar completamente por não conseguir prever os riscos inerentes ao desenvolvimento de determinada tecnologia.

Outro aspecto da regulação de novas tecnologias é a complexidade. A inovação é um fenômeno de caráter complexo, devendo ser encorajada por um mix de instrumentos públicos e privados que sejam coerentes e alinhados numa resposta que ao mesmo tempo promova o florescimento da economia e das empresas, ao passo que garanta os direitos fundamentais. A ponderação entre esses valores, no caso concreto, por vezes se mostra difícil pois existem inúmeras zonas cinzentas sobre até onde resguardar o interesse individual. Por isso, é possível que o Estado seja taxado por paternalista ou por libertário a depender das inflexões regulatórias.

Em relação à flexibilidade regulatória, tal atributo é praticamente uma derivação da incerteza, isto é, pelo fato do regulador não ter como prever efeitos que irão ocorrer na realidade após a elaboração de uma norma[2], por vezes seria prudente não adotar legislações com caráter de definitividade. É possível que o legislador queira dar espaço para atividade – *incubating period*[3] – para aprender com o tempo sobre as suas fragilidades. Nesse meio tempo, as legislações poderiam ser adaptadas, não teriam caráter de permanência.

Esse chamamento do Estado para atuar de maneira preventiva pode ser explicado quando o risco inerente às tecnologias é alto. Dá-se o nome de dilema de *Collingridge* (BAPTISTA; KELLER, 2015) quando há dúvidas sobre o melhor momento para regular um recurso tecnológico. No caso do reconhecimento facial, enquanto tal tecnologia não é tão

[2] O comando do Estado pode variar conforme a estratégia que se queira adotar: comando e controle, incentivos, autorregulação, nudge, autorregulação dentre outros.

[3] Um dos setores mais sensíveis a inovações é o financeiro. A velocidade que a tecnologia vem mudando na área de mercado de capitais poderia ser melhor estudada através desse mecanismo regulatório, que permitiria observação de novas formas de atuação, que podem ser aproveitadas em larga escala caso verifique-se que a atividade não causaria danos.

popularizada, ainda há tempo de moldá-la de forma a antecipar consequências indesejáveis. Obviamente, não serão todas previsíveis mas, com o tempo, é possível fazer as devidas adaptações[4]. Não sendo possível o equilíbrio, o que se observa é o banimento do produto ou serviço por meio de regulação. Tal ação já ocorreu no caso de São Francisco em relação ao reconhecimento facial. A percepção do regulador sobre a invenção é fundamental na escolha dos mecanismos jurídicos a serem utilizados quando encaram o elemento chave das escolhas públicas de novas tecnologias: o risco.

Escolher falar de risco em relação a novas tecnologias deve ser sempre uma preocupação inerente ao regulador. Primeiro, porque precisa decidir se uma determinada inovação tem probabilidade de resultar em algum tipo de benefício para a coletividade. Segundo, porque caso a resposta anterior seja positiva, precisa escolher se efetivamente vale ou não a pena intervir com vistas a parametrizar o setor, eis que poderia simplesmente deixar que os próprios agentes privados se autorregulem. Terceiro, porque se escolherem regular, precisam decidir a intensidade do controle que será utilizado na sua normatização[5].

Caso escolham normatizar, os reguladores precisam decidir sobre a abrangência da norma. No setor de tecnologia, há dois riscos bastante distintos. Enquanto a regulação específica de uma inovação pode ocasionar uma rápida perda do objeto por uma mudança de paradigma tecnológico, uma regulação ampla pode não contemplar especificidades de alguns segmentos que contenham alguma probabilidade de causar dano.

A literatura sobre a possibilidade de regulação de novas tecnologias é ampla. Para Daniel J. Gervais (GERVAIS, 2010), o melhor curso de ação a ser tomado seria a ausência de intervenção estatal, com exceção apenas quando se estivesse diante de tecnologias que pudessem impactar gravemente algum aspecto de segurança pública. O autor justifica sua escolha com base no princípio da precaução. Afirma que a ausência de regulação também pode ser considerada uma medida regulatória, pois a análise do regulador impacta na escolha pela intervenção ou não no setor específico. Diz ainda que a tecnologia, especialmente em seus estágios iniciais, tende a reagir mais ao mercado (demanda de usuários) e à regulação, mas depois de algum tempo adquire "vida própria". A regulação poderia transformar a tecnologia de forma que a deixasse muito longe das expectativas dos usuários e do potencial que ela teria

[4] Conforme se observa, modelos de negócios diferentes possuem características bastante distintas no que tange ao seu início em termos de tecnologia. Enquanto os patinetes e os aplicativos de transporte individual aproveitaram uma onda de permissividade impulsionada pela aceitação popular, o reconhecimento facial já nasce com polêmica em relação a controvérsias sobre privacidade e segurança pública.

[5] Lyria Bennet Moses (MOSES, 2014) faz importante ressalva sobre a regulação de novas tecnologias. Para ela, apenas o fato de uma nova tecnologia ser ou não disruptiva não significa necessariamente que vá ocorrer uma regulação específica. Nem toda nova tecnologia estaria inserida no Paradoxo de *Collingridge*.

caso não sofresse ingerência estatal. Não está descartado que tais mudanças não intencionais na tecnologia poderiam criar problemas iguais ou piores que aqueles identificados no objetivo regulamentar inicial.

Por sua vez, Tim Wu (WU, 2011) afirma que setores que utilizam tecnologia em condições de alta incerteza – como é o reconhecimento facial –, se beneficiariam mais com regimes de controle informais que controles rígidos, substituindo as punições com sistemas de ameaças, guias e princípios interpretativos. No entanto, ele não afirma que essa substituição deveria ocorrer em todas as circunstâncias. De acordo com Wu, quando absolutamente necessário, o regulador precisaria aplicar medidas de *enforcement* estatal, podendo ser do tipo comando e controle.

Essa teoria de Wu se mostra de acordo com doutrinas mais clássicas de direito regulatório, em especial com Ian Ayres e John Braithwaite quando explicam a teoria das *benign big guns*[6]. A mera possibilidade de utilização de força por parte do Estado, por vezes, pode ser uma opção suficiente para encorajar os agentes privados a cooperarem através de *soft law*.

Sob diferente perspectiva, Nathan Cortez (CORTEZ, 2014) contesta a ideia de que a utilização de *soft law* a longo prazo forneça resultados positivos em nível ótimo. Para ele, com o passar do tempo, a postura flexível do regulador poderia de alguma forma ser calcificada, criando uma posição de inércia deste em relação aos agentes econômicos. Significa dizer que a medida que a inovação amadurece e seus riscos se tornam mais evidentes, justificativas iniciais para algumas legislações podem não subsistir.

Isso pode de fato ocorrer, especialmente quando haja uma grande discrepância entre os níveis de intensidade das punições que o próprio Estado pode aplicar. Explica-se: pela teoria das *benign big guns* numa escala de zero a dez em nível de força, caso o Regulador possua punições de nível 2 e 10 tão somente, fica bastante limitado a utilização da punição número 2, de forma que os agentes privados, na grande maioria dos casos, poderiam desconsiderar a punição de força 10, pois teria um custo demasiadamente alto ao regulador para utilizá-la de forma frequente.

Em que pese as diferentes opiniões dos autores sobre a necessidade de atuação do estado ou mesmo a intensidade de controle das novas tecnologias, diferentes estratégias precisarão ser criadas a depender do risco concreto. Por esse motivo, serão analisados os principais pontos que devem chamar a atenção do regulador no momento de avaliar as políticas regulatórias a

[6]Ian Ayres e John Braithwaite (AYRES, BRAITHWAITE, 1992, p. 40) explicam a teoria como agências reguladoras que dificilmente puniam de forma muito dura, mas a mera ameaça de punição já era suficiente para o cumprimento da legislação em razão da abrangência de seus poderes.

serem criadas no setor de reconhecimento facial. É possível que numa análise de custo-benefício (SUNSTEIN, 2014) se opte por não realizar restrições de cunho regulatório, porém, as situações necessitarão ser ao menos estudadas e avaliadas, justificando-se o porquê da aplicação ou não de uma medida.

2. Principais riscos inerentes à regulação do reconhecimento facial

A tecnologia de reconhecimento facial, além de possuir todos os elementos alertados no tópico anterior, ligados a complexidade, incerteza e risco, também se caracteriza por ser um instrumento em que os lados da relação sofrem de antigos problemas regulatórios ligados a assimetria de informação e racionalidade limitada daqueles que têm seus dados coletados. Anthony Ogus (OGUS, 2004, p. 38) discorre sobre o consenso dos economistas sobre a incapacidade de se erigir um modelo de tomada de decisão baseado numa racionalidade "pura", devendo-se sempre levar em consideração uma vontade humana de satisfação própria, sem importar os riscos. Se, numa situação hipotética, um aplicativo não pode ser utilizado sem que haja a cessão de dados, será que o indivíduo deixaria de utilizar o serviço com medo do que poderia ocorrer com suas informações? A probabilidade de se buscar uma satisfação própria não é objeto de estudo do direito, mas o comportamento humano tampouco pode ser deixado de fora da análise ao se pensar na função regulatória.

No presente tópico, serão apresentados os principais riscos ligados especificamente ao reconhecimento facial, dentre eles: a) Problemas com a precisão da tecnologia; b) Controle da Privacidade; c) Opacidade Informacional; d) O uso pelo Estado na segurança pública; e e) Necessidade de consentimento.

2.1. Problemas com a precisão da tecnologia

Um dos principais problemas observáveis hoje com a tecnologia de reconhecimento facial é, em primeiro lugar, a sua falta de precisão. Diferentemente de outros recursos já amplamente disseminados – como o exame de DNA para verificar a paternidade de crianças com taxas acima de 99,9% de precisão – a identificação de pessoas por meio de algoritmos ainda se mostra uma inovação em desenvolvimento. O legislador brasileiro, criou uma legislação sobre o exame de DNA que afirma àquele que se recusa a fazer o exame de paternidade, que será considerado pai (Lei nº 12.004/2009). Isso se dá porque o exame é

extremamente preciso. No caso do reconhecimento facial, um sistema que tenha taxa de acerto não tão seguro, não deve possuir um regramento deste tipo, sob pena de poder ocasionar que um inocente tenha que produzir provas impossíveis ou de difícil produção.

Confiar cegamente neste tipo de instrumento não se revela uma condição acertada, embora seja possível a sua conjugação com outros tipos de tecnologia para evitar maiores incidentes. O ponto em que tal tecnologia seria aceitável para ser utilizada como prova, por exemplo, ainda dependeria da avaliação do regulador e do próprio judiciário. Questões importantes do direito penal poderiam ser questionadas por margens de erro muito grandes, por exemplo.

Há estudos (KLARE, et al, 2012) que comprovam que a tecnologia ainda não consegue ter uma margem de erro pequena, gerando resultados que são tendenciosos ou que aumentam o risco na tomada de decisão. Infere-se, portanto, que esse risco é derivado da técnica, e a abordagem deve dizer respeito ao desenvolvimento da tecnologia de reconhecimento facial. Um destes estudos, citado na introdução do artigo (BUOLAMWINI; GEBRU, 2018) afirma a incapacidade de reconhecimento do rosto de pessoas negras ou de mulheres por um determinado programa. Isso revela um comportamento dos programadores da inteligência artificial em relação ao banco de dados: a discriminação algorítmica (BAROCAS; SELBST, 2016). Esse conceito não pode ser tomado ao pé da letra como uma ação fundada num suposto preconceito do programador. Ao contrário, o que ela quer explicar são os efeitos nocivos que os códigos podem ter na vida das pessoas, mesmo sem ser essa sua intenção.

Há outro estudo (WILLIAMS; BROOKS; SHMARGAD, 2018) que concluiu que algoritmos podem sim apresentar vieses não previstos por seus criadores, especialmente quando aplicados ao *machine learning* na qual os softwares realizam por si mesmos correlações baseadas em perfis próximos. No que tange ao reconhecimento facial, isto poderia implicar em situações limites nas quais o sistema sempre poderia apresentar falsos positivos em relação a um determinado grupo de pessoas em detrimento de outras.

Isso ocorreu nos EUA com congressistas americanos. Ao utilizar o aplicativo "Rekognition" da Amazon em deputados e senadores, o sistema apresentou falsos positivos em 28 destes, afirmando que haviam cometido algum tipo de crime. A aplicação relacionou as imagens dos políticos a fotos em bancos de dados de pessoas presas. A Associação para as Liberdades Civis dos EUA (SNOW, 2018) confirmou a informação de que o algoritmo de reconhecimento facial vem apresentando falhas quando se trata de pessoas negras. Cerca de 40% dos políticos falsamente identificados como infratores estavam inseridos nesse segmento

da população, o que causa surpresa, visto que ele representa apenas 20% dos membros de ambas as casas do Congresso americano. Além disso, destaca-se que os próprios criadores da aplicação de reconhecimento facial afirmam que ele tem sucesso em 80% das vezes, sendo inclusive vendido para órgãos de segurança pública. Várias entidades de defesa civil já se posicionam de forma contrária à venda deste aplicativo pela Amazon aos entes públicos, questionando sempre sua taxa de sucesso.

Ao menos os aplicativos e programas que se tem notícia no mercado ainda não possuem um nível de sofisticação que consiga bater os 100% de acerto, justamente ao contrário. Este ponto, em que pese não ser um problema regulatório em si, merece a atenção do regulador na medida em que a tecnologia se presta eminentemente para identificação. Se isso não é feito a uma altíssima taxa de sucesso, a ferramenta é inócua, e talvez seja positivo não permitir que ela seja utilizada de forma isolada em determinadas situações como prova definitiva.

2.2. Controle da Privacidade

Outro aspecto fundamental sobre o reconhecimento facial é o debate sobre o nível de privacidade[7] que as pessoas devem possuir. O reconhecimento facial tem um grande poder não só de identificação do indivíduo, mas também o de correlacionar informações pessoais com seu rosto. É possível avaliar idade, sexo, e até mesmo emoções pessoais. Outro apelo da tecnologia é a possibilidade de acompanhamento desses indivíduos em tempo real.

Por isso, existem três posições muito distintas sobre privacidade: a primeira, reconhece a tecnologia de reconhecimento facial como um risco além do tolerável, de modo que a sociedade como um todo tenha a possibilidade de ser controlada invariavelmente pelo Estado e pelas empresas do mercado. Para essa primeira corrente, o caminho natural seria o de banimento total desta tecnologia. Uma segunda visão, de caráter intermediário, defende uma visão de sopesamento entre prós e contras, limitando-as com regras naquilo que puder ser prejudicial à sociedade como um todo. Uma terceira via, seria a retirada do Estado de qualquer tipo de controle do reconhecimento facial, passando tal encargo para a iniciativa privada, que poderia se organizar de diferentes formas como a autorregulação, ou estabelecendo diretrizes e códigos de conduta para minimizar impactos.

[7] Lisa Austin (AUSTIN, 2003) faz um contraponto também sobre o conceito de privacidade na atualidade. Para a autora, a tecnologia não está simplesmente erodindo a privacidade. Ela também pode estar forçando a repensar o que se entende por privacidade. Cada vez mais, haveria uma maior preocupação com as práticas que envolvam coletar, usar e divulgar informações que não sejam sensíveis ou íntimas e isso é cada vez mais coletado em público, preocupações que não caem facilmente dentro do domínio da teoria da privacidade tradicional.

O direito ainda não possui normas para se adequar a uma realidade dessas que, por mais que pareçam distantes no tempo, já existem e são praticadas pela iniciativa privada[8]. O risco à privacidade atrelado ao reconhecimento facial é mais evidente do que o de qualquer outra tecnologia de identificação por dados sensíveis (impressão digital, íris, linhas das mãos, biometria vascular e voz), pois não se pode ter certeza de quando se está sendo vigiado se tal situação não for informada.

Tais aspectos perpassam pela noção de tratamento de dados e, a partir do momento em que se encontram em poder das empresas, estas podem adaptar tais sistemas de acordo com suas necessidades. Um exemplo disso seria a identificação de pessoas com histórico de algum tipo de crime ou contravenção em tempo real por seguranças de shopping ou sistemas de notas por comportamento como já ocorre na China.

Não obstante aos riscos de abusos, também há uma janela de oportunidade sobre a coleta de dados, em especial com o viés de aproveitamento sobre gostos, encaminhamento de publicidade direcionada e aumento de facilidades como o desbloqueio de celulares. O que se quer evidenciar são os cuidados que se deve ter em relação ao mau uso da tecnologia. Com o reconhecimento facial, é possível pensar em soluções personalizadas para os clientes a partir do momento em que acessam algum estabelecimento comercial ou mesmo suas próprias casas. Nenhuma dessas soluções é capaz de apresentar uma ameaça substancial à autonomia individual, razão pela qual atendem a finalidade que se espera da tecnologia.

Como foi visto, não é vedado o tratamento de dados no Brasil, e o desenvolvimento de tal atividade garante que empresas tenham uma vantagem competitiva em relação às outras, e isto, por si só, não ofende qualquer direito fundamental.

Igualmente, a preocupação exposta em relação às empresas se aplica parcialmente em relação ao Estado. A própria legislação brasileira se encarregou de ressalvar a regência da atividade de segurança pública pela LGPD. A ponderação de princípios jurídicos pelo legislador, neste caso, fez prevalecer o interesse coletivo sobre o individual. O papel do regulador, neste caso, é refletir sobre os limites da liberdade empresarial e individual, e tentar prover os usuários de alguns tipos de controle específico para terem ciência do que se passa com seus dados.

[8]Um estudo da Universidade de Direito de Harvard (HARVARD UNIVERSITY, 2007) evidencia a limitação do sistema jurídico americano atual para responder os desafios apresentados pelo reconhecimento facial através de normas de responsabilidade civil tradicionais, e que um novo arcabouço jurídico deveria ser criado para dar tratamento a tais dificuldades.

2.3. Opacidade Informacional

Um dos grandes problemas verificados no ambiente de coleta de dados, é a opacidade informacional. Significa dizer que o usuário comum, após a entrega de seus dados, sejam ou não sensíveis, não serão notificados a cada vez que há uma transferência de suas informações para um terceiro. Nos termos do art. 18, inciso VII da Lei nº 13.709/2018, o usuário que é o proprietário dos dados possui direito a receber informações sobre o compartilhamento de seus dados somente mediante requisição.

Esse tipo de procedimento pode provocar uma grande assimetria de informação(BINENBOJM, 2016). Isso porque não se sabe se o terceiro que recebeu os dados do usuário irá poder repassá-los a outras empresas, fazendo com que o indivíduo tenha sempre que perseguir a sua própria informação. Isso não ocorreria caso as notificações se dessem de forma automatizada, melhorando o controle e provendo informações para a parte que menos força possui na relação de poder[9].

Hoje, ainda antes da produção de efeitos da LGPD (está em *vacatio legis* até agosto de 2020), os reais detentores dos bancos de dados não informam para ninguém o que fazem com seu acervo, visto que, tecnicamente, não há qualquer obrigação legal para isso, no momento. São esses bancos de dados os responsáveis pelo treinamento da inteligência artificial que funciona no reconhecimento facial. O funcionamento delas se dá da seguinte maneira: algumas tecnologias "aprendem" a identificar o rosto de pessoas com informações obtidas em bancos de dados e, mesmo depois de anos, baseando-se em novas fotos, podem adaptar-se a mudanças como o envelhecimento, uso de acessórios e até mesmo uso de barba. Os bancos de dados das empresas são fundamentais para gerar padrões complexos que permitem individualizar os dados biométricos. Quanto maior o banco de dados, mais valioso ele é dada a dificuldade de conseguir tantos rostos.

Sob perspectiva estatal, a própria Administração Pública não pode compartilhar as informações dos usuários para terceiros. Porém, essa regra possui algumas exceções, previstas no art. 26 da Lei nº 13.709/2018. O inciso I prevê que, em casos de execução descentralizada de atividade pública que exija a transferência de dados, o Poder Público pode realizá-la. Pensando no reconhecimento facial, isso abre brechas para a utilização do instrumento para

[9] A situação pode se resumir ao controle que o indivíduo pode ter em sua vida. Para Lawrence Lessig (LESSIG, 1999), é necessário que os indivíduos tenham poder de conhecer as situações que estão inseridos, especialmente quando se trata de tecnologias que estão aptas a controlar o comportamento social. O autor afirma que, caso esse controle se desse de forma física, provavelmente a sociedade como um todo não iria aceitar tão facilmente.

qualquer atividade de segurança, em especial nas imigrações de portos, aeroportos e fronteiras secas. Esse ponto irá demandar atenção do regulador, visto que o Estado terá uma grande base de dados para realizar atividades de segurança pública sem a necessária autorização do indivíduo. Compartilhar tais informações com empresas privadas (concessionárias de aeroportos, por exemplo) em atividades de fiscalização de segurança em fronteiras exigirá um regramento bastante restritivo no tratamento desses dados.

2.4. O uso pelo Estado na segurança pública

Os artigos 23 a 30 da Lei nº 13.709/2018 fazem referência à forma como o tratamento de dados se dará no âmbito da Administração Pública. O art. 11, inciso I e § 2º desta mesma lei permite ao Estado o exercício de algumas atividades independentemente de consentimento de terceiros, em especial quando ficar caracterizada uma obrigação legal ou em políticas públicas. Como as políticas públicas são matérias a serem decididas pelo chefe do Executivo, ele possui discricionariedade para escolher as melhores ferramentas para auxiliar as forças de segurança pública. O reconhecimento facial é uma delas. O objetivo seria a inibição da criminalidade sem que fosse necessário o consentimento dos cidadãos.

Esse raciocínio faz sentido pois a obtenção de tal consentimento em lugares públicos inviabilizaria completamente a tecnologia utilizada para este fim. Em verdade, o software não teria como filtrar quem poderia ou não ser reconhecido no meio de uma multidão em espaços públicos. A obtenção de consentimento, neste caso, não teria pertinência. A tecnologia seria aplicada a todos, ou a ninguém.

Em que pese o tratamento de dados pessoais para fins de segurança pública ainda estar pendente de regulamentação, é preciso considerar que a tecnologia de reconhecimento facial já se encontra presente hoje, e a tendência é de ampliação do seu uso se não houver posicionamento contrário por parte do Estado[10]. O que se verifica no setor hoje é uma verdadeira desconexão regulatória (VIANNA, 2019) entre as normas em vigência no ordenamento e a realidade fática que se impõe em todo o mundo.

Testes já foram realizados em diversos lugares do Brasil, como Rio de Janeiro, Salvador e Búzios. Nesse "vazio" normativo específico, a Administração Pública age com uma maior discricionariedade (KRELL, 2004), sem qualquer limitador específico derivado de lei pois,

[10] Além da cidade de São Francisco ter banido o reconhecimento facial em maio de 2019, outras cidades baniram o reconhecimento facial por parte do Estado. São exemplos dessas cidades: Somerville em junho de 2019 e Oakland em julho de 2019.

além da LGPD não ter poder ser aplicada até agosto de 2020 e a ANPD foi recém-criada, nem mesmo há previsão de aprovação da legislação específica para questões de segurança pública e defesa nacional. Resta evidente a ocorrência do descompasso regulatório na coordenação da tecnologia.

Tais utilizações do sistema de reconhecimento facial também não tiveram dados do seu funcionamento divulgado ao público. Sabe-se que algumas pessoas foram detidas pela polícia, mas não a quantidade de falsos positivos gerados pelo sistema. Os testes, também foram realizados em ambientes específicos para que se pudesse aprender a utilizar a tecnologia. Esse tipo de experimentalismo (JORDÃO; MENDONÇA, 2019) é positivo para a Administração Pública, em especial às forças de segurança, pois grandes eventos certamente trazem riscos de maiores proporções que o Estado tem o dever de coibir usando todo o ferramental disponível dentro de limites da proporcionalidade. A identificação e perseguição de potenciais infratores é eficaz a partir do momento em que se possa confiar na tecnologia. Assim, a sociedade como um todo se sente mais protegida ao passo que condutas ilícitas pelo medo de identificação são inibidas.

Uma das situações que ficarão a cargo do regulador é se o sistema de reconhecimento facial irá atuar de maneira simultânea às gravações ou apenas será utilizado em caso de ocorrência de algum ilícito de forma posterior (GARVIE, et al, 2016). Há uma diferenciação substancial entre uma situação e outra a ser ponderada. No primeiro caso, os ilícitos poderiam ter uma resposta mais rápida, no entanto, a depender do banco de dados utilizado, a polícia poderia verificar quem são as pessoas presentes nos eventos e tratá-las de forma diferenciada baseado em aspectos como a reincidência penal. Isso seria um aspecto negativo. No segundo caso, ninguém poderá ser identificado imediatamente, garantindo a privacidade do cidadão perante a Administração Pública, podendo-se até mesmo evitar algum tipo de perseguição política imediata. Por outro lado, a resposta simultânea ficaria prejudicada, tendo em vista que o *software* não estaria funcionando simultaneamente, mas sim através de solicitações humanas.

Outro desafio enfrentado pela Administração Pública no campo da segurança pública diz respeito à captação de dados. Ainda não restou claro na legislação como a gestão de dados biométricos será feita ou como tais dados serão obtidos, se serão por meio de cadastros que o Estado já possui ou por meio de solicitação de empresas privadas ou ainda via convênios internacionais. A lei, em regra, somente impede o acesso da iniciativa privada aos dados do poder público (art. 27), mas é silente em relação ao inverso.

É esse outro importante assunto sobre a segurança pública que deve ser aqui abordado. Alguns dos deveres de proteção de dados conferidos por lei foram delegados para a Autoridade Nacional de Proteção de Dados, entre elas: dispor sobre as formas de publicidade das operações de tratamento de dados (art. 23, §1º) e regulamentar como será feita a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoas de direito privado (art. 27, parágrafo único).

Uma preocupação que o regulador deve se ater é sobre a diferença entre o compartilhamento de dados comuns ou dados sensíveis entre o Estado e as empresas. Em que pese as hipóteses de transferências serem limitadas, no caso do reconhecimento facial, pensa-se em hipóteses de que os dados não necessariamente deveriam ser compartilhados com o concessionário de serviço público, mas sim oferecido o software para sua utilização, sem possibilidades de acesso ao banco de dados em si. Tal solução satisfaria os anseios do Poder Público no quesito segurança, sem a necessidade de compartilhamento de dados que já são obtidos sem consentimento.

Ainda, em relação ao Estado, há o risco de vigilância de um único indivíduo (GARVIE, et. al, 2016), de forma específica, por muito tempo. Este tema terá condão de despertar bastante polêmica, podendo a vir se constituir em prova ilícita caso a jurisprudência se firme no sentido que seria necessária intervenção do Judiciário tal qual ocorre com grampos telefônicos.

Daí a importância de uma lei que regule a legalidade das operações estatais na área de reconhecimento facial e segurança pública que já foi prevista na LGPD pois, enquanto esta prevê normas gerais para utilização de dados no setor privado, aquela terá função de regulamentar a utilização de dado biométrico em um setor que pode gerar diversas violações à intimidade.

2.5. Necessidade de consentimento

Um problema relacionado a assimetria de informação é o fato do desconhecimento por parte do indivíduo se uma determinada câmera consegue ou não identificá-lo na multidão. No caso citado na introdução sobre o metrô de São Paulo, essa informação não era fornecida ao usuário do serviço público. Isso porque não é a câmera que vai ser importante para a inovação, mas sim o algoritmo do sistema por trás dela. É nesse momento em que aspectos sobre quem deve ter acesso a tal tecnologia devem surgir. Michal Copps (COPPS, 2005) afirma que o setor privado pode, deve e vai atuar como uma verdadeira locomotiva de inovação, com função de

liderar as mudanças que vem ocorrendo. Cabe ao regulador tentar prever tais movimentos e reagir a eles de forma a parametrizar o que pode e o que não pode ser feito.

As empresas já conseguem extrair informações como idade, sexo, personalidade, estado de saúde e emocional somente utilizando câmeras, o que torna fundamental a adoção de comportamentos que deem transparência a respeito de quais dados estão sendo coletados e por qual tratamento estão passando. Vazamentos de dados são uma tônica da sociedade atual, e qualquer evidência de que os dados coletados estão servindo para objetivos não informados, ou ilícitos, causarão grande impacto sobre a reputação (BALDWIN, et al, 2015) da empresa violada.

Os sistemas mais avançados de reconhecimento facial estão sendo desenvolvidos hoje por empresas do setor privado, e não somente pelos Estados. Estes, por sua vez, estão tomando várias medidas para obter mais informações. Nos EUA, por exemplo, foi revogada legislação (PEREDA, 2017) que estabelecia que os provedores de internet deveriam proteger a privacidade de seus clientes e que impunham várias restrições sobre o uso de informações, além da promulgação de novas legislações temerárias como a *Cloud Act*[11].

No entanto, o fato do modelo de negócio das empresas envolver a coleta de dados não faz com que elas não possam desenvolver mecanismos de reconhecimento facial, visto que há uma demanda por mais tecnologia na sociedade como um todo. A regulação sobre essa ferramenta não implica em inviabilizá-la no setor privado, mas sim compatibilizá-la com as melhores práticas possíveis. Dar ciência ao transeuntes sobre o sistema de reconhecimento facial parece ser uma medida que faz sentido, assim como apresentar informações de maneira clara em termos de uso de aplicativos e sites.

3. Conclusão

Todos os problemas que derivam de novas tecnologias tem grande potencial de apresentar questionamentos em razão da novidade que apresentam. Isso não implica dizer que não há possibilidade de controlá-las de alguma forma mínima. Algumas vezes, é preciso vislumbrar movimentos de mercado para ter certeza do que fazer, utilizando o experimentalismo. Por outras, é preciso vetar a disseminação da tecnologia por apresentar um

[11] Apelidada de Cloud Act (sigla para Clarifying Lawful Overseas Use of Data Act) a legislação permite abrir o sigilo de servidores de empresas americanas hospedados fora dos EUA. A promessa é de que a lei facilitará a obtenção de dados digitais como provas em processos da Justiça americana. A crítica a esta prerrogativa é que poderia haver dano a direitos fundamentais de cidadãos estrangeiros, e por consequência, afetação da soberania de outros países.

perigo muito alto para a sociedade. Por fim, é possível que ela seja amplamente disseminada no mundo sem que o Estado precise ingressar para regular qualquer aspecto, visto que a complexidade e incerteza estão em patamares mínimos aceitáveis ou ainda inexistentes.

O que se quis passar no presente artigo é que a regulação do reconhecimento facial é necessária, possui peculiaridades que não estão presentes em outros tipos de inovação, e merecem tratamento diferenciado do Estado. Para isso, alguns pontos que vem chamando mais atenção foram abordados na tentativa de despertar a atenção da sociedade como um todo e principalmente, daqueles que terão a complexa tarefa de pensar soluções para o enfrentamento da questão. Obviamente, outros riscos mais agudos poderão surgir com o tempo. O que o mapeamento realizado se propôs foi ser um marco inicial no apontamento de dificuldades e gargalos que devem ser enfrentados pelos proponentes das normas.

Por ser uma temática que implica numa compreensão global, é possível que muitos regulamentos sobre o reconhecimento facial venham a surgir no mundo com diferentes propósitos. Enquanto na China, poderia ser tolerável um controle maior da população por meio de reconhecimento facial, dificilmente a população de outros países de cunho mais liberal aceitariam a proposta de serem monitorados pelo Estado de forma a saber até mesmo suas reações ou intenções.

Em que pese não se tenha chegado a um patamar no qual a tecnologia seja tão precisa, certamente é uma questão de tempo para seu aprimoramento, o que vai despertar discussões mais acaloradas da sociedade sobre a dicotomia entre privacidade e publicidade em face de empresas e ao Estado. Nesse momento, não só o regulador será chamado a elaborar normas, mas também o legislador movido pelos clamores de diferentes grupos presentes na sociedade. Em que pese se tratar de dados e haver lei e um órgão próprio (talvez uma agência futura), há dúvidas se poder-se-á falar de uma suposta reserva do regulador (GUERRA, 2018) em tema tão caro a interferência legislativa sob fundamento de se estar tratando de política pública.

Não obstante, temas sensíveis como consentimento, privacidade, participação popular e assimetrias de informação entre o indivíduo e as empresas perpassarão por escolhas do regulador. Não necessariamente uma solução única de comando e controle será suficiente para dar conta de toda a complexidade do setor para obter níveis ótimos de resposta da iniciativa privada. Na realidade, acredita-se que instrumentos como a autorregulação regulada (SADDY, 2015) e *nudges*, bem como políticas de *Big Guns* podem ser aplicadas no setor de reconhecimento facial, a depender de quem está usando a ferramenta (empresas, governo ou indivíduos).

Por fim, diante dos poucos escritos no Brasil sobre o tema, o presente texto não teve o objetivo de esgotar a discussão. Pelo contrário, por ser um assunto que tende a crescer diante da aceleração de troca de dados e desenvolvimento tecnológico mundial, pode-se afirmar que é um pontapé inicial na academia jurídica brasileira. Regular tecnologias, como se viu, não é simples, e quanto mais cedo os riscos de setores complexos forem levantados, maiores serão as discussões, e consequentemente o desenvolvimento de respostas para temáticas instigantes.

4. Referências bibliográficas

ABBOT, Carolyn. Bridging the Gap - Non-state Actors and the Challenges of Regulating New Technology. **Journal of Law and Society**, Vol. 39, nº 3, pp. 329-358, 2012.

AMIGO, Ignacio. **The Metro Stations of São Paulo That Read Your Face**. Disponível em: <https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/>. Acesso em 16/06/2019.

AMINI, Alexander et al. **Uncovering and Mitigating Algorithmic Bias through Learned Latent Structure**. Proceedings of the 2019 AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society (AIES), 2019.

AUSTIN, Lisa M. Privacy and the Question of Technology. **Law and Philosophy**, Vol. 22, 2003.

AYRES, Ian; BRAITHWAITE, John. **Responsive Regulation**: Transcending the Deregulation Debate. Nova York: Oxford University Press, 1992.

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding Regulation**: Theory, Strategy and Practice. 2ª ed. Londres: Oxford Scholarship, 2015.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. **Revista de Direito Administrativo**, Rio de Janeiro, v. 273, p. 123-163, 2016.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review**, Vol. 104, pp. 671-732, 2016.

BINENBOJM, Gustavo. Novas tecnologias e mutações regulatórias nos transportes públicos municipais de passageiros: um estudo a partir do caso uber. **Revista de Direito da Cidade**. vol. 08, nº 4. pp. 1690- 1706, 2016.

BUOLAMWINI, J.; GEBRU, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. *In*: **Conference on Fairness, Accountability and Transparency**, pp. 77–91, 2018. Disponível em:

<http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Acesso em 16/06/2019.

COGLIANESE, Cary; ZECKHAUSER, Richard; PARSON, Edward. Seeking Truth for Power: Informational Strategy and Regulatory Policymaking. **Minnesota Law Review**, Vol. 89, pp. 277-341, 2004

COPPS, Michael J. Disruptive Technology: Disruptive Regulation. **Michigan State Law Review**. 2005.

CORTEZ, Nathan. Regulating disruptive innovation. **Berkeley Technology Law Journal**, n. 29, p. 175-228, 2014.

COUTINHO FILHO, A. Regulação 'Sandbox' como instrumento regulatório no mercado de capitais. **Revista Digital de Direito Administrativo**, Vol. 5, nº 2, p. 264-282, 2018

FEIGELSON, Bruno; SILVA, Luiza Caldeira Leite. ANPD - Autoridade autoritária de dados. **JOTA**, 01 de janeiro de 2019. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/anpd-autoridade-autoritaria-de-dados-01012019>. Acesso em 18/06/2019.

FERRETI, Maria Paola. Risk and Distributive Justice: The Case of Regulating New Technologies. **Science and Engineering Ethics**, pp. 501-515, 2010.

GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. **The Perpetual Line-Up**: Unregulated Police Face Recognition in America. George-town Law, Center on Privacy & Technology, 2016.

GERVAIS, Daniel J., The Regulation of Inchoate Technologies. **Houston Law Review**, Vol. 47, nº 3, 2010.

GOMES, Helton Simões. **Por que uma das maiores cidades dos EUA baniu o reconhecimento facial**? Disponível em: <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/05/16/por-que-uma-das-maiores-cidades-dos-eua-baniu-o-reconhecimento-facial.htm>. Acesso em 16/06/2019.

GUERRA, Sérgio. **Discricionariedade, regulação e reflexividade**: uma nova teoria sobre as escolhas administrativas. 5ª. ed. Belo Horizonte: Fórum, 2018.

HARVARD UNIVERSITY. In the Face of Danger: Facial Recognition and the Limits of Privacy Law. **Harvard Law Review**, vol. 120, nº 7, pp. 1870–1891, 2007.

JORDÃO, Eduardo Ferreira; MENDONÇA, José Vicente dos Santos. A lei de liberdade econômica e a 'regulação experimentalista'. **Conjuntura Econômica** (Rio de Janeiro), v. 73, p. 30-31, 2019.

KLARE, Brendan F; BURGE, Mark J; CKLONTZ, Joshua; BRUEGGE, Richard W Vorder, JAIN, Anil K. Face recognition performance: Role of demographic information. **IEEE Transactions on Information Forensics and Security**, Vol. 7, nº 6, pp. 1789–1801, dez/2012.

KRELL, Andreas J. A recepção das teorias alemãs sobre "conceitos jurídicos indeterminados" e o controle da discricionariedade no Brasil. **Revista Interesse Público**, Porto Alegre, v. 23, p. 21-49, 2004.

LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. **Harvard Law Review**, Vol. 113, nº 2, pp. 501-549, 1999.

LYNCH, Jennifer. **What Facial Recognition Technology Means for Privacy and Civil Liberties**. Written testimony to the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law. 18 de Julho de 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134497>. Acesso em: 19 de julho de 2019

MARCHANT, Gary E.; ALLENBY, Braden R.; HERKERT, Joseph R. **The growing gap between emerging technologies and legal-ethical oversight**: the pacing problem. Dordrecht: Springer, 2011.

MARKETSANDMARKETS. **Facial Recognition Market worth $7.0 billion by 2024**. Disponível em: <https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp>. Acesso em: 21/06/2019.

MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with 'technology' as a regulatory target law. **Innovation and Technology**, pp. 1-20, 2014.

OGUS, Anthony. **Regulation**: Legal Form and Economic Theory. Oxford: Hart Publishing, 2004.

PEREDA, Cristina F. EUA aprovam lei que permite aos provedores de internet vender dados dos usuários. **Él País**, 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/03/28/internacional /1490738196_593249.html>. Acesso em 17/06/2019.

RANCHORDAS, Sofia. Does Sharing Mean Caring: Regulating Innovation in the Sharing Economy. 16 Minn. **J.L. Sci. & Tech**. pp. 413-476, 2015.

SADDY, André. **Regulação Estatal, Autorregulação Privada e Códigos de Conduta e Boas Práticas**. Rio de Janeiro: Lumen Juris, 2015.

SALINAS, Natasha Schmitt Caccia. **Regulação em números**: Mecanismos de Participação das Agências Reguladoras Federais. Disponível em: <https://direitorio.fgv.br/sites/direitorio.fgv.br/files/u2999 /working_paper_-_mecanismos_de_participacao_de_agencias_reguladoras.pdf>. Acesso em: 11/07/2019.

SMITH, Brad. **Reconhecimento Facial: é hora de agir**. Disponível em: <https://news.microsoft.com/pt-br/reconhecimento-facial-e-hora-de-agir/>. Acesso em 16/06/2019.

SNOW, Jabob. **Amazon's face recognition falsely matched 28 members of congress with mugshots**. Disponível em: < https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>. Acesso em 20/06/2019.

SUNSTEIN, Cass R. **After the Rights Revolution**: Reconceiving the Regulatory State. Harvard University Press, 1993.

SUNSTEIN, Cass R.. O mundo real da análise de custo-benefício: 36 questões (e quase tantas respostas quanto). **Revista de Direito Administrativo**, Rio de Janeiro, v. 266, p. 13-47, mai. 2014

THALER, Richard H. SUNSTEIN, Cass R. **Nudge**: improving decisions about health, wealth, and happiness. Michigan: Caravan. 2008.

VIANNA, Eduardo Araujo Bruzzi. **Regulação das fintechs e sandboxes regulatórias**. Dissertação de mestrado - Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. 168 f. 2019.

WILLIAMS, Betsy Anne; BROOKS, Catherine F.; SHMARGAD, Yotam. How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications. Penn State University Press. **Journal of Information Policy**, Vol. 8, pp. 78-115, 2018.

WOOD, Daniel Ricardo Augusto; KNOERR, Fernando Gustavo. Direitos Transgeracionais do Estado e o Direito Internacional: Balanço Social. **Revista Jurídica**, [S.l.], v. 3, n. 32, p. 404-421, dez. 2013. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/694>. Acesso em: 20 jul. 2019.

WU, Tim. Agency threats. **Duke Law Journal**, Vol. 60, p. 1841-1857, 2011.