MARÇO, 2021

Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública:

Tecnologia de Reconhecimento Facial

AUTORAS
Alessandra Lemos
Elora Fernandes
Juliana Medeiros
Paula Guedes
Priscilla Silva

EDITORAÇÃO E REVISÃO
Celina Bottino
Christian Perrone

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

SUMÁRIO

RESUMO EXECUTIVO

O presente relatório tem como objetivo a análise no tocante da tecnologia de rec onhecimento facial do anteprojeto de **Lei de Proteção de Dados para segurança pública e persecução penal** — conhecido como "LGPD Penal" —, entregue no dia 05 de novembro de 2020 à Câmara dos Deputados pelo presidente da Comissão de Juristas, o Ministro do Superior Tribunal de Justiça (STJ), Néfi Cordeiro. Apesar de o anteprojeto de Lei ser, a princípio, tecnologicamente neutro,[1] propondo, como âmbito de aplicação, o tratamento de dados pessoais pelo setor público para fins de segurança pública e persecução criminal, optou-se por focar, no presente documento, apenas quanto as tecnologias de reconhecimento facial. A opção se deu em razão dos altos riscos vinculados a essas ferramentas, o que demanda uma análise mais pormenorizada e específica.

Inicialmente, diante da exclusão das atividades de segurança pública, investigação e persecução penal do escopo de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), prevista no art. 4º, inciso III, alíneas "a" e "d", ressalta-se a importância do referido anteprojeto de Lei e sua consequente tramitação no Congresso Nacional como um ponto de partida para a regulamentação do uso de dados pessoais para estes fins. A iniciativa legislativa é essencial para a garantia de direitos fundamentais dos cidadãos, evitando que a atuação estatal extrapole limites razoáveis, mas sem impedir os avanços positivos que podem advir do uso de novas tecnologias.

Nos últimos anos, houve um crescimento de projetos de lei voltados para a segurança pública, o que desperta um alerta em relação a um possível vigilantismo estatal frente a seus cidadãos.[2] Em paralelo a estas iniciativas, depara-se com o uso, cada vez mais frequente, de tecnologias que utilizam dados pessoais para auxiliar no exercício da segurança pública e em atividades de persecução penal pelos diferentes órgãos estatais. O reconhecimento facial, usado para identificação de foragidos e suspeitos, torna-se uma das tecnologias propostas com maior frequência para atingir fins de segurança pública.

A utilização dessas novas ferramentas tecnológicas pelos órgãos públicos, especialmente em um cenário de ausência de legislação específica aplicável, pode criar riscos significativos para os direitos fundamentais dos cidadãos, como privacidade, liberdades de expressão e associação, além da presunção de inocência. Monitoramento em tempo real por câmeras de segurança, identificações equivocadas (falsos positivos)[3], além de decisões automatizadas e enviesadas (discriminatórias e geradoras de exclusão) são apenas algumas das problemáticas existentes.

1. DO ESCOPO DO ANTEPROJETO, QUE ABARCA APENAS O TRATAMENTO DE DADOS PARA FINS DE SEGURANÇA PÚBLICA E ATIVIDADES DE INVESTIGAÇÃO E PERSECUÇÃO PENAL.

O art. 4º, da Lei Geral de Proteção de Dados (LGPD - Lei 13.709/2018) apresenta algumas exceções, para as quais a lei não se aplicaria. Seu inciso III exclui do escopo da Lei os tratamentos de dados utilizados exclusivamente para fins de "a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais". Percebe-se, portanto, que o anteprojeto aqui em discussão regula somente as alíneas "a" e "d", deixando para regulação posterior os tratamentos de dados para defesa nacional e segurança do Estado.

Considera-se que essa escolha foi acertada. Além de o ato de criação da comissão[4] restringir seu trabalho à regulação das alíneas "a" e "d", entende-se que o balanceamento entre interesses coletivos e individuais difere bastante quando se trata de defesa nacional e segurança do Estado. Nesse sentido, abarcar todas alíneas do art. 4º, III, em uma mesma lei poderia prejudicar a intenção deste anteprojeto de ser uma lei geral — se obrigando a apresentar diversas exceções — e impedir um debate público de qualidade, devido às variadas finalidades.

Isso significa, porém, que haveria ainda uma lacuna no ordenamento jurídico brasileiro, no que tange ao tratamento de dados pessoais no âmbito das alíneas "b" e "c". Essa lacuna demandaria a criação de regulação o mais brevemente possível, a fim de proteger de forma adequada os direitos dos titulares de dados individual e coletivamente. Deve-se destacar, ainda, que podem ocorrer situações (i) nas quais há uma zona cinzenta entre essas diferentes finalidades de tratamento de dados; e (ii) nas quais pode haver a reutilização de dados para finalidades distintas.[5]

A título de exemplo, consideremos os sistemas de reconhecimento facial da Receita Federal do Brasil instalados nos aeroportos brasileiros. Nessa situação, podemos vislumbrar o uso de reconhecimento facial para três tipos de finalidades: (i) segurança privada, a partir da facilitação do processo de identificação de pessoas no embarque e desembarque (ii) segurança pública, considerando que o sistema é interligado à base de dados do Departamento de Polícia Federal, situação em que se pode evitar que pessoas com mandado de prisão em aberto fujam do estado ou país e (iii) segurança nacional, através do monitoramento de pessoas suspeitas que estão sendo investigadas por serviços de inteligência. A situação em tela gera, inclusive, potencial sobreposição ou confusão de competência, como se verá no tópico a seguir.

2. DEFINIÇÃO DO CONSELHO NACIONAL DE JUSTIÇA (CNJ), NO ART. 61 DO ANTEPROJETO, COMO AUTORIDADE COMPETENTE PARA SUPERVISÃO E MONITORAMENTO, SEM QUAISQUER MENÇÕES À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD).

A opção da comissão de juristas pelo CNJ como autoridade competente no âmbito da LGPD Penal tem como objetivo garantir uma independência necessária para a proteção do cidadão e a colaboração internacional, concentrando os poderes de supervisão em um órgão fora da estrutura do Executivo.

Na medida em que o CNJ não possui, até então, subórgão específico competente para analisar questões de regulação de dados, a lei garante a autonomia e expertise técnicas do órgão com a criação da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) dentro da própria estrutura do CNJ.

Ademais, a escolha do CNJ como Autoridade Competente reforça as críticas direcionadas à opção legislativa da LGPD em subordinar a ANPD à Presidência da República,[6] o que poderia impactar na autonomia e independência do órgão no exercício de suas funções, especialmente em um contexto tão sensível como o tratamento de dados pessoais para fins de segurança pública e investigações criminais.

Todavia, a não menção da ANPD ao longo do anteprojeto pode gerar dúvidas acerca de competências possivelmente concorrentes entre as duas autoridades e de como elas poderão atuar em conjunto. Isso se reforça ao se considerar o presente momento, em que a ANDP inicia seu processo de constituição e elaboração de diretrizes que irão nortear sua atuação de forma mais detalhada.

Sem a condução estratégica da ANPD e CNJ, as múltiplas interpretações de esferas públicas tenderão a causar insegurança jurídica e muitas ações judiciais, que poderiam ser evitadas — em boa parte dos casos — por instruções e orientações prévias de delimitação, acordos de competência e atuação coordenada.

Ressalta-se que o supramencionado art. 4º, inciso III, §3º, da LGPD estabelece que "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo — dentre as quais: segurança pública e atividades de investigação e repressão de infrações penais — e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.". Ao mesmo tempo, a "LGPD Penal" atribui exclusivamente a atuação do CNJ em segurança pública e defesa nacional sem, contudo, modificar expressamente a redação da LGPD, gerando uma possível situação de insegurança jurídica a respeito da atuação da ANPD nas matérias.

Retomando o exemplo do monitoramento em aeroportos, em que há possível sobreposição ou interseção de requisitos para o tratamento de dados, a atuação do CNJ e da ANPD poderia ser melhor delimitada no projeto de lei ou ser objeto de alguma forma de coordenação.

Por fim, resta a questão da utilização de dados para a investigação por parte do Ministério Público.[7] A atuação deste não necessariamente se enquadra na competência do CNJ, tendo o Conselho Nacional do Ministério Público (CNMP) certo grau de autonomia, gerando outra potencial fonte de tensão que deveria ser melhor explorada pela lei.

3. DA VEDAÇÃO DO USO DE FERRAMENTAS DE MONITORAMENTO E RECONHECIMENTO FACIAL DE FORMA MASSIVA, DE FORMA INDETERMINADA E SEM PRÉVIA AUTORIZAÇÃO JUDICIAL

O Capítulo VII, do Anteprojeto da "LGPD Penal", traz disposições gerais sobre o uso de tecnologias de monitoramento e o tratamento de dados de elevado risco. A escolha de tratar da temática no âmbito desta proposta legislativa reforça a importância do direito à proteção de dados na discussão a respeito do uso de tecnologias, como a do reconhecimento facial, na segurança pública.

O artigo 5º, inciso XXIII, do anteprojeto define tecnologias de monitoramento como sendo equipamentos, programas de computador ou sistema informático que possam ser usados para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio.

Para coibir o vigilantismo estatal e preservar o direito à proteção de dados na seara da segurança pública, o Anteprojeto de "LGPD Penal" trouxe duas proibições ao uso de tecnologias de monitoramento. A primeira vedação se encontra no artigo 42, caput, em que se condiciona a possibilidade de uso destas tecnologias à existência de autorização legal específica prévia. Esta autorização deve ser precedida de relatório de impacto de vigilância (ou análise de impacto regulatório, como referido pelo §2º, do mesmo dispositivo) e estabelecer garantias aos direitos dos titulares.

A segunda proibição, por sua vez, está disposta no artigo 43, o qual veda "a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial".

Assim, muito embora o anteprojeto tenha optado por relegar a outro processo legislativo a autorização ou proibição de tecnologias de monitoramento, optou por, desde já, trazer restrições contextuais ao seu uso no artigo 43. Ainda que neste dispositivo não tenham sido mencionadas especificamente as tecnologias de reconhecimento facial, ele parece ser direcionado particularmente para a utilização de biometria, uma vez que faz referência a tecnologias acrescidas

de técnicas de identificação. Por esta razão, importa ressaltar brevemente como esta vedação afeta o uso de tecnologias de reconhecimento facial na área de segurança pública.

Os sistemas de reconhecimento facial podem ser utilizados para diversas finalidades, sendo as principais a verificação e a identificação. No que tange à verificação, o reconhecimento tem por finalidade verificar a probabilidade de a pessoa presente na imagem recebida ser a mesma daquela presente nas imagens de um banco de dados. O sistema faz uma análise de um para um e visa responder à pergunta: "você é quem diz ser?". Pode-se citar como exemplo a verificação de identidade realizada em fronteiras, a partir do passaporte. A imagem captada do indivíduo naquele momento é comparada à imagem do mesmo indivíduo presente no banco de dados. Deve-se destacar que, neste caso, o indivíduo tem o conhecimento de que o reconhecimento facial está ocorrendo.

Por outro lado, quando se trata de identificação, o sistema de reconhecimento facial é utilizado para escanear faces e procura responder outros tipos de perguntas, como: "quem é a pessoa que cometeu determinado ato"; ou "onde está uma determinada pessoa que se procura". Em resumo, busca-se saber quem é determinada pessoa, em uma análise de um para muitos (uma imagem coletada em comparação com diversas outras do banco de dados). Quando utilizado em espaços amplos, onde transeuntes estarão presentes, como em uma determinada rua ou em um local de protesto, as imagens captadas nesse espaço serão comparadas com as de um banco de dados — por exemplo, o banco de imagens de pessoas procuradas pela polícia ou do registro civil. Um dos grandes problemas do uso do reconhecimento facial para a identificação é a possibilidade de indivíduos terem suas faces analisadas por tecnologias de reconhecimento facial sem a sua ciência e/ou consentimento pelo fato de esta coleta e tratamento de dados biométricos poder ser feito à distância e inclusive em momento posterior ao que as imagens foram coletadas.[8]

Ao limitar os cenários em que a tecnologia de reconhecimento facial pode ser usada para realizar tarefas de identificação, o anteprojeto de lei acerta e mitiga os riscos de violação de diversos direitos como a privacidade, a liberdade de expressão e a liberdade de associação.

Nota-se que pode também existir um impacto para a livre expressão e desenvolvimento da personalidade. A ciência da observação tende a impactar no comportamento livre dos indivíduos, o que leva a que o uso da tecnologia, particularmente em espaços públicos, sem as devidas salvaguardas e garantias, possa ter um um efeito inibidor ou resfriador.[9] Essa situação é mais delicada em contextos de manifestações e protestos, uma vez que nesses casos se engaja também a participação cívica e democrática.[10] Portanto, deve existir um cuidado no desenho e na implementação de tecnologias dessa categoria para que haja o uso responsável e de acordo às salvaguardas e garantias necessárias.

Somado a isso, o atual estado da tecnologia de reconhecimento facial pode reforçar discriminações enraizadas na sociedade, especialmente contra minorias e grupos marginalizados.[11] Um estudo do National Institute of Standars and Technology (NIST)[12] de 2019 concluiu que a maioria dos sistemas de reconhecimento facial existentes no mundo tinha de 10 a 100 vezes mais chances de identificar rostos negros ou asiáticos de forma imprecisa em comparação com o rosto de homens brancos.[13] Tais resultados são agravados quando a análise é feita em faces de mulheres, o que acentua a tendência de essas tecnologias reproduzirem vieses raciais e de gênero.[14]

O problema de enviesamento das aplicações de reconhecimento facial torna-se ainda mais grave quando deslocamos a discussão para o contexto do Sul Global. No caso brasileiro, não há indústrias nacionais relevantes que desenvolvam essa tecnologia, o que torna o país consumidor de sistemas de reconhecimento facial de empresas estrangeiras, vindas de realidades e contextos sociais distintos, a exemplo da Europa, Estados Unidos e Ásia. Essa diferença contextual potencialmente reforça as chances de reprodução de discriminações por meio de resultados enviesados e imprecisos.[15]

Entretanto, apesar de o anteprojeto ter acertado ao escolher limitar o uso de tecnologias de reconhecimento facial para a tarefa de identificação, a atual redação do artigo 43 abre margem para dúvidas a respeito de quais situações estão permitidas ou proibidas por este dispositivo.

Para ilustrar as dúvidas que podem ser suscitadas, indica-se o seguinte exemplo. Em estados brasileiros como o Rio de Janeiro[16], a tecnologia de reconhecimento facial tem sido testada em locais públicos de grande movimento de transeuntes com o intuito de identificar pessoas em desfavor das quais há mandados de prisão em aberto. Em casos como este, é possível afirmar que está sendo feito o uso de tecnologia acrescida de identificação de pessoas indeterminadas em tempo real e de forma contínua — o banco de dados integral está constantemente sendo buscado. A princípio, esta atuação estaria vedada pelo teor do artigo 43. Esta vedação, no entanto, não é absoluta. O próprio anteprojeto prevê uma exceção a essa vedação ao autorizar esta modalidade de uso quando ela estiver conectada a uma atividade de persecução penal individualizada autorizada por lei e decisão judicial. Esta exceção permite o uso de reconhecimento facial para identificar uma pessoa em desfavor da qual foi expedido um mandado de prisão. No entanto, não fica claro se essa permissão autoriza a busca contínua e simultânea de várias pessoas com mandados de prisão em aberto. Isto é, o uso de tecnologias de reconhecimento facial com uma base de dados composta por faces de centenas pessoas com mandados de prisão expedidos individualmente contra cada uma delas poderia ser considerado atividade de persecução penal individualizada? A busca por mais de uma pessoa simultaneamente afastaria o caráter individual do uso?

Outro ponto da atual redação do artigo 43 que pode gerar controvérsia é a definição de uso contínuo de tecnologia de identificação. Em nenhum momento é definido no anteprojeto o que seria "uso de forma contínua". Inexiste a especificação de um marco temporal inicial e final ou da periodicidade que permitisse a identificação do uso contínuo. Uma definição clara do que é "uso de forma contínua" se faz necessária para evitar usos abusivos da tecnologia que importem em graves violações aos direitos fundamentais dos cidadãos brasileiros.

Ao não estabelecer o que vem a ser "uso de forma contínua", o anteprojeto acaba por abrir margem para que outras leis, federais ou estaduais, e o judiciário definam o que vai constituir esta forma de uso. Isso pode gerar disparidades na utilização de reconhecimento facial no território brasileiro, o que levará à proteção distinta dos direitos dos cidadãos, incluído o direito à proteção de dados.

A título exemplificativo, tem-se a Lei 6.782/2020, do Distrito Federal, que dispõe sobre o uso de tecnologia de reconhecimento facial (TRF) na segurança pública e dá outras providências. Em seu artigo 2º, inciso II, ela define vigilância contínua como "a utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem, durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos". Outras legislações estaduais poderiam seguir os seus passos e trazerem uma definição de uso de forma contínua parecida ou distinta da adotada nesta lei.

Importante ressaltar que, segundo o princípio da legalidade, os órgãos estatais só podem fazer aquilo que está autorizado ou previsto em lei. Na seara penal, este princípio assume uma especial importância face aos direitos em jogo (*e.g.* presunção de inocência e direito de ir e vir) e a natureza das sanções (penas privativas de liberdade e penas restritivas de direitos). A gravidade de uma atuação policial ilegal ou abusiva pode ter consequências terríveis e, por isso, ela deve estar regulamentada de forma precisa, evitando ambiguidades ou obscuridades.

O grande desafio do anteprojeto de "LGPD Penal" é estabelecer um equilíbrio entre a proteção de direitos individuais — como o direito de ir e vir, direito à proteção de dados, privacidade e liberdade de expressão — e direitos coletivos, como o direito à segurança pública. Ao não trazer definições claras em um dispositivo tão importante quanto o artigo 43, o anteprojeto se afasta deste ideal de equilíbrio e pode abrir brechas para o uso abusivo da tecnologia de reconhecimento facial e para violações de direitos fundamentais.

CONCLUSÃO

Centrada no ideal de autodeterminação informativa, autonomia e controle do cidadão de seus dados, a LGPD trouxe um novo paradigma que passou a fundamentar a abordagem do direito à privacidade. Esse novo ambiente regulatório busca harmonizar a proteção dos direitos dos indivíduos e a provisão de segurança jurídica nas relações permeadas pelo tratamento de dados pessoais.

Numa conjuntura em que se passa a monitorar dados sobre todos os aspectos das vidas das pessoas, fica claro que a hipervigilância pode vir a constituir uma ameaça a direitos e liberdades fundamentais como à privacidade, liberdade de expressão, igualdade, liberdade de associação, dentre outros. Desta forma, essa enorme expansão da vigilância constitui, em última análise, uma ameaça ao próprio Estado Democrático de Direito.

Nesse sentido, o texto da "LGPD Penal" é um bom ponto de partida para o debate fundamental sobre a relevância de se regular uma participação mais ativa e transparente no controle e acesso às informações dos titulares aos seus dados, em especial no caso de dados sensíveis e biométricos, como o uso de tecnologias de reconhecimento facial. O anteprojeto estabelece requisitos e limitações aos usos admissíveis dos dados pessoais por parte das autoridades, cria obrigações de transparência a serem respeitadas pelos controladores de dados e prevê a elaboração de relatórios de impacto na ocasião do tratamento de dados pessoais sensíveis.

A Seção IV do anteprojeto traz algumas limitações ao tratamento de dados, reforçando a necessidade da minimização do tratamento de dados pessoais. De acordo com o anteprojeto, o agente de tratamento deve descartar aqueles dados que se mostrem irrelevantes e excessivos à finalidade da operação. Contudo, no que se refere a tratamento de dados pessoais para fins de segurança pública, traçar um limite do que seria necessário ou relevante para a finalidade da operação pode ser bastante complicado ao se levar em consideração os aspectos práticos do uso da tecnologia.

Soma-se a isso o fato de que o objeto do reconhecimento facial é a face humana e, ao contrário de outros dados sensíveis e biométricos, como a íris ocular e a digital, ela está exposta a todo tempo, o que torna ainda mais complexo a delimitação de seu uso.

Através do uso de câmeras equipadas com reconhecimento facial nas ruas são coletadas as imagens de muitas pessoas que não estão sendo investigadas por crimes, em desfavor das quais não há um mandado de prisão expedido e que não estão prestes a cometer crimes. Assim, a delimitação do que é relevante no tratamento de dados pessoais para fins de segurança pública deveria ser expressamente previsto na lei, pois, a contrário senso, permanecem questionamentos como: não havendo correspondência exata com os dados dos indivíduos e a base de dados já existente, todas as imagens gravadas devem ser excluídas?

As imagens coletadas devem ser gravadas e guardadas por algum tempo para se verificar se houve a prática de crimes? Por quanto tempo? Qual o limite da relevância dos dados pessoais coletados?

O anteprojeto prevê ainda a necessidade dos sistemas responsáveis por decisões automatizadas serem auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia. Cabe mencionar que, para os fins de não discriminação, o anteprojeto deveria levar em conta que as taxas gerais de alta acurácia caem significativamente quando se analisa grupos específicos da população como, por exemplo, mulheres negras. Assim, por mais que o anteprojeto tenha o objetivo de dar garantias aos indivíduos a respeito da necessidade e acurácia da tecnologia de reconhecimento facial, ao criar três níveis de proteção para sua implementação,[17] é necessária uma maior conceituação dos termos e procedimentos.[18]

Como vimos, se por um lado o anteprojeto parece seguir no caminho de viabilizar proteções dos direitos fundamentais, um ponto que desperta atenção e que em alguma medida causa preocupação, se refere às tentativas de expandir os poderes policiais do Estado. Nesse sentido, merece atenção especial o art. 43 do anteprojeto que, embora vede a utilização de tecnologia de vigilância em massa, a questão que se impõe é sobre qual seria a definição de atividade de persecução penal individualizada e, mais ainda, pelo que se pode analisar das previsões da lei, o uso individualizado não parece sustentar os fins almejados de segurança pública. Assim, apesar dos dispositivos do anteprojeto caminharem na intenção de garantir os direitos aos titulares, as propostas como são dispostas, isto é, sem considerar os aspectos práticos, acabam por não sustentar essa garantia de direitos.

Considerando ainda as importantes previsões aos princípios que norteiam a LGPD – dispostos nos artigos 2° e 6° –, devemos, na análise de impacto do anteprojeto, partir do reconhecimento desses direitos, avançando e não retrocedendo em sua garantia. Ainda que o intuito do anteprojeto pareça seguir no sentido de disciplinar tais princípios, as diretrizes e as linhas mestras da proteção de dados no referido âmbito de segurança pública, não se pode olvidar a relevância de uma previsão clara, levando em consideração os aspectos práticos do uso da tecnologia, dos princípios que norteiam a atividade interpretativa e disciplinam o tratamento, uso e coleta de dados, bem como a garantia dos direitos dos titulares dos dados às informações acerca do tratamento.

Diante do exposto, o ITS reconhece a importância do tema e congratula a iniciativa, mas ressalta a importância do debate multissetorial - um debate tão necessário diante da crescente utilização de dados pessoais por agentes públicos para fins de segurança pública, investigação e persecução penal, especialmente auxiliada por ferramentas tecnológicas que tratam dados pessoais sensíveis, como é o caso do reconhecimento facial.

NOTAS FINAIS

1. O conceito de "tecnologicamente neutro" surgiu no campo da regulação estatal, a partir de regulações imparciais que não discriminam ou dão tratamento mais favorável para determinadas ferramentas, em detrimento de outras. Nesse sentido, legislações devem definir objetivos a serem alcançados de forma ampla, de forma a não impor ou discriminar, a favor ou contra, o uso de determinado tipo de tecnologia para alcançar esses objetivos; ALI, Rajab. Technological Neutrality. Lex Electronica, Revenue du Centre de Recherche en Droit Public, vol. 14, nº 2, 2009. Disponível em: https://www.lex-electronica.org/files/sites/103/14-2_ali.pdf.

2. Coalizão de Direitos na Rede. Alerta! Novas propostas de lei visam aumentar o vigilantismo no Brasil. Disponível em: https://direitosnarede.org.br/2019/11/18/novas-propostas-lei-vigilantismo-brasil/

3. Falsos positivos revelam situações em que a imagem facial analisada é inequivocamente relacionada com outra, presente em um determinado banco de dados. No contexto de segurança pública, isso pode significar um indivíduo falsamente identificado dentro de uma lista de suspeitos do governo, impactando negativamente seus direitos e gerando constrangimentos desnecessários. Mundialmente, já existem casos de reconhecimento facial incorreto, o que é agravado em contexto de segurança pública, a exemplo das prisões equivocadas ocorridas em 2019 no Rio de Janeiro e em 2020 no estado de Michigan, nos Estados Unidos.

Cf.: G1. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. Rio de Janeiro, 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em 02 de março de 2021; BURTON-HARRIS, Victoria; MAYOR, Philip. Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart. American Civil Liberties Union (ACLU), 24 jun. 2020. Disponível em: https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/. Acesso em 02 de março de 2021; European Union Agency for Fundamental Rights (FRA). Facial recognition technology: fundamental rights considerations in the context of law enforcement. FRA Focus.

4. O ato de criação da comissão de juristas pelo presidente da Câmara dos Deputados, Rodrigo Maia, pode ser visualizado em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/conheca-a-comissao/criacao-e-constituicao/ato-de-criacao

5. Exemplo disso é a atuação de Estados europeus que frequentemente tratavam dados para fins de combater o terrorismo, mas que acabavam sendo utilizados para outras finalidades, o que foi julgado pelo Tribunal de Justiça da União Europeia. Mais informações em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf

6. As propostas de textos que antecederam o veto parcial do presidente à LGPD eram no sentido de que a Autoridade Nacional de Proteção de Dados seria um órgão independente com natureza de autarquia federal. No entanto, a partir do veto presidencial, a Lei nº 13.853, de 2019, instituiu a ANPD como órgão da administração pública federal, integrante da Presidência da República. Veja mais sobre análises da natureza da Autoridade Nacional de Proteção de Dados aqui: TEFFÉ, Chiara Spadaccini de; MANGETH, Ana Lara. Lei de Dados Pessoais precisa de uma Autoridade independente, 2018. Disponível em: https://feed.itsrio.org/lei-de-dados-pessoais-precisa-de-uma-autoridade-independente-34137c7bbc64

7. A Portaria CNMP-PRESI nº 55/2020 criou o Grupo de Trabalho formado por 19 integrantes de todos os ramos do Ministério Público e coordenado pelo conselheiro do CNMP. O grupo é responsável por elaborar proposta normativa para o Ministério Público Brasileiro quanto à regulamentação da Lei Geral de Proteção de Dados Pessoais. Ver mais em: CNMP. CNMP avança nos estudos para regulamentar a proteção de dados pessoais e a conformidade com a LGPD no âmbito do MP brasileiro, 2020. Disponível em: https://www.cnmp.mp.br/portal/todas-as-noticias/13707-cnmp-avanca-nos-estudos-para-regulamentar-a-protecao-de-dados-pessoais-e-a-conformidade-com-a-lgpd-no-ambito-do-mp-brasileiro

8. Um caso exemplificativo do uso de tecnologias de reconhecimento facial sem ciência dos monitorados foi reportado que ocorreu em Washington DC. Manifestantes que participaram de um protesto relacionado ao movimento Black Lives Matter teriam sido identificados pela polícia de Washington através do uso de tecnologias de reconhecimento facial. A polícia, que queria identificar o manifestante que havia agredido um policial, encontrou um vídeo do protesto no Twitter, selecionou uma imagem em que aparecia o rosto do manifestante responsável pela agressão e utilizou a tecnologia para descobrir a identidade do suposto agressor. Através da tecnologia chegaram ao nome do acusado de agressão. (HAMILTON, Isobel Asher. Police used facial recognition tech on a Twitter video to find and charge a Lafayette Square protester with assault. 03 de novembro de 2020. Disponível em: <https://www.businessinsider.com/police-facial-recognition-twitter-video-protester-lafayette-square-assault-2020-11#:~:text=Police%20used%20facial%20recognition%20tech,Lafayette%-20Square%20protester%20with%20assault&text=Court%20documents%20spotted%20by%20the,at%20Lafayette%20Square%20in%20June>. Acesso em: 02 de março de 2021.)

9. European Union Agency for Fundamental Rights (FRA). Facial recognition technology: fundamental rights considerations in the context of law enforcement. FRA Focus.

10. European Union Agency for Fundamental Rights (FRA). Facial recognition technology: fundamental rights considerations in the context of law enforcement. FRA Focus. Nesse contexto, relatório da Anistia Internacional revelou como o medo generalizado da vigilância torna quase impossível que ativistas de direitos humanos e políticos de oposição realizem certas atividades, como envio de e-mails ou organização de protestos pacíficos, o que vem ocorrendo em locais como Hong-Kong e Varsóvia. Por exemplo, em janeiro de 2017, a polícia de Varsóvia, na Polônia, publicou documento na tentativa de identificar manifestantes capturados pelas câmeras de vigilância do local de protesto (Anistia Internacional. New Technologies and their impact on the promotion and protection of human rights in the context of assemblies. Submission to the United Nations High Commissioner for Human Rights (out. 2019). Disponível em: https://www.amnesty.org/download/Documents/IOR4012842019ENGLISH.pdf).

11. Vide nota de rodapé nº 3.

12. GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Standards and Technology (NIST), NISTIR 8280, dez. 2019. Disponível em: https://nvlpubs.nist.gov/ nistpubs/ir/2019/NIST.IR.8280.pdf.

13. GUEDES, Paula. Discriminação tecnológica: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes. Trabalho final do IV Grupo de Pesquisa do Instituto de Tecnologia e Sociedade do Rio de Janeiro. Disponível em: https://itsrio.org/wp-content/uploads/2020/10/Discrimina%C3%A7%C3%A3o-tecnol%C3%B3gica_Paula_Guedes.pdf. p.3.

14. BRUEGGE, Richard W. Vorder; BURGE, Mark J; JJAIN, Anil K; KLARE, Brendan F.; KLONTZ, Joshua C. Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security. Disponível em: https://www.openbiometrics.org/ publications/klare2012demographics.pdf.

15. DA SILVA, Paula Guedes Fernandes. Sorria você está sendo reconhecido: o reconhecimento facial como violador de direitos humanos?. Médium do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio). Publicado em 26 ago. 2020. Disponível em: https://feed.itsrio.org/sorria-você-está-sendo-reconhecido-o-reconhecimento-facial-como-violador-de-direitos-humanos-4113914441d3.

16. PLATONOW, Vladimir. Reconhecimento facial leva a três prisões no Rio de Janeiro. Agência Brasil. Rio de Janeiro, 02 de setembro de 2019. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/reconhecimento-facial-leva-tres-prisoes-no-rio-de-janeiro>. Acesso em: 11 de dezembro de 2020.

17. Os três tópicos de proteção para tecnologias de monitoramento seriam: exigência de legislação específica precedida de uma análise de impacto regulatório (1º nível), previsão de uma série de direitos e garantias de uso da tecnologia na legislação a ser criada (2º nível) e, depois da aprovação dessa lei, necessário o relatório de impacto de uso (3º nível).

18. DORA, Daniela; ABREU, Jacqueline; MENDES, Laura Schertel. Live DPBR - LGPD Penal: proteção de dados pessoais, segurança pública e investigações, 2020. Disponível: https://www.youtube.com/watch?v=ZCnvMtPtDho&t=3271s.

SOBRE AS AUTORAS

Alessandra Lemos
Advogada. Mestra em Criminologia e Justiça Criminal pela Universidade de Oxford. Mestra e Bacharela em Direito pela Universidade Federal do Paraná. Bolsista FCDO - Chevening entre 2017-2018. Foi Fellow no ITS – Instituto de Tecnologia e Sociedade através do programa UK-Brazil Data Protection Fellowship realizado em 2020.

Elora Fernandes
Doutoranda em Direito Civil na Universidade do Estado do Rio de Janeiro (UERJ). Mestra em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF) e graduada em Direito pela mesma instituição, com período de intercâmbio acadêmico na Universidad de Salamanca (Espanha). É alumna do Deutscher Akademischer Austauschdienst (DAAD) e faz parte do corpo editorial da Revista de Estudos Empíricos em Direito (REED). É integrante do IV Grupo de Pesquisa do ITS, na área de Direito e Tecnologia.

Juliana Medeiros
Advogada. Mestranda em Teoria do Estado e Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), pós-graduanda em Direito Digital pelo Instituto New Law e graduada em Direito com láurea acadêmica magna cum laude pela faculdade IBMEC. Membro do Grupo de Pesquisa de Direito e Tecnologia do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio), certificada pela Harvard Law School em Direitos Autorais no curso Copyrightx em parceria com o ITS-Rio e a Universidade Estadual do Rio de Janeiro (UERJ) e autora dos livros “O fenômeno das fanfictions e o direito autoral brasileiro” e “Manual do Estudante de Direito”.

Paula Guedes
Advogada; mestranda em Direito Internacional e Europeu pela Universidade Católica Portuguesa – Escola do Porto (UCP Porto); pós-graduanda em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) em parceria com a Universidade Estadual do Rio de Janeiro (UERJ); participante do grupo de pesquisa em Direito e Tecnologia do ITS-Rio; pós-graduada em Direito Digital pela Fundação Escola Superior do Ministério Público (FMP); e formada pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).

Priscilla Silva
Doutoranda e Mestre em Teoria do Estado e Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio); pós graduada em Direito Público e Privado pela Fundação Escola Superior do Ministério Público do Rio de Janeiro (FEMPERJ); Graduada em Direito pela PUC Rio; Fellow em Direito e Religião na Universidade de Oxford; pesquisadora em Direito e Novas Tecnologias do Institutito de Tecnologia e Sociedade (ITS Rio) e membro do grupo de pesquisa em Direito e Novas Tecnologias DROIT.

EDITORAÇÃO:

Celina Bottino
Mestre em direitos humanos pela Universidade de Harvard. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Diretora de projetos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Christian Perrone
Pesquisador Fulbright (Universidade de Georgetown, EUA). Doutorando em Direito Internacional (UERJ); Mestre em Direito Internacional (L.L.M/Universidade de Cambridge, Reino Unido). Ex-Secretário da Comissão Jurídica Interamericana da OEA. Coordenador da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Esse relatório contou com o generoso
apoio financeiro do Reino Unido através
de programa *Digital Access*

GREAT *for* PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org