Ao Senhor,

Waldemar Gonçalves Ortunho Júnior
Diretor-Presidente
Autoridade Nacional de Proteção de Dados Pessoais

Assunto: Licitude da Solução Automatizada de Identificação Biométrica da Polícia Federal

Estimado Senhor Diretor-Presidente da Autoridade Nacional de Proteção de Dados Pessoais,

A Coalizão Direitos na Rede, entidade que congrega 45 entidades de direitos digitais no Brasil, fundada em 2016, em conjunto com a Comissão de Proteção de Dados e Privacidade da Seccional do Rio de Janeiro da Ordem dos Advogados do Brasil (OAB-RJ) e as demais entidades que assinam o presente ofício, vem, com fulcro na Estrutura Regimental da Autoridade Nacional de Proteção de Dados Pessoais (Decreto 10.474/2020) e na Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), expor e requerer o que segue.

I - Dos Fatos

Em 06 de julho de 2021, foi anunciado pelo Ministério da Justiça e Segurança Pública a Solução Automatizada de Identificação Biométrica. O sistema tem capacidade de coletar dados de mais de 50 milhões de brasileiros em 48 meses e vai proporcionar a unificação dos dados das Secretarias de Segurança Pública com vistas a permitir uma maior agilidade na análise de vestígios papiloscópicos revelados em cenas de crimes e será disponibilizada em todas as unidades da polícia federal do país. A solução prevê a possibilidade de completa integração com outros modelos de identificação biométrica como íris e voz.

Conforme relatado pela jornalista Paula Soprana da Folha de São Paulo, "chamado de Abis (sigla para Solução Automatizada de Identificação Biométrica), o programa poderá identificar pessoas a partir do cruzamento de registros provenientes de reconhecimento facial e de impressão digital. Trata-se de uma evolução do Afis (Sistema Automatizado de Identificação de Impressões Digitais), usado há 16 anos pela PF" (ver "PF compra sistema que cruzará dados biométricos de 50 milhões de brasileiros"). Segundo a Folha de São Paulo, o Abis vai "proporcionar a unificação de dados" de secretarias de segurança pública

estaduais e fornecer às polícias judiciárias acesso seguro e eficiente ao que chama de base biométrica nacional.

Diante do anúncio da solução, entidades civis especializadas reagiram com preocupações sobre o direito fundamental à proteção de dados pessoais. A Associação Data Privacy Brasil de Pesquisa, em comunicado à imprensa de 07 de julho de 2021, afirmou que "a Solução Automatizada potencializa o compartilhamento de informações sem uma demonstração prévia de salvaguardas e procedimentos de compatibilização de finalidades de bases de origens diversas. Adicionalmente, a proliferação de bases de dados dedicadas ao armazenamento e coleta de dados pessoais para fins de persecução penal preocupa em um país que ainda não estabeleceu as salvaguardas necessárias para os titulares em atividades de tratamento de dados pessoais para fins de segurança pública". A entidade também afirmou que a solução pode levar a uma ampliação das operações da Diretoria de Inteligência dentro da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública (SEOPI), confundindo tratamentos orientados à segurança pública, tratamentos orientados à investigação criminal e tratamentos orientados à inteligência, que possuem contextos distintos e condições de legitimidade diversas".

Preocupa, ainda, o viés racial do uso de reconhecimento biométrico na segurança pública. Pesquisa realizada em 2019 pela Rede Observatórios de Segurança mostrou que 90,5% das pessoas presas através deste sistema eram negras. E pesquisa posterior, realizada pelo Condege mostrou que 83% das pessoas em prisão injusta por erro de reconhecimento são pessoas negras. Estudos realizados em diversos países já mostraram que os erros na programação algorítmica afetam pessoas negras e pessoas trans com maior incidência, seja pela ausência de acurácia do algoritmo ou pelo manejo indevido dos sistemas nos órgãos de segurança. Num país com racismo e colonialidade como cerne, este é um problema que não pode ser ignorado.

Diante das repercussões, outros veículos de mídia destacaram preocupações da sociedade civil. Em matéria assinada em 07 de julho por Rafael Bucco, Bárbara Simão do InternetLab, organização sem fins lucrativos sediada em São Paulo, argumentou que a Polícia Federal não informa claramente se analisou o impacto da adoção da tecnologia nas vidas de todos os cidadãos brasileiros. Para Simão, "Embora não tenhamos claro que autoridade vai tratar disso, a LGPD dá a prerrogativa à ANPD de exigir relatório de impacto

à proteção de dados. A ANPD poderia exigir um que a PF explicasse o porquê da adoção da tecnologia, qual o impacto para os cidadãos e qual a necessidade para suas operações".

Até o momento não houve qualquer disponibilização de documentação técnica sobre a solução e detalhamentos tornados públicos.

II - Do Direito

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) afirma, em seu artigo primeiro, que a legislação tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao revés da cautela expressada na LGPD, tem-se observado um aumento da opacidade como política de segurança pública governamental, com imposição de sigilo arbitrário e outras medidas de restrição de acesso a informações públicas. A soma de práticas violadoras de direitos humanos se torna ainda mais temerosa quando não há uma definição precisa sobre como tem acontecido o registro, manutenção, uso e compartilhamento de informações pessoais colhidas por reconhecimento biométrico nos diversos locais do país que já operam este sistema.

A lei também tem como fundamento a autodeterminação informativa, concebida como direito básico do cidadão saber como, por que, e para quem seus dados são compartilhados, considerando que a autodeterminação informativa é (i) um direito que se relaciona ao livre desenvolvimento da personalidade e (ii) um direito que se apresenta como pré-condição de participação democrática, na medida em que cria as condições para que cidadãos sejam reconhecidos como co-construtores das decisões relacionadas aos seus dados. Conforme decidido pela Corte Constitucional Alemã em 1983, em caso utilizado como referência normativa para a ADI 6387 do Supremo Tribunal Federal, "uma ordem social e uma ordem jurídica que a sustente, nas quais cidadãos não sabem mais quem, o que, quando, e em que ocasião se sabe sobre eles, não seriam mais compatíveis com o direito de autodeterminação na informação. Quem estiver inseguro sobre se formas de comportamento divergentes são registradas o tempo todo e definitivamente armazenadas, utilizadas ou transmitidas, tentará não chamar a atenção através de tais comportamentos. (...) Isso não prejudicaria apenas as chances de desenvolvimento individual do cidadão, mas também o bem comum, porque a autodeterminação é uma condição funcional elementar para uma

comunidade democrática e livre, fundada na capacidade de ação e participação de seus cidadãos".

A autodeterminação informacional, assim, se configura como um dos pilares do direito à proteção de dados pessoais, este reconhecido como um direito fundamental autônomo pelo Supremo Tribunal Federal na ocasião do julgamento das ações que questionaram a constitucionalidade da Medida Provisória n.º 954/2020.

No caso concreto, evidente que o cidadão não possui conhecimento e participação na decisão sobre como seus dados são reutilizados e compartilhados para finalidades diversas das que havia imaginado. Isso é especialmente problemático na medida em que envolve "dados sensíveis", concebidos juridicamente como dados pessoais "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Conforme explicado pelo pesquisador Pablo Nunes, coordenador executivo do Aqualtunelab, "o sistema adquirido vai ser usado em investigações, com vídeos e fotografias coletados de câmeras de vigilância de portarias, fotos de redes sociais". Segundo Nunes, a tecnologia apresenta diversos problemas no tratamento de dados sensíveis. Estamos diante, portanto, de tratamento de dados com alto potencial discriminatório, dado o caráter unívoco da biometria facial e sua facilidade para instauração de procedimentos de natureza repressiva (como identificação individual e condução da pessoa para delegacia de polícia, em caso de "matching" a partir de modelagem estatística sobre acurácia).

Convém aqui destacar que muito embora a LGPD tenha excetuado, em seu Artigo 4, inciso terceiro, os tratamentos destinados a fins exclusivos de segurança pública, defesa nacional, segurança do Estado e persecução penal de seu escopo de aplicação, ela afirmou a necessidade dessas operações serem disciplinadas por legislação específica, que deverá observar os princípios gerais de proteção de dados, o devido processo legal, o princípio da proporcionalidade e a preservação do interesse público. Isso porque os danos decorrentes das atividades de tratamento realizadas para tais finalidades carregam alguns dos maiores riscos para os direitos e liberdades dos titulares.

Dada a natureza do tratamento e seus potenciais riscos, é função da Autoridade Nacional de Proteção de Dados Pessoais exigir, por parte do Ministério da Justiça e

Segurança Pública, a elaboração de um relatório de impacto à proteção de dados pessoais. O fundamento jurídico desse dever-poder de exigir um relatório de impacto decorre do próprio Artigo 4 da LGPD, em seu parágrafo terceiro. Diz a lei neste ponto: "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais".

O relatório, nos termos do Artigo 5, XVII, é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

III - Dos Pedidos

Considerando a competência da Autoridade Nacional de Proteção de Dados Pessoais para "zelar pela proteção dos dados pessoais" e "solicitar, a qualquer momento, aos órgãos e às entidades do Poder Público que realizam operações de tratamento de dados pessoais, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento da Lei nº 13.709, de 2018", conforme Decreto 10.474/2020, requere-se que a Autoridade Nacional de Proteção de Dados Pessoais:

1. Solicite, nos termos de sua competência legal, que o Ministério da Justiça e Segurança Pública:
    a. Interrompa as operações da Solução Automatizada de Identificação Biométrica e;
    b. Formule um Relatório de Impacto à Proteção de Dados Pessoais; e
    c. Torne o Relatório de Impacto à Proteção de Dados Pessoais público e aberto a comentários da comunidade técnica;

2. Instaure procedimento de avaliação das condições de licitude da Solução Automatizada de Identificação Biométrica do Ministério da Justiça e Segurança Pública, considerando, em especial:

a. A natureza dos dados biométricos utilizados e compatibilização de utilização, de forma secundária, de informações coletadas originalmente para fins diversos;
b. As condições de interoperabilidade dos dados e quais serão os agentes de tratamento de dados que terão acesso a eles;
c. As medidas de mitigação de riscos a liberdades fundamentais, como acesso indevido de informações biométricas por órgãos de inteligência sem devido processo e fundamentação;

3. Adote as providências cabíveis para a garantia do direito autônomo à proteção de dados pessoais e do respeito aos direitos dos titulares, com especial atenção aos princípios norteadores das atividades de coleta e processamento de dados pessoais presentes no Art. 6º da Lei n. 13.709, de 14 de agosto de 2018.

Nestes termos, pede deferimento.

Brasília, 19 de julho de 2021

As entidades listadas abaixo subscrevem o presente ofício:

1. *Coalizão Direitos na Rede*
2. *Comissão de Proteção de Dados e Privacidade da Seccional do Rio de Janeiro da Ordem dos Advogados do Brasil (OAB-RJ)*
3. *Aliança Nacional LGBTI+*
4. *Grupo Dignidade*
5. *Centro Popular de Direitos Humanos - CPDH*
6. *Conectas Direitos Humanos*
7. *Kurytiba Metropole*
8. *Instituto Brasileiro de Defesa do Consumidor - IDEC*
9. *Intervozes*
10. *Instituto de Tecnologia e Sociedade (ITS Rio)*
11. *Instituto Vero*
12. *AqualtuneLab*