CÂMARA MUNICIPAL DE
SÃO PAULO

29º GV - Vereadora Janaina Paschoal (PP)

REQUERIMENTO N° ____/2025

Requer a constituição de uma Comissão Parlamentar de Inquérito, composta por 7 (sete) membros e com duração de 120 dias, para apurar a atuação da empresa Tools for Humanity que, por meio do projeto World ID, oferecera recompensas financeiras para realizar o escaneamento da íris de cidadãos paulistanos.

Excelentíssimo Senhor Presidente da Câmara Municipal de São Paulo,

Logo no início deste ano de 2025, surgiram diversas matérias jornalísticas, noticiando a vasta adesão da população da cidade de São Paulo, sobretudo da periferia, ao escaneamento de suas próprias íris em troca do recebimento de um valor em criptomoeda emitida pela empresa pagadora.

Instada a se explicar, a empresa declarou que seu produto foi idealizado para oferecer ao usuário a possibilidade de fazer uma prova de autenticidade humana na rede, diferenciando de inteligências artificiais.

Logo que teve acesso a tal informação, a subscritora da presente se manifestou em suas redes sociais, alertando para a relevância da ocorrência, bem como para a possibilidade de ser melhor apurada por meio de Comissão Parlamentar de Inquérito.

Com efeito, considerando que as informações de biometria são classificadas como dados sensíveis segundo a LGPD (Lei Geral de Proteção de Dados), esta parlamentar vem acompanhando com vigilante interesse a atuação da World Foundation em seu projeto World ID, iniciativa da empresa Tools for Humanity, que tem pontos espalhados por toda a Capital.

Esta Vereadora não ignora a crescente adesão de diversos setores na utilização da autenticação biométrica, método que trata informações pessoais relacionadas ao corpo humano

como senha única de acesso. No entanto, resta importante notar que tal senha, uma vez comprometida, não pode ser alterada, gerando grande prejuízo ao portador.

O valor, a princípio ofertado, chegava à casa de R$ 700,00 (setecentos reais), para que qualquer indivíduo tivesse suas informações extraídas e transformadas em um token digital armazenado em bases de dados estrangeiras.

A remuneração se tornou o grande atrativo para as pessoas, que passaram a formar enormes filas, esperando para terem seus olhos escaneados em troca de uma porção de moedas virtuais emitidas pela própria empresa no seu aplicativo. Com isso o projeto já arrecadou dados de mais de 400 (quatrocentos mil) paulistanos (https://g1.globo.com/tecnologia/noticia/2025/01/25/pagamento-por-foto-da-iris-atraiu-meio-milhao-de-brasileiros-com-foco-na-periferia-de-sp-ate-ser-barrado-pelo-governo.ghtml).

A ora subscritora não fecha os olhos ao fato de que cada vez mais nos aproximamos de um tempo em que a autenticação biométrica se torna tecnologia necessária para o mundo digital. Não obstante, tal tecnologia requer muito cuidado no tratamento destas informações, haja vista que seu método basilar necessita utilizar dados biológicos, fenotípicos e únicos, muito íntimos e intrinsecamente relacionados à cada pessoa. Quanto ao procedimento de coleta, envolve proximidade extrema, desconforto e até mesmo riscos.

Embora a signatária não esteja advogando no momento, atuou por muitos anos como advogada criminalista e lembra, nitidamente, de todas as discussões havidas relativamente ao indiciamento civil e criminal.

Com efeito, quantos não foram os trabalhos acadêmicos e os habeas corpus, em que estudiosos e operadores do Direito buscavam demonstrar que, quando o investigado já era identificado civilmente, não se fazia necessária sua identificação criminal, com coleta de digitais.

Muitos foram os acórdãos das mais elevadas Cortes a referendar a não necessidade de expor o indivíduo a esse procedimento invasivo.

Ora, eis que passados alguns anos, qualquer portaria de prédio se julga habilitada a exigir digital, fotografia e todos os documentos de qualquer mortal, que ouse querer entrar em suas dependências.

E, como num passe de mágicas, surge uma empresa estrangeira e propõe negociação estranha, em que paga, EM MOEDA PRÓPRIA, pela preciosa identificação de nossos cidadãos, por meio do delicado procedimento de escanear suas íris.

O poder público não pode ficar alheio a essa, no mínimo, curiosa situação. É preciso garantir a segurança da finalidade de uso dos dados de biometria, bem como a pessoalidade, a inviolabilidade do sigilo, a confiabilidade da coleta e o resguardo no armazenamento destes dados, sob risco de prejuízo a uma população inteira caso sejam vazados, fraudados ou usados de maneira leviana ou mesmo de má fé. Quando uma base de dados é comprometida todas as informações nela contidas são afetadas, isso faz de quaisquer eventuais problemas potencialmente catastróficos e com prejuízos massivos.

A subscritora da presente ministra a disciplina Biodireito na Faculdade de Direito da Universidade de São Paulo e, em um dos vários módulos da matéria, analisa a história das pesquisas com seres humanos, sendo certo que, no passado (remoto e recente), bem como no presente, atrocidades foram cometidas em países considerados subdesenvolvidos, em nome da Ciência, não raras vezes, mediante remuneração a pessoas, ou grupos, vulneráveis.

Até mesmo organizações criminosas voltadas para comprar rins, em localidades carentes, já agiram no Brasil.

Com isso, não se está a dizer que a prática que, mediante este requerimento se busca investigar, seja criminosa; entretanto, nesse primeiro momento, não é possível afastar tal possibilidade. E, ainda que fosse, não se pode negar ser imperioso entender os detalhes do que essa empresa e seus administradores pretendem no Brasil e, mais especificamente, em São Paulo.

Atenta à sensibilidade da situação, a Autoridade Nacional de Proteção de Dados (ANPD) emitiu resolução, suspendendo a possibilidade de remuneração ao usuário por escaneamento de íris, sendo certo que, em 11 (onze) de fevereiro do ano corrente, o Conselho Diretor da ANPD indeferiu recurso da empresa, mantendo a suspensão (https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-recurso-administrativo-conselho-diretor-mantem-suspensao-de-pagamento-por-coleta-de-iris).

O Despacho Decisório nº 3/2025/FIS/CGF, que primeiro determinou a suspensão da compensação financeira feita pela empresa, cita como justificativa "o teor da Nota Técnica nº 4/2025/FIS/CGF/ANPD". Essa nota aponta que a compensação financeira invalidaria o livre consentimento:

> "7.6 Apesar da resposta negativa, a compensação financeira é confirmada pela própria regulada ao indicar que o titular pode optar por solicitar os tokens WLD e ao explicar que a conversão na moeda local exige lapso de 24 horas. De fato, no Brasil, tal compensação está em torno de R$ 300 e R$ 470, a depender da cotação dos 25 tokens WLD oferecidos aos titulares pelo registro.
>
> 7.7 À primeira vista, a oferta de contraprestação pecuniária pode ser interpretada como elemento que interfere na autonomia do titular: ela influencia sobremaneira na decisão quanto à disposição de seus dados pessoais, especialmente em casos nos quais potencial vulnerabilidade e hipossuficiência tornem ainda maior o peso do pagamento oferecido para a sua tomada de decisão. A manifestação da vontade, nesses casos, é menos autônoma e mais influenciada por fatores externos, prejudicando o qualificador "livre" exigido pela LGPD para que o consentimento seja válido – especialmente por se tratar de um dado pessoal sensível, em relação ao qual os parâmetros de proteção são mais elevados. Por outro lado, seria razoável ponderar que, mesmo no caso de direitos fundamentais, é possível a sua limitação voluntária como expressão – precisamente – da autonomia de cada indivíduo. Nesse caso, fatores como duração, abrangência, intensidade e finalidade de cada situação concreta precisam ser considerados para avaliar a legitimidade das autolimitações impostas a esses direitos."

(disponível em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzNecesYdd_tZp-0w7M55fZJpoHOzEMG_PdSXLtjMpJTrCwyUvB0ZP8nCbud-aECp3wS48Cc6UYN8co-Z_cSDs6h).

O mesmo documento evidencia outras práticas da empresa em desconformidade com a LGPD e que comprometem a acessibilidade de informações importantes:

> "8.6 É flagrante, direta e evidente, portanto, a existência de comportamento em desconformidade com a LGPD, cuja gravidade é acentuada pela natureza do tratamento realizado, que envolve dados sensíveis e em relação aos quais existem, ainda, dúvidas e ponderações.
>
> 8.7 Diante do exposto, sugere-se a adoção de medida preventiva, com fundamento nos arts. 30 e 32, §1º, do Regulamento de Fiscalização, para determinar à World Foundation, por meio da Tools for Humanity, que realize a indicação de encarregado de dados pessoais em seu site, nos termos do que dispõem os arts. 41, §1º, da LGPD e 8º e 9º do Regulamento do Encarregado.
>
> 8.8 A título de registro, aponte-se que, para além da ausência do encarregado, os sites da World Foundation e da TFH dificultam a busca de informações pelos titulares. Por exemplo, a página sobre os pontos de coleta no Brasil não possui links diretos para os Termos de Uso das organizações, suas Políticas de Privacidade ou o Termo de Consentimento para a coleta dos dados. Para acessar esses documentos, é necessário que o titular busque as perguntas frequentes e selecione a pergunta "Como a Rede World cumprirá as leis que regulam a coleta de dados biométricos e a transferência de dados?" para ter acesso ao link que leva aos Termos de Uso e à Política de Privacidade da TFH. Registre-se que, por padrão, essas páginas são abertas em inglês, cabendo ao titular de dados escolher "português" na lista de seleção que aparece ao lado esquerdo da tela. Paralelamente, há também os Termos de Uso da World Foundation e, após muitas buscas, é possível encontrar o Formulário Consentimento – novamente, em site distinto do que informa os pontos de coleta no Brasil."

A assessoria desta Vereadora acessou a íntegra do processo em trâmite perante a ANPD e constatou passagens muito suspeitas na política de privacidade da World Foundation, pois a própria empresa noticia o envio dos dados coletados para outros países, admitindo que não são resguardados pelas mesmas garantias vigentes no Brasil, nos seguintes termos:

> "7.1 Transferência de dados.
>
> Quando você nos fornece os seus dados, estes podem ser transferidos, armazenados ou tratados num local diverso do local onde os seus dados foram originalmente coletados. O país para o qual os seus dados são transferidos ou no qual são armazenados ou tratados pode não ter as mesmas leis de proteção de dados que o país onde você forneceu inicialmente os seus dados. Envidamos os melhores esforços para cumprir os princípios previstos em cada jurisdição relativamente às leis de privacidade. Apenas partilhamos dados pessoais com agentes de tratamento fora da sua jurisdição se tal transferência for lícita e se estivermos confiantes de que o subcontratado protegerá os seus dados, conforme exigido pelas leis aplicáveis e, além disso, de acordo com os nossos padrões.
>
> 7.2 Riscos da transferência
>
> Segue, abaixo, uma lista de possíveis riscos que podem surgir se transferirmos os seus dados pessoais (caso os seus dados sejam considerados dados pessoais) para os Estados Unidos e para a União Europeia. Abaixo, também resumimos como mitigamos os respectivos riscos. Não transferimos os seus dados pessoais para as Ilhas Cayman. Embora façamos o possível para garantir que os nossos subcontratados estão contratualmente obrigados a proteger adequadamente os seus dados, estes subcontratados podem não estar sujeitos à lei de privacidade e proteção de dados do seu país. Se os subcontratados tratarem ilegalmente os seus dados sem autorização, poderá ser difícil reivindicar os seus direitos de privacidade contra esses subcontratados. Mitigamos este risco à medida que celebramos acordos rigorosos de tratamento de dados com os nossos subcontratados, que os obrigam a proteger os seus dados. É possível que a legislação em matéria de privacidade e proteção de dados no seu país seja incompatível com a legislação dos EUA ou da União Europeia (UE). Tentamos sempre observar os padrões mais rigorosos de proteção de dados a que

estamos sujeitos. É possível que os seus dados pessoais estejam sujeitos ao acesso por agentes públicos e autoridades governamentais. Nesses casos, nos comprometemos a contestar em tribunal qualquer pedido de acesso governamental inválido, genérico ou ilegal

Utilizamos ainda encriptação avançada para impedir acessos não-autorizados. Observe que esta lista contém exemplos, mas pode não incluir todos os possíveis riscos aplicáveis a você. ” (Disponível em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzPKCelEeHL5YCo3tLINZxK8E-8ggXF228VGoyXsWPRlhZpFiWuJDVjb2Os1Zne75f-zBQgto9rOu0vi4InYI7vQ).

Na seção 8 do mesmo documento, que trata de quando a empresa compartilha os dados, se encontram os seguintes itens:

“Podemos compartilhar os seus dados pessoais com os nossos advogados e outros consultores profissionais quando necessário para obter aconselhamento ou de outra forma proteger e gerir os nossos interesses comerciais.

Podemos compartilhar os seus dados pessoais no âmbito de ou durante negociações relativas a qualquer fusão, venda de ativos da empresa, financiamento ou aquisição de toda ou parte da nossa atividade por outra empresa.

Os dados, incluindo as suas informações pessoais, podem ser compartilhados entre as nossas atuais e futuras empresas-mãe, afiliadas e subsidiárias e outras empresas sob controle e propriedade comuns. ”

A pergunta que precisa ser respondida é a seguinte: Por qual razão esses parceiros internacionais têm interesse nas íris dos cidadãos paulistanos? É incrível que, até o presente momento, nenhuma autoridade tenha olhado com a devida profundidade para essa desafiadora situação. Esta Parlamentar, talvez por seus estudos acadêmicos, talvez por ser da área do Direito, entende firmemente que esta Casa tem o poder, na verdade, o DEVER, de apurar meticulosamente essa situação.

Não é sem motivo que diversos países suspenderam a atuação da empresa em seus territórios, podendo-se citar Espanha (https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/worldcoin-se-compromete-paralizar-su-actividad-en-espana), Coreia do Sul (https://www.coinspeaker.com/worldcoin-tools-for-humanity-fined-830k-south-korea/), Portugal (https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/123157), Argentina (https://www.batimes.com.ar/news/economy/buenos-aires-province-imposes-sanction-on-worldcoin-for-irregular-handling-of-iris-scanning.phtml) e Alemanha (https://www.reuters.com/technology/german-data-watchdog-probing-worldcoin-crypto-project-official-says-2023-07-31/).

No âmbito de leis que tratam das identificações biométricas, uma das legislações pioneiras, já aprimoradas, é o ato regulatório do Estado americano de Illinois, *Biometric Information Privacy Act*, de 2008, que chama atenção para o contexto da regulamentação e o rigor com que trata dos dados sensíveis, notavelmente no trecho transcrito a seguir, seguido de livre tradução:

> "(740 ILCS 14/15)
>
> Sec. 15. Retention; collection; disclosure; destruction.
>
> (a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.
>
> (b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally
>
> authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally

authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the

subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or

biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a

financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by

State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid

warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all

biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all

biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(Source: P.A. 95-994, eff. 10-3-08.)" (Texto disponível em: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004).

Livre tradução:

"(740 ILCS 14/15)

Seção 15. Retenção; coleta; divulgação; destruição.

(a) Uma entidade privada em posse de identificadores biométricos ou informações biométricas deve desenvolver uma política escrita, disponibilizada ao público, estabelecendo um cronograma de retenção e diretrizes para destruir permanentemente identificadores biométricos e informações biométricas quando o propósito inicial para coleta ou obtenção de tais identificadores ou informações tiver sido satisfeito, ou dentro de 3 anos da última interação do indivíduo com a entidade privada, o que ocorrer primeiro. Na ausência de um mandado ou intimação válidos emitidos por um tribunal de jurisdição competente, uma entidade privada em posse de identificadores biométricos ou informações biométricas deve cumprir seu cronograma de retenção estabelecido e diretrizes de destruição.

(b) Nenhuma entidade privada pode coletar, capturar, comprar, receber por meio de comércio ou de outra forma obter o identificador biométrico ou informações biométricas de uma pessoa ou cliente, a menos que primeiro:

(1) informe o sujeito ou o representante legalmente autorizado do sujeito por escrito que um identificador biométrico ou informação biométrica está sendo coletado ou armazenado;

(2) informe o sujeito ou o representante legal autorizado do sujeito por escrito sobre o propósito específico e o período para o qual um identificador biométrico ou informação biométrica está sendo coletado, armazenado e usado; e

(3) receba uma liberação por escrito executada pelo sujeito do identificador biométrico, ou informação biométrica ou representante legalmente autorizado do sujeito.

(c) Nenhuma entidade privada em posse de um identificador biométrico ou informação biométrica pode vender, arrendar, negociar ou lucrar de outra forma com o identificador biométrico ou informação biométrica de uma pessoa ou cliente.

(d) Nenhuma entidade privada em posse de um identificador biométrico ou informação biométrica pode divulgar, rediscutir ou de outra forma disseminar o identificador biométrico ou informação biométrica de uma pessoa ou cliente, a menos que:

(1) o sujeito do identificador biométrico ou informação biométrica ou representante legalmente autorizado do sujeito consinta com a divulgação ou rediscussão;

(2) a divulgação ou redistribuição conclua uma transação financeira solicitada ou autorizada pelo sujeito do identificador biométrico ou das informações biométricas ou pelo representante legalmente autorizado do sujeito;

(3) a divulgação ou redistribuição é exigida por lei estadual ou federal ou portaria municipal; ou

(4) a divulgação é exigida de acordo com um mandado ou intimação válido emitido por um tribunal de jurisdição competente.

(e) Uma entidade privada em posse de um identificador biométrico ou informações biométricas deve:

(1) armazenar, transmitir e proteger contra divulgação todos os identificadores biométricos e informações biométricas usando o padrão razoável de cuidado dentro da indústria da entidade privada; e

(2) armazenar, transmitir e proteger contra divulgação todos os identificadores biométricos e informações biométricas de uma maneira que seja tão ou mais protetora do que a maneira pela qual a entidade privada armazena, transmite e protege outras informações confidenciais e sensíveis. (Fonte: P.A. 95-994, em vigor em 10-3-08.) ”

Vale ressaltar que referido diploma legislativo nasceu da preocupação com a segurança de dados biométricos, em decorrência da recuperação judicial da empresa Pay By Touch, que oferecia a possibilidade de pagamentos usando a impressão digital, algo bem menos invasivo que a biometria por íris.

A referendar a necessidade desta Casa se debruçar sobre os fatos ora trazidos à apreciação, imperioso consignar que a empresa, que vem "comprando" as íris dos cidadãos paulistanos, por nascimento ou afeto, não pode atuar nos Estados Unidos, da forma que vem atuando em São Paulo (https://blockworks.co/news/worldcoin-not-in-us). O próprio site da empresa não lista nenhum lugar em solo norte-americano onde se possa encontrar seus equipamentos de escaneamento de íris. É preciso buscar as razões.

A fim de ilustrar os sérios riscos a que nosso povo foi exposto, lembra-se que, no Afeganistão, o grupo Talibã teve acesso a bases de dados de biometria, resultando em perseguições e graves violações dos direitos humanos. A matéria do CMI – Anti-corruption Resource Centre traz o trecho transcrito a seguir incluindo tradução livre:

> "A March 2022 Human Rights Watch(HRW) report documents how tracking and identification of previous-regime employees in Afghanistan after the 2021 Taliban takeover has been supported by person-registers introduced by international organisations. Separate from the Afghan Tazkira – the official national identity register – biometric registries to manage payrolls for the police, security staff, army and judges were created. It is believed that the Taliban now have access to some of these.
>
> For example, the HRW report includes the case of a former judge who was arrested when trying to renew his passport to leave the country. His fingerprints were scanned and tracked in a payroll database, which helped the Taliban to identify his previous role.
>
> Such biometric data helps the Taliban to decide who goes free and who is punished. There is particular concern for former civil servants or activists, and for women who used to work in roles that are now considered 'unsuitable'.
>
> Tools intended for development, and to help reduce fraud and corruption, have become tools for persecution. " (Texto disponível em: https://www.u4.no/blog/biometric-data-putting-people-at-risk-in-the-name-of-anti-corruption).

CÂMARA MUNICIPAL DE
SÃO PAULO

29º GV - Vereadora Janaina Paschoal (PP)

Tradução livre:

> "Um relatório da Human Rights Watch (HRW) de março de 2022 documenta como o rastreamento e a identificação de funcionários do regime anterior no Afeganistão após a tomada do poder pelo Talibã, em 2021, foram apoiados por registros de pessoas introduzidos por organizações internacionais. Separados do Tazkira afegão – o registro oficial de identidade nacional – foram criados registros biométricos para gerenciar as folhas de pagamento da polícia, equipe de segurança, exército e juízes. Acredita-se que o Talibã agora tenha acesso a alguns deles.
>
> Por exemplo, o relatório da HRW inclui o caso de um ex-juiz, que foi preso ao tentar renovar seu passaporte para deixar o país. Suas impressões digitais foram escaneadas e rastreadas em um banco de dados de folha de pagamento, o que ajudou o Talibã a identificar sua função anterior.
>
> Esses dados biométricos ajudam o Talibã a decidir quem fica livre e quem é punido. Há uma preocupação particular com ex-funcionários públicos ou ativistas, e com mulheres que costumavam trabalhar em funções que agora são consideradas "inadequadas".
>
> Ferramentas destinadas ao desenvolvimento e para ajudar a reduzir fraudes e corrupção tornaram-se ferramentas de perseguição. "

Para guardar a mais absoluta transparência, importante mencionar que, tão logo a subscritora da presente externou parte de suas preocupações em suas redes sociais, um advogado, representando a empresa, solicitou audiência. Não obstante, quando a assessoria sugeriu data para que viesse ao Gabinete expor mais detalhadamente a atuação questionada, ou enviasse maiores esclarecimentos, quedou-se inerte, talvez por não ter como refutar os pontos delicados nesta elencados.

Pelo exposto, requer-se constituição de uma Comissão Parlamentar de Inquérito - CPI, composta por 7 (sete) membros, com duração de 120 dias, prorrogáveis segundo o regimento, para:

1. Investigar o escaneamento de íris na Cidade de São Paulo, com ou sem remuneração, por parte da World Foundation;
2. Entender a finalidade para a qual dados sensíveis da população vêm sendo massivamente coletados na cidade de São Paulo;
3. Entender o procedimento de coleta e as medidas de segurança adotadas no armazenamento, bem como a natureza do banco de dados;
4. Entender por qual razão a empresa responsável pela tecnologia que se busca investigar foi proibida de atuar em tantos países e por quais motivos escolheu o Brasil e, em especial, a Cidade de São Paulo;
5. Entender por qual razão a empresa transfere os dados dos cidadãos, que aceitam "vender" suas íris, para o exterior (informação passível de ser confirmada em: https://anpd-super.mj.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?yPDszXhdoNcWQHJaQlHJmJIqCNXRK_Sh2SMdn1U-tzMDh9BcZS-cN6BKK5m3mxCllrwClU6rvlcNmSm_214T2bjC1Be9xo4kQjNdbsAFGFNwYtw0Af7IoDSQXsq4fUbL);
6. Investigar a compensação financeira que foi oferecida pela empresa em troca das informações, inclusive no que concerne à natureza dessa remuneração, por moeda própria, à revelia e paralelamente ao sistema financeiro;
7. Apurar se há outras pessoas físicas e/ou jurídicas realizando práticas correlatas;

Para bem desempenhar sua missão, a Comissão Parlamentar de Inquérito a ser instalada, poderá lançar mão de todos os meios de investigação em direito admitidos, com destaque para a expedição de ofícios à Autoridade Nacional de Proteção de Dados (ANPD), bem como a oitiva dos dirigentes e prepostos da empresa, de vítimas e especialistas, o que, desde logo, se requer. Haja vista a eventual necessidade de ouvir experts e autoridades estrangeiras, pleiteia-se, igualmente, a realização de audiências à distância.

Imperioso consignar que esta vereadora não quer iniciar uma cruzada contra a tecnologia ou contra a empresa e as pessoas envolvidas nessa estranha operação. O intuito é não permitir que, pelas carências de nosso País, nosso povo seja utilizado como cobaia, com exposição de seus dados para finalidades espúrias.

CÂMARA MUNICIPAL DE
SÃO PAULO

29º GV - Vereadora Janaina Paschoal (PP)

Para esse nobre fim roga-se o apoio dos pares!

_____

Janaina Paschoal

Vereadora PP