TRANSCRIÇÕES DA 39ª AUDIÊNCIA PÚBLICA

ADPF 1.143

REGULAÇÃO DO USO DE FERRAMENTAS DE MONITORAMENTO SECRETO DE APARELHOS DE COMUNICAÇÃO PESSOAL

Ministro-Relator Cristiano Zanin



SUPREMO TRIBUNAL FEDERAL - STF

SECRETARIA JUDICIÁRIA – SEJ

COORDENADORIA DE PROCESSAMENTO FINAL/GERÊNCIA DE TRANSCRIÇÃO

DIA 10/7/2024 – MANHÃ

LAURA SHERTEL MENDES (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL - COMISSÃO DE DIREITO DIGITAL).....16

ALISSON ALEXSANDRO POSSA (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL – COMISSÃO DE DIREITO DIGITAL).....21

SAMARA CASTRO (PRESIDÊNCIA DA REPÚBLICA – SECRETARIA DE POLÍTICAS DIGITAIS DA SECRETARIA DE COMUNICAÇÃO SOCIAL).....23

WESLEY VAZ (TRIBUNAL DE CONTAS DA UNIÃO - SECRETARIA DE CONTROLE EXTERNO DE GOVERNANÇA, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL DO ESTADO).....30

BÁRBARA SIMÃO (ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA).....34

PEDRO JOSÉ NASSER SALIBA (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA – DATA PRIVACY BRASIL).....42

RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC)...51

HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA AGÊNCIA NACIONAL DE INTELIGÊNCIA - ABIN - INTELIS).....59

PERGUNTAS AOS EXPOSIDORES.....65

DIA 10/7/2024 – TARDE

SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP).....92

LAURO RODRIGUES DE MORAES RÊGO JÚNIOR (PARTIDO VERDE).....98

ANDRÉ CYRINO (CONEXIS BRASIL DIGITAL - SINDICATO NACIONAL DAS EMPRESAS DE TELEFONIA E DE SERVIÇO MÓVEL CELULAR E PESSOAL).....103

VINICIUS GOMES DE VASCONCELLOS (INSTITUTO BRASILEIRO DE DIREITO PROCESSUAL PENAL - IBRASPP E REVISTA BRASILEIRA DE DIREITO PROCESSUAL PENAL - RBDPP).....110

VINICIUS VALENTIN RADUAN MIGUEL (UNIVERSIDADE FEDERAL DE RONDÔNIA).....117

RENATO OPICE BLUM (ESCOLA BRASILEIRA DE DIREITO - EBRADI).....124

ESTELA ARANHA (CONSELHO CONSULTIVO DE ALTO NÍVEL DA ONU PARA INTELIGÊNCIA ARTIFICIAL).....130

JOÃO FELIPE ATAÍDE DA CUNHA RÊGO (GESTOR PÚBLICO).....137

PERGUNTAS AOS EXPOSIDORES.....142

ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB).....162

CARINA QUITO (INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS - IBCCRIM).....169

CARLOS HÉLDER C. FURTADO MENDES (INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS - IBCCRIM).....173

LARAH BRAHIM (UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO-FD-USP - CENTRO DE PESQUISA E EXTENSÃO EM CIÊNCIAS CRIMINAIS-CPECC).....177

GIOVANNI DINIZ (UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO-FD-USP; CENTRO DE PESQUISA E EXTENSÃO EM CIÊNCIAS CRIMINAIS - CPECC).....180

ALEXANDRE PACHECO (FGV – DIREITO SP – CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO)..185

HELOISA ESTELITTA (FGV - DIREITO SP - CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO).....190

CHARLENE NAGAE (INSTITUTO TORNAVOZ, MEDIA DEFENCE E ASSOCIAÇÃO BRASILEIRA DE JORNALISMO INVESTIGATIVO – ABRAJI).....192

PERGUNTAS AOS EXPOSITORES.....199

DIA 11/7/2024

VICTOR EPITÁCIO CRAVO TEIXEIRA (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA).....220

LEONARDO CARDOSO MAGALHÃES (DEFENSOR PÚBLICO-GERAL).....226

RODRIGO MORAIS FERNANDES (POLÍCIA FEDERAL).....234

LILIAN CINTRA DE MELO (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA – SECRETARIA DE DIREITO DIGITAL).....239

GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL).....247

SENHOR JOÃO RICARDO DA CUNHA CROCE LOPES (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - EXÉRCITO).....255

ANDRÉ LUIZ CORRÊA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - AERONÁUTICA).....264

PATRICIA DA SILVA VIEIRA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - MARINHA).....270

ANA BÁRBARA GOMES (INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS).....283

NADIA ZILOTTI ALENCAR (POLÍCIA RODOVIÁRIA FEDERAL).....291

PERGUNTAS AOS EXPOSITORES.....294

JULIANO SOUTO MOREIRA MADALENA (ASSOCIAÇÃO FIQUEM SABENDO).....314

THIAGO PAVIN RODRIGUES (FUNDAÇÃO INSTITUTO DE PESQUISAS ECONÔMICAS - FIPE).....321

TEREZA MELLIN GIMENES (ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA ELÉTRICA E ELETRÔNICA - ABINEE).....328

10/7/2024 – MANHÃ

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Bom dia a todos. Eu queria cumprimentar a Doutora Elizeta Paiva Ramos, Subprocuradora Geral da República, que subscreve a petição inicial desta ação na condição de Procuradora-Geral da República em exercício à época. Queria cumprimentar o Doutor Marcelo Turbay, que aqui representa o Conselho Federal da Ordem dos Advogados do Brasil, cumprimentar todas as autoridades presentes, as senhoras e os senhores.

Agradecendo imensamente a presença de todas e de todos, farei uso de alguns minutos iniciais para introduzir o assunto que passaremos a abordar.

Designei a presente audiência nos autos desta Ação de Arguição de Descumprimento de Preceito Fundamental 1.143, que trata dos limites e possibilidades da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e da ferramenta de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, ou seja, as popularmente conhecidas ferramentas de monitoramento secreto de aparelhos de comunicação pessoal.

O tema é bastante rico e complexo e seus contornos necessitam, de fato, de maior aprofundamento. Há referência à suposta violação sistemática de

preceitos fundamentais no uso desses equipamentos para monitorar magistrados, advogados, jornalistas, políticos, defensores de direitos humanos, dentre outros envolvidos.

Em jogo se encontram - citei ao longo dos despachos que proferi - os direitos fundamentais à intimidade, à vida privada e à inviolabilidade do sigilo das comunicações pessoais, todos expressamente previstos na Constituição Federal.

O objetivo desta audiência é instruir o processo com informações de todos os segmentos da sociedade, seja através de órgãos públicos, de representantes da sociedade civil, especialistas ou simplesmente interessados que possuem experiência e autoridade no assunto discutido. Ou seja, entendo que esta audiência é uma oportunidade de colher manifestações diversas em um tema de interesse público, é o momento de a sociedade civil, nos seus mais diversos segmentos, participar do processo decisório de um tema tão relevante que está em discussão em diversos países, em especial em algumas Cortes Constitucionais e também em Supremas Cortes.

De fato, a audiência pública tem esse objetivo de coletar informações qualificadas para que se forme um convencimento acerca do tema objeto da ação, buscando-se uma interpretação constitucional que leve em conta a diversidade de vozes e compreensões para, além de trazer o conhecimento do

Supremo Tribunal Federal, fatos que tenham relevância para análise dos preceitos fundamentais tratados na petição inicial.

Para atingir essa especialidade e diversidade de pensamento, dei publicidade a todos os atos convocatórios desta audiência, e enviamos convites a diversas autoridades. Além dos convites protocolares, também enviei convites a todas as empresas mencionadas na petição inicial, mesmo sabendo que foram nominadas apenas para fins exemplificativos. Porém, infelizmente, todas declinaram.

Lembro ainda que a ação foi ajuizada pela Procuradoria-Geral da República, subscrita pela Doutora Elizeta Paiva Ramos em peça bastante delineada, e que aproveito para enaltecer. Recordo também que, inicialmente, a ação tramitava sob a forma de ação direta de inconstitucionalidade por omissão, ADO, mas, a pedido da própria PGR, decidi converter o processo em ADPF, instrumento processual de natureza mais plural e heterogênea.

Para atingir os objetivos desta audiência e dar oportunidade a todos a possibilidade de manifestação, esclareço que optei por designar aos expositores o tempo de 10 minutos para fazer uso da palavra com suas colocações e prestar os seus esclarecimentos.

Ao final de cada período desta audiência, caso haja tempo suficiente, abrirei para perguntas às pessoas que participaram do respectivo bloco.

Assim, para que tudo isso funcione e todos consigam participar, solicito a colaboração de todos para cumprir rigorosamente este tempo. Teremos um relógio indicando o tempo e nossos colaboradores do cerimonial também farão os alertas aos expositores.

Feita essa pequena introdução, tenho a honra de passar de imediato a palavra à Doutora Elizeta Maria de Paiva Ramos para se manifestar pela Procuradoria-Geral da República, autora da ação.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Bom dia a todas e a todos! Cumprimento o Excelentíssimo Senhor Ministro Cristiano Zanin, Relator da ADPF 1.143, na pessoa de quem saúdo os demais integrantes da Mesa e os participantes desta audiência pública.

A presente solenidade foi designada nos autos da arguição de descumprimento de preceito fundamental, proposta pela Procuradoria-Geral da República, que versa sobre a regulação do uso por órgãos e agentes públicos de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal.

O tema em questão tem envergadura constitucional e desafia intensos debates em torno das técnicas especiais de investigação e de inteligência, em consonância com a preservação dos direitos e garantias fundamentais.

Na vida moderna, o uso de *smartphones*, *notebooks* e outros dispositivos informáticos é essencial. A versatilidade dessas tecnologias diminui distâncias e otimiza muitas tarefas do cotidiano. Em um só desses dispositivos é possível registrar incontáveis dados pessoais, como fotografias e vídeos em momentos em família, mensagens, senhas de acesso a bancos, documentos oficiais, meios de pagamento e registros de localização.

Toda essa gama de informações merece a especial atenção e proteção de inviolabilidade salvaguardada pela Constituição. Não é sem razão que já se anuncia, no plano do Direito comparado, o direito fundamental informático, que tem como objeto a proteção do próprio sistema informático pessoal e, por consequência, do indivíduo que o utiliza.

É nesse contexto que o emprego de técnicas especiais de investigação, aptas a relativizar a intimidade e a vida privada das pessoas, ganhou especial atenção no debate jurídico contemporâneo. A relevância da questão posta fica evidenciada pela proliferação de discussões no cenário internacional, notadamente na União Europeia e nos Estados Unidos da América, tendo o assunto chamado a atenção do Alto Comissariado da Organização das Nações Unidas para os Direitos Humanos, que, inclusive, emitiu pronunciamento objetivando permitir que fossem desenhadas estruturas jurídicas que garantam a privacidade de cidadãos com respeito aos direitos humanos.

Contudo, ao mesmo tempo em que é imperiosa a tutela dos direitos individuais, não se pode negligenciar que os criminosos atualizam continuamente suas técnicas para incorporar as mais recentes tecnologias emergentes em seus *modus operandi.* Eles foram os primeiros a operar nas ruas com *pagers*, com celulares, para trocar mensagens codificadas e evoluíram muito desde então.

O crime organizado é sempre o primeiro a adotar a tecnologia. Os criminosos adotaram o mundo *on-line* muito antes que a polícia pudesse ao menos ter contemplado a ideia e, desde então, estão sempre um passo ou vários passos à frente das autoridades.

O emprego de programas espiões por autoridades públicas representa atualmente um dos assuntos mais controversos em tema de investigações criminais tecnológicas. Enquanto as autoridades operam pelos meios tradicionais de investigação, crimes graves são atualmente cometidos com o importante componente tecnológico.

Infelizmente, a lei não acompanhou o ritmo da tecnologia e essa desconexão tem criado um significativo problema de segurança pública. Nessa conjuntura, a Procuradoria-Geral da República, sensível aos desafios que emergem do natural descompasso entre a rápida evolução das tecnologias e a construção de soluções jurídicas, propôs perante o Supremo Tribunal Federal a ação direta de

constitucionalidade por omissão, posteriormente convertida na presente arguição de descumprimento de preceito fundamental.

O desenvolvimento desta ação de controle concentrado demanda que se conheçam com profundidade as tecnologias disponíveis e passíveis de utilização como instrumentos aplicáveis à investigação criminal. A obtenção de informações técnicas e avaliações formadas a partir de saberes específicos sobre os temas da discussão lançada à Corte se mostra imprescindível, portanto, para subsidiar a formação do convencimento deste Tribunal.

Fica, assim, reforçada a importância deste ato, que há de contribuir para uma visão holística da questão, sobretudo em razão do expressivo e qualificado quórum de participantes, autoridades e especialistas.

É com grande expectativa que a Procuradoria-Geral da República se faz presente nesta audiência pública, registrando seus agradecimentos pelo convite destinado ao Procurador-Geral da República e pela oportunidade do uso da palavra e acompanhamento das exposições programadas.

Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutora Elizeta Paiva Ramos.

Faço o registro da presença da Doutora Caroline Santos Lima e do Doutor Lucas Sales, Juízes Instrutores do meu Gabinete, aqui na Mesa, ao meu lado.

Passo a palavra ao Doutor Marcelo Turbay, Presidente da Comissão Especial de Estudos e Regulamentação sobre Investigação Defensiva, que representa o Conselho Federal da Ordem dos Advogados do Brasil.

Doutor Marcelo Turbay, com a palavra.

O SENHOR MARCELO TURBAY (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL) - Obrigado, Presidente!

Bom dia a todos e a todas!

Meus solenes cumprimentos ao eminente Ministro Cristiano Zanin, Relator da ADPF 1.143, que preside o ato.

Saúdo e parabenizo respeitosamente a Doutora Elizeta Ramos, representante do Ministério Público, pela iniciativa de promover a petição inicial e ser o abre-alas desta discussão tão relevante, tão cara ao Direito brasileiro, tão cara aos órgãos investigativos e, sobretudo, tão cara à Ordem dos Advogados do Brasil.

Cumprimento também os representantes de todas as entidades presentes.

Senhor Presidente, este é um tema absolutamente caro. A advocacia enfrenta rotineiramente diversos embates em relação aos meios de coleta de prova penal, aqueles já regulamentados e que há muito tempo são utilizados pelos órgãos investigativos. Ainda assim, há esse constante conflito, o conflito retórico, dialético, próprio do Direito, em relação aos limites, às metodologias empregadas pelos órgãos investigativos e, não raro, o Judiciário é obrigado a dirimir esses conflitos, tratando dos limites, fazendo valer a interpretação protetiva da legislação infraconstitucional e constitucional, para a preservação de direitos fundamentais, preservação dos direitos do investigado e também do advogado militante.

Com isso, a Ordem dos Advogados do Brasil é frequentemente instada a se posicionar, frequentemente instada a responder consultas de colegas que, no dia a dia da condução de casos penais, defrontam-se com a extensão de métodos investigativos que, ainda que já regulamentados, mostram sempre novidades com as quais a defesa é obrigada a lidar.

Apenas à guisa de exemplo, em uma determinada busca e apreensão que tive a oportunidade de tomar conhecimento dentro do Conselho Federal, a autoridade policial encaminhou um formulário para que a pessoa que estava sofrendo a busca e apreensão e teve o celular recolhido preenchesse

numericamente, fazendo um desenho mesmo, o código de acesso dele no iPhone, por exemplo, ou que ele indicasse as setas para a liberação do acesso ao Motorola, uma coisa absolutamente inventiva, sem que ele fosse cientificado do direito de não produzir prova contra si, sem que ele fosse cientificado do direito de não fornecer aquele código de acesso em um formulário entregue dentro de um auto de apreensão e recolhimento do aparelho celular.

Então, a defesa, instada, ao se defrontar com aquilo, busca o Conselho Federal da OAB para levar ao conhecimento da OAB este fato e fazer um pedido de consulta, um pedido de intervenção, diante da ofensa aos direitos do investigado, que também reflete uma ofensa às prerrogativas do profissional da advocacia.

Então, são muitos os temas e sobretudo em relação a uma matéria tão nova que está em discussão efervescente, sobretudo, no ano passado, depois de inúmeras matérias jornalísticas veiculadas em relação ao uso, pela Abin, de um determinado software para monitoramento e localização de pessoas em escala enorme, indistintamente. Então, as dificuldades são enormes.

Mesmo em relação à interceptação telefônica, à quebra de sigilo em geral, aos monitoramentos todos, à telemática, a advocacia frequentemente se vê obrigada a tratar e levar ao conhecimento dos tribunais problemas como

desproporcionalidade e grau de invasividade do meio investigativo, preservação de cadeia de custódia - e há precedente recente do STJ, de relatoria do Ministro Ribeiro Dantas, que firmou as balizas, de forma muito profunda, a respeito da preservação da cadeia de custódia, no caso de extração de dados de computador em busca de apreensão -; usurpação da competência investigativa, que é aquela muito conhecida investigação lateral de agente com prerrogativa de foro, e há *leading case,* aqui, do Supremo Tribunal Federal, num caso muito conhecido, já antigo, em que uma autoridade com prerrogativa de foro, um ex-senador da República, foi lateralmente investigado numa interceptação telefônica contra um terceiro que não detinha o foro. Então, se isso acontecia pela interceptação telefônica, que dirá para um meio de intrusão virtual remota ainda não regulamentado e que, a cada dia, se reinventa com novas metodologias.

Além disso, a necessidade de identificação de operadores e agentes que acessam a informação. Isso é fundamental para entender quem está manuseando o dado. Isso dentro, também, de uma metodologia de cadeia de custódia.

Além disso, o problema da *phishing expedition*, que vai ser um problema extremamente grave, a depender de como vier a regulamentação. Ora, se o agente investigativo tem acesso irrestrito ao aparelho celular, de forma remota, então, muito dificilmente, será possível identificar qual é o objeto da investigação

que ele está buscando dados a serem coletados. A *phishing expedition* vai ser um problema gravíssimo em relação aos meios de intrusão virtual remota.

Não há dúvida, é necessário regulamentar, é necessário que a sociedade debata esse tema e que o Judiciário seja a casa onde tudo isso vai transcorrer. Encontro fortuito, busca genérica de informações, dentre outros problemas.

Então, o Conselho Federal da Ordem dos Advogados do Brasil se posiciona, aqui, neste dia, com enorme preocupação, mas, ao mesmo tempo, entusiasmado, sabendo que essa discussão, que vai ser tratada aqui, hoje, será fundamental para os caminhos da regulamentação e para que as Cortes já se atentem para os meios investigativos que já estão acontecendo e de forma pouco clara, pouco transparente.

A minha fala é apenas introdutória, Excelência, agradecendo muito a oportunidade, mas deixo o detalhamento, deixo a profundidade do tema para a Comissão de Direito Digital, na pessoa da presidente, Doutora Laura, que está ali, e agradeço novamente a oportunidade e saúdo e parabenizo pela iniciativa. Muito obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Marcelo Turbay.

Então, eu vou, agora, a passar a palavra ao expositor Doutor Alisson Possa, que é advogado, mestre em Direito Constitucional, com ênfase em novas tecnologias, pesquisador e professor.

Ah, perfeito. Então, também fará exposição, conjuntamente, a Doutora Laura Mendes, que é Presidente da Comissão de Direito Digital do Conselho Federal da Ordem dos Advogados do Brasil, professora adjunta de Direito Civil da Universidade de Brasília e do Instituto Brasiliense de Direito Público, o IDP. Doutora *summa cum laude* em Direito Privado pela Universidade Humboldt, Berlim.

Doutora Laura, então, tem a palavra.

A SENHORA LAURA SHERTEL MENDES (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL - COMISSÃO DE DIREITO DIGITAL) - Bom dia a todas e a todos! Excelentíssimo Senhor Ministro Cristiano Zanin, Relator da ADPF 1.143, Excelentíssima Subprocuradora da República, Doutora Elizeta Maria Ramos, Colega, Doutor Turbay, Doutora Carolina, Doutor Lucas, Senhores e Senhoras.

É uma honra poder falar aqui em nome da Comissão de Direito Digital do Conselho Federal da Ordem dos Advogados do Brasil sobre um tema que pode ter tamanho impacto sobre os direitos fundamentais do cidadão brasileiro.

O presente caso trata da possibilidade da intrusão virtual em sistemas digitais por meio de ferramentas de monitoramento secreto e invasivo para fins de investigação criminal. Se, por um lado, poder-se-ia alegar o aumento da eficiência das atividades de investigação estatais por meio do uso dessas ferramentas, por outro, é certo que o potencial invasivo é tamanho que, sem a implementação das devidas garantias do Estado Democrático de Direito, em especial a reserva legal e a reserva de jurisdição, corremos o risco de criar um verdadeiro Estado de vigilância.

Nunca foi tão verdadeira a percepção de que as nossas vidas são um híbrido entre o real e o virtual. O que somos e vivemos sofre tamanho impacto do que acontece no mundo virtual que não mais podemos separar esses dois mundos com nitidez. Vivemos a era do *on-life*, nos termos de Luciano Floridi, isto é, uma realidade hiperconectada, na qual não faz mais sentido indagar se estamos *on-line* ou *off-line*. Mais do que nunca, é preciso garantir a autodeterminação e o desenvolvimento da personalidade no ambiente virtual para que possamos desfrutar desses direitos de forma real. Estamos a falar de softwares espiões, que se infiltram clandestinamente nos sistemas de informação, como computadores e celulares, permitindo àquele que controla esse software o acesso remoto a todas as informações armazenadas no aparelho, bem como às informações produzidas em tempo real, como mensagens e *e-mails* digitados, mas não enviados. Seria possível,

inclusive, falar, eventualmente, de uma manipulação de prova, que não está excluída quando se utiliza esse tipo de sistema.

Além disso, a infiltração pode possibilitar ao controlador o acionamento remoto da câmera e do microfone do aparelho, sem qualquer conhecimento do afetado. Nesse sentido, a infiltração permite uma coleta de dados mais ampla do que a interceptação telefônica ou telemática, pois não se trata apenas de interceptar um determinado tráfico de dados, mas de coletar todos os dados de um determinado aparelho já armazenados ou que estão sendo produzidos em tempo real.

É fácil perceber, Senhor Ministro, Senhoras e Senhores, que nem mesmo uma câmara instalada dentro de nossa casa teria um potencial invasivo tão grande como o desses softwares, que podem adentrar o mundo virtual de cada um de nós de forma clandestina e sorrateira. É sob esse olhar do alto grau de interferência na vida das pessoas e da sensibilidade das informações que podem ser coletadas que deve ser analisada juridicamente a instalação desse dispositivo em sistemas pessoais.

A utilização desse software para investigação policial foi analisada em decisão da Corte Constitucional Alemã de 2008, que extraiu uma nova dimensão do direito ao livre desenvolvimento da personalidade: o direito à confidencialidade e à integridade dos sistemas informáticos. O caso dizia a respeito

à análise da constitucionalidade da lei do Estado de Nordrheim-Westfalen, que permitia às autoridades locais de inteligência fazerem a busca remota das informações e do monitoramento *on-line* de computadores. O Tribunal, na ocasião, declarou inconstitucional a referida lei sob o fundamento de violação do direito geral à personalidade a partir dessa nova dimensão, o direito à garantia da confidencialidade e da integridade dos sistemas informáticos, também chamado em alemão o *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Em uma expressão mais simples, talvez, ele foi conhecido como um direito fundamental informático ou *Computergrundrecht*. No contexto de dependência das pessoas em relação aos sistemas informáticos, faz-se necessário assegurar a confiança dos cidadãos e dos indivíduos nesses sistemas, de modo a garantir que eles funcionem e que atendam às expectativas dos indivíduos. A decisão esclareceu que a infiltração desses sistemas não estaria completamente vedada pela lei fundamental alemã, mas estabeleceu determinadas condições, em especial a existência de uma lei específica autorizativa, a presença de autorização judicial, a identificação de um perigo concreto a um bem jurídico e, ainda, atendido todos esses requisitos, era necessário garantir que o núcleo da intimidade, ou seja, sempre que fossem coletadas informações extremamente íntimas, que essas informações pudessem ser descartadas ou protegidas de forma mais segura pela autoridade policial.

Acho também importante dizer, Ministro, Senhoras e Senhores, que, neste ano, a Corte Interamericana de Direitos Humanos, no mesmo sentido, condenou o Estado colombiano pela perseguição ao Coletivo de Advogados José Alvear, liderada pelo Juiz Rodrigo Modrovich. Reconheceu de forma inédita um novo direito humano, uma nova dimensão dos direitos humanos, o direito à autodeterminação informativa.

No Brasil, Senhoras e Senhores, nosso arcabouço constitucional também já tem a capacidade de trazer respostas adequadas para esse desafio, seja em razão do importante desenvolvimento jurisprudencial dessa Corte, que reconheceu no ano de 2020, sob a relatoria da Ministra Rosa Weber, o direito fundamental à proteção de dados, seja em razão da importante atuação do Congresso Nacional, que alterou a Constituição para garantir, de forma expressa, o direito fundamental à proteção de dados.

Um olhar para esse direito fundamental à proteção de dados permite enxergar caminhos para o presente caso. Certamente a gente pode enxergar a ampla coleta de dados, possibilitada por esse softwares espiões, como uma espécie de limitação desse direito fundamental, que somente pode ocorrer se condições específicas forem atendidas como uma base jurídica segura, com a clareza necessária sobre a finalidade do tratamento de dados para que se avalie o nível de intervenção dos direitos fundamentais e que seja também proporcional,

adequada e necessária à finalidade pretendida, adotando ainda as providências preventivas mínimas de cunho procedimental e organizacional, orientadas à segurança dos cidadãos envolvidos e à diminuição dos riscos de danos aos seus direitos da personalidade. Quanto mais grave for essa restrição, mais contundentes devem ser a justificativa, os critérios e as precauções.

Peço licença, Ministro, para chamar meu colega da OAB, Doutor Alisson, para terminar essa fala.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois não, Doutora Laura.

O SENHOR ALISSON ALEXSANDRO POSSA (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL – COMISSÃO DE DIREITO DIGITAL) - Excelentíssimo Ministro, demais Colegas da mesa, eu assumo aqui, em continuidade à fala da Doutora Laura, para falar sobre a jurisprudência do Supremo Tribunal Federal - e não é estranho o tema da coleta de dados, como o Doutor Turbay mencionou - e sobre o que nós temos de reserva legal e a possível aplicabilidade no caso.

Recentemente, em 2024, no HC 222.141 do STF, foi demonstrado que, mesmo no caso de decisão judicial reconhecendo a possibilidade da coleta dos dados, se existentes previsões, na reserva legal, acerca de limitação, por exemplo, do armazenamento dos dados, ele se impõe. Então, a decisão judicial precisa

observar os parâmetros legais, em sintonia com que a Doutora Laura falou a respeito da reserva legal.

Atualmente, no Brasil, nós temos duas legislações que são paradigmaticamente estudadas para aplicabilidade dos softwares espiões, a Lei das Interceptações Telefônicas e a Lei das Organizações Criminosas, que preveem agente virtuais infiltrados. Nenhuma das duas prevê medidas que, de fato, encaixem os *malwares*, pois, conforme a Doutora Laura mencionou, eles são extremamente mais invasivos. O Doutor Turbay também comentou a possibilidade de acesso a uma quantidade muito grande de dados, ficando quase impossível filtrar exatamente aquilo que o agente investigador vai de fato acessar ou não.

Então, em sede conclusiva, a gente tem um meio de prova atípico. Nós não temos uma legislação aplicável ao caso. Em se fazendo, portanto, a partir do princípio da reserva legal, a necessidade de uma legislação que autorize a instalação dos softwares espiões, fixando os seus limites e prevendo garantias adequadas de proteção contra formas de abuso e, de antemão, ser possível, considerar ilegal a utilização desses programas por autoridades policiais ou por qualquer outro ente, considerando carecer de fundamento jurídico.

Ministro, encerro a minha fala aqui no sentido de reforçar o que o contexto doutrinário brasileiro vem estudando, há muitos anos, acerca desses

novos mecanismos de investigação, os quais desafiam os limites dos direitos fundamentais já existentes.

Muito obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Alisson Possa.

Eu passo a palavra para a Doutora Samara Castro, advogada, Diretora do Departamento de Promoção da Liberdade de Expressão da Secretaria de Políticas Digitais da Secretaria de Comunicação Social da Presidência da República e representante da Secom no Observatório de Violência contra Jornalistas e Comunicadores do Ministério da Justiça e Segurança Pública.

Com a palavra a Doutora Samara.

A SENHORA SAMARA CASTRO (PRESIDÊNCIA DA REPÚBLICA – SECRETARIA DE POLÍTICAS DIGITAIS DA SECRETARIA DE COMUNICAÇÃO SOCIAL) - Bom dia!

Excelentíssimo Senhor Relator, Ministro Cristiano Zanin, Excelentíssima Subprocuradora-Geral da República, Doutora Elizeta Ramos, Doutor Marcelo Turbay, Doutora Caroline Lima, Doutor Lucas Sales, Senhoras e Senhores, demais autoridades presentes.

Represento aqui a Secretaria de Políticas Digitais da Secom. Entre as nossas competências estão a formulação e a implementação de políticas

públicas para a promoção da liberdade de expressão, do acesso à informação, do combate à desinformação, da proteção de vítimas de violações de direitos nos serviços digitais de comunicação. Além disso, também é nosso papel a promoção do pluralismo, da diversidade midiática e do desenvolvimento do jornalismo profissional.

O impacto das ferramentas de intrusão virtual na privacidade e na percepção de liberdade de expressão nos cidadãos é muito profundo. Visto que teremos contribuições de diversas áreas do governo aqui hoje, gostaria de reforçar a importância do papel crucial que o jornalismo desempenha na manutenção dos princípios constitucionais e na proteção do interesse público e do direito à informação.

O direito à informação abrange tanto a liberdade do emissor quanto o direito do destinatário de se informar e de ser informado. Assim, o direito de informar e o direito de receber informações são componentes integrados do mesmo direito.

O direito à informação é intrinsecamente ligado ao exercício do jornalismo e à atividade da imprensa, tanto quanto o direito à livre expressão. Esta Corte já reconheceu que o jornalismo é a própria manifestação e difusão do pensamento e da informação de forma contínua, profissional e remunerada.

Portanto, o jornalismo, o direito de acesso à informação e a liberdade de expressão são atividades interligadas por sua própria essência e não devem ser concebidas ou abordadas de forma independente.

A plena liberdade de exercício do jornalismo mantém uma relação simbiótica e mutualista com a democracia. Esta Corte reconheceu essa interdependência, afirmando que a imprensa, cuja materialização se dá pelo exercício da atividade jornalística, mantém com a democracia uma relação intrínseca.

O artigo 220 da Constituição preserva um amplo regime de liberdade de imprensa, explicitando que nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística.

Esta Corte também estabeleceu a impossibilidade de o Estado fixar quaisquer condicionamentos e restrições relacionados ao exercício da profissão jornalística, inclusive no que se refere à violação da garantia constitucional do sigilo da fonte. O jornalismo, mesmo em sua faceta crítica, contundente e muitas vezes incômoda, não é suscetível de censura ou embaraço *a priori*, seja legislativa, seja judicialmente intentada. As relações de imprensa prevalecem como superiores bens jurídicos, com as demais relações surgindo como eventuais responsabilizações ou consequências do pleno exercício dessa liberdade.

O art. 19 do Pacto Internacional sobre Direitos Civis e Políticos, ao qual o Brasil aderiu em 24 de janeiro de 1992, garante a todos o direito de ter opiniões, sem interferência. O seu § 2º protege o direito de todos de buscar, receber e disseminar informações e ideias de todos os tipos, independentemente de fronteiras, por qualquer meio de comunicação. Restrições a esse direito devem ser previstas por leis, se necessárias e proporcionais para proteger direitos de terceiros, segurança nacional, ordem pública ou saúde e moral pública.

É evidente a existência de diretrizes relevantes na Constituição brasileira para assegurar a proteção especial aos jornalistas.

A vigilância, especialmente aos jornalistas, tem profundas implicações para a liberdade de expressão, criando incentivos para autocensura e prejudicando a capacidade dos profissionais de conduzir investigações e de manter relacionamentos com fontes de informação de maneira segura.

O *Relatório Especial da ONU sobre Liberdade de Expressão* de 2017 destacou os efeitos prejudiciais da vigilância sobre jornalistas, exemplificados pelo uso do software Pegasus, no México. A vigilância digital desses jornalistas é um problema grave no contexto atual e, pelo menos, 180 jornalistas em todo o mundo foram espionados com o software Pegasus. Isso foi revelado pela *Forbidden Stories* e é o que a gente sabe.

A gravidade é ainda maior quando consideradas as interseccionalidades de raça e gênero, que aqui também estão presentes.

Em 2021, por exemplo, a Unesco realizou uma pesquisa com 901 jornalistas em 125 países, por meio de entrevistas conduzidas em 5 idiomas. Das jornalistas entrevistadas, 18% revelaram ter sofrido vigilância digital, um indicativo do alto risco à segurança dessas profissionais e de suas fontes confidenciais.

Embora o desejo de provas substanciais e investigações criminais também possa estimular o desejo de acesso ao trabalho dos jornalistas por meio dessa vigilância direcionada, a Relatoria Especial da ONU para a Liberdade de Expressão já afirmou que essas alegações são quase sempre infundadas e exageradas e podem servir de pretexto para enfraquecer o jornalismo e suprimir as vozes dissidentes.

O risco é muito alto.

Consideramos que, na ausência de uma regulação específica sobre sistemas de vigilância direcionados, é necessário vedar o uso de ferramentas de vigilância digital contra jornalistas.

Isso não implica, de nenhuma forma, outros processos legais legítimos, incluindo a vigilância não digital, mas reconhece o caráter invasivo das

tecnologias de vigilância digital, a dificuldade de segregar um ou outro elemento do conjunto de usos de dispositivos digitais por jornalistas e o potencial dos abusos.

O Artigo 2º do Pacto Internacional sobre Direitos Civis e Políticos impõe aos Estados a obrigação de respeitar, de garantir os direitos reconhecidos no Pacto, incluindo a prevenção, investigação, punição e reparação de abusos de direitos humanos por terceiros. Os princípios orientadores sobre empresas e direitos humanos na ONU instam os Estados a exercer supervisão adequada para cumprir suas obrigações internacionais de direitos humanos quando contratam ou legislam para empresas prestarem serviços ou fazem licitações para empresas prestarem serviços que podem impactar o usufruto dos direitos humanos.

A utilização de ferramentas de intrusão virtual e o monitoramento secreto por parte do Estado levanta várias e sérias questões sobre sua constitucionalidade.

Mesmo que esta Corte considere, Ministro, a possibilidade de uso dessas tecnologias em alguns casos, é imperativo que seja reconhecido o potencial impacto na liberdade de expressão, na liberdade de imprensa e na proteção do direito constitucional dos jornalistas de manter o sigilo da fonte, caso estes profissionais de alguma forma não sejam resguardados.

Nós defendemos que essas ferramentas não devem ser utilizadas contra jornalistas em nenhuma situação. A proteção demandada aos jornalistas em nada deve parecer estranha a esta Corte, que, seguidas vezes, reafirmou a liberdade de expressão e de acesso à informação como fundantes do Estado Democrático de Direito.

Estou aqui, portanto, como Diretora de Promoção da Liberdade de Expressão, representando a Secretaria de Políticas Digitais, comprometida em cumprir nosso papel de incentivar um ambiente de liberdade de expressão para desenvolvimento do jornalismo profissional.

Nosso objetivo é reforçar a importância do entendimento desta Suprema Corte, que tem sido firme no trabalho de defesa das instituições, de que a proteção aos jornalistas, enquanto categoria que materializa a ideia imprensa, é essencial para a defesa da democracia.

Agradecemos o espaço privilegiado concedido para essa discussão, reafirmamos nosso compromisso com a promoção da liberdade de expressão e proteção dos direitos fundamentais essenciais para o fortalecimento das nossas instituições democráticas.

Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Samara!

Convido agora para falar o Doutor Wesley Vaz, Secretário de Controle Externo de Governança, Inovação e Transformação Digital do Estado, no Tribunal de Contas da União. É professor da Fundação Dom Cabral, possui certificado executivo em estratégia e inovação pelo MIT e mestrado em ciência da computação pela Unicamp.

Doutor Wesley, tenha a palavra, por gentileza.

O SENHOR WESLEY VAZ (TRIBUNAL DE CONTAS DA UNIÃO - SECRETARIA DE CONTROLE EXTERNO DE GOVERNANÇA, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL DO ESTADO) - Muitíssimo obrigado! Queria saudar o Excelentíssimo Ministro Zanin, Relator desta ADPF 1.143, a Excelentíssima Subprocuradora-Geral da República, Doutora Elizeta, o Doutor Marcelo Turbay, a Doutora Carolina Lima, o Doutor Lucas Sales, Senhoras e Senhores, autoridades presentes.

Uma satisfação estar aqui em nome do Tribunal de Contas da União, nessa brevíssima fala, em que pretendo explicar a todos a atuação do TCU, desde o ano de 2020, associada à fiscalização de sistemas de coleta, acesso e análise de dados para atividades de inteligência e segurança pública no país.

Antes de falar dos casos concretos, Excelentíssimo Ministro, gostaria de ressaltar que há em comum, nesses casos, três pontos cobrados do TCU para essas fiscalizações.

O primeiro deles: os aspectos de contratações dessas ferramentas pelas empresas e órgãos públicos. O segundo: a finalidade do uso dessas ferramentas pelos agentes públicos. E o terceiro, e talvez o mais importante de todos: os tipos de controles existentes para que essa ferramenta seja utilizada segundo a sua finalidade, tentando manter algum tipo de auditabilidade e rastreabilidade do seu próprio uso.

Como disse, são cinco processos já encerrados no Tribunal de Contas desde o ano de 2020. Queria falar brevemente sobre cada um deles e ressaltar que há outros dois processos, Senhor Ministro, ainda em apreciação no Tribunal de Contas da União sobre o tema.

O primeiro deles se trata de uma análise sobre uma licitação para um tipo de serviço de solução de coleta e análise desse tipo de dados, em que o edital foi revogado a partir da representação do TCU. Um julgamento, portanto, por perda de objeto no ano 2020 - Acórdão nº 1.525, para quem tiver interesse, do ano 2020, TCU, Plenário.

O segundo processo também é avaliar uma licitação para um programa específico de análise, acesso e coleta de informações dessa natureza, que gerou o Acórdão nº 1.331, de 2022. O Tribunal de Contas, a partir dessa decisão, determinou que fizesse constar do contrato e dos modelos de contrato desta

natureza, critérios e funcionalidades de segurança e auditabilidade, de modo que nós, enquanto Estado, possamos entender claramente o que cada agente público faz e vinculado a que tipo de processo faz algum tipo de análise desse tipo de sistema.

No ano de 2021, a partir do Acórdão nº 1.353 do ano seguinte, 2022, o Tribunal de Contas deu ciência de irregularidade na habilitação de algumas empresas associadas à contratação de soluções de inteligência em fontes abertas, mídias sociais, *deep* e *dark web*. Esse é um outro foco da atuação do Tribunal de Contas da União: identificar irregularidades na habilitação dessas empresas e fazer com que essas irregularidades sejam sanadas.

Por meio do Acórdão nº 180, de 2023, o TCU também decidiu, mediante a análise de um pregão para a contratação de solução de TI, de comunicação e de coleta de dados, que não houve evidência de direcionamento nem vedação de manifestação de participantes no caso em questão. Faz mais uma vez referência a uma contratação específica desse tipo de ferramenta.

E, por último, em acórdão mais recente, o Acórdão nº 1.529, de 2022, do TCU, Plenário, avaliou o suposto uso indevido de um sistema de informação por meio de um órgão público. O que se avaliou nesse acórdão é que não houve a evidência de desvio de finalidade no caso concreto, porém se

identificou a necessidade de recomendar ao órgão que se colocasse, se inserissem controles no sistema, de modo a que, mais uma vez, Senhoras e Senhores, possamos estar diante do uso responsável desse tipo de sistema por meio da auditabilidade, por meio de o Estado conseguir saber o que é feito em cada um desses casos.

Ressalto também que há outros dois processos ainda em andamento no Tribunal de Contas da União, de modo que não consigo ter uma posição definitiva sobre a decisão, obviamente, mas que tratam exatamente do mesmo objeto e que, na nossa percepção, estudando a jurisprudência do Tribunal de Contas da União sobre essa temática, não vai deixar de refletir sobre os controles internos e os controles de aplicação absolutamente necessários para o uso desse tipo de sistema. Entende-se que é necessário pensar as maneiras, quando necessário usar esse tipo de sistema, quando tenhamos o Estado utilizando. Sempre vinculando a uma finalidade de interesse público, sempre vinculando a um caso concreto, sempre vinculando ao agente público responsável por isso e ter todo esse processo rastreável e disponível para as autoridades que necessariamente vão fazer uso desse tipo de informação em sede de eventual corregedoria ou coisa do gênero.

Como disse, muitíssimo breve a minha fala, fazendo esse pequeno resumo da jurisprudência do Tribunal referente à contratação e uso de sistemas de coleta, extração e análise de dados por parte das instituições de

inteligência e de segurança pública. Reforço basicamente a forma de atuar do TCU, que é tentar identificar um conjunto de riscos para a operação e sugerir e recomendar a implementação de controles que possam mitigar esse risco, sem, obviamente, deixar de, quando identificada uma irregularidade, atuar sobre ela, determinando sua imediata aderência ao processo legal.

É isso, Senhor Ministro, muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Wesley, pela exposição.

Convido agora a Doutora Bárbara Simão, Coordenadora de Pesquisa na Área de Privacidade e Vigilância do InternetLab, mestre em Direito e Desenvolvimento pela Fundação Getúlio Vargas, graduada pela Faculdade de Direito da Universidade de São Paulo. Já atuou como pesquisadora na área de direitos digitais do Instituto Brasileiro de Defesa do Consumidor - IDEC, e foi conselheira do projeto Proteção de Dados em Serviço de Saúde Digital da Fiotec, Fiocruz.

Doutora Bárbara, tenha a palavra.

A SENHORA BÁRBARA SIMÃO (ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA) - Muito bom dia!

Excelentíssimo Ministro Cristiano Zanin, demais presentes, prezados colegas, queria iniciar agradecendo a possibilidade de participação nesta

audiência pública em nome do InternetLab - centro independente de pesquisa interdisciplinar que promove o debate acadêmico e a produção de conhecimento nas áreas de Direito e tecnologia. Atuamos como ponto de articulação entre acadêmicos e membros dos setores público, privado e da sociedade civil, incentivando o desenvolvimento de projetos que abordem os desafios na elaboração, implementação de políticas públicas em novas tecnologias e questões relacionadas à privacidade, liberdade de expressão, gênero e identidade.

Anualmente, também organizamos o Congresso de Direitos Fundamentais e Processo Penal na Era Digital, que visa justamente a promover o debate em relação às novas capacidades de investigação do Estado geradas pelas novas tecnologias e a manutenção das garantias penais e fundamentais de todos os cidadãos.

A ação que discutimos aqui hoje visa a dar efetividade plena e conferir proteção eficaz aos mandamentos contidos no art. 5º, X, XII e LXXIX, da Constituição Federal, diante dos recentes avanços tecnológicos que culminaram na proliferação global de ferramentas de intrusão virtual. Essas ferramentas têm sido utilizadas por serviços de inteligência, órgãos de repressão estatais e de defesa nacional e promovem uma vigilância remota, secreta e invasiva dos dispositivos eletrônicos. Elas permitem que um agente obtenha acesso clandestino às comunicações digitais, o que engloba produtos de trabalho, dados de navegação,

pesquisas, históricos de localização e atividades *on-line* e *off-line* dos indivíduos. São as ferramentas mais intrusivas que existem à disposição do Estado. Por conta disso, não podem simplesmente ser equiparadas à interceptação telefônica ou à invasão de domicílio, dado que o grau de intrusividade da medida sobre a vida privada pode ser inclusive considerado pior. Informações de um dispositivo eletrônico podem revelar aspectos profundos da identidade de seu titular, desde moradia, costumes, renda, pessoas com quem se relaciona. Compõem um retrato abrangente da vida privada desse indivíduo, que engloba hábitos de vida, interesses, associações familiares ou religiosas, coisas que podem não ter nenhuma relação com uma investigação que esteja em curso.

O arcabouço normativo hoje vigente na legislação brasileira diz que toda interceptação, requisição, compartilhamento e quebra de sigilo de dados deve ter fundamentação clara, tanto no respeito à letra da lei quanto na justificativa que se chega após o sopesamento entre o interesse público na investigação criminal e os riscos que se apresentam às garantias fundamentais do titular de dados.

Vale mencionar também a adesão do Brasil ao Pacto de Direitos Civis e Políticos e ao Pacto de São José da Costa Rica, que defendem a liberdade de opinião e expressão e que definem que restrições a esses direitos devem obedecer a um teste tripartite, no qual o primeiro critério deve ser a legalidade da medida, o

segundo, a necessidade e proporcionalidade da medida e terceiro, a necessidade para que se alcance um objetivo legítimo.

O Estado, portanto, tem o ônus de provar uma conexão direta e imediata entre uma possível ameaça e a restrição a esses direitos e de impor também um instrumento menos intrusivo a esses direitos.

No que toca ao acesso a dados associados às comunicações, relatórios de liberdade de expressão das Nações Unidas e da Comissão Interamericana de Direitos Humanos já afirmaram que vigilância massiva não atende ao critério da proporcionalidade, mesmo que sirva a um propósito legítimo.

Cabe questionar, portanto, quando e se a utilização de *spywares*, ferramentas de vigilância direcionada pelo Estado, poderia ser considerada proporcional diante do direito humanitário. Para isso, vou dar um passo atrás e dizer que o mercado de *spywares* e de ferramentas direcionadas opera a partir de uma lógica de vulnerabilidades nos sistemas de informação. São descobertas e exploradas vulnerabilidades nos sistemas eletrônicos, nos softwares e nas redes de infraestrutura de telecomunicações. Ao comprar, adquirir ou usar de qualquer maneira essas ferramentas, o Estado está, portanto, explorando um mercado que cria vulnerabilidades nas comunicações e sistemas informacionais de todos os cidadãos. Isso possui um impacto sobre o ambiente democrático.

Essas vulnerabilidades colocam em risco a segurança dos usuários e de toda cadeia de uso da infraestrutura das comunicações. Isso inclui também setores econômicos, como empresas financeiras e de saúde, nas quais a necessidade de segurança no tráfico de informações é de importância vital para a existência confiável desse mercado.

Frise-se que a falha em se reparar uma vulnerabilidade no sistema não afeta unicamente uma pessoa que, eventualmente, esteja sendo investigada, mas todo um sistema produtivo que depende da confiança nessas informações para que suas operações sejam realizadas.

Diante de um cenário normativo institucional em que vulnerabilidades não só existem, mas são incentivadas economicamente pelo Estado, a gente tem afetada a qualidade do nosso debate público e a confiança nas instituições democráticas, pela possibilidade de usos que fujam aos limites da legalidade, ética e proporcionalidade na Administração Pública e, não apenas por isso, mas pelos possíveis efeitos inibidores que o uso dessas tecnologias possui sobre a liberdade de expressão.

Os casos ocorridos no Brasil e no mundo evidenciam como o aparato de vigilância do Estado, quando não limitado e condicionado a regras estritas, pode ser desvirtuado. Em vez de servir para fins institucionais lícitos, como combate a crimes graves, pode ser usado para fins individuais e até mesmo de

perseguição política que ameacem o Estado Democrático de Direito e os princípios da impessoalidade e legalidade na Administração Pública.

A legitimação do uso indiscriminado dessas ferramentas impõe um ambiente de desconfiança nas instituições democráticas, uma vez que privacidade e liberdade de expressão estão diretamente relacionadas. A vigilância estatal, sem controle ou justificativa, possui impacto prejudicial sobre o comportamento humano. A privacidade, portanto, possui uma relevância de natureza social e política, sendo um componente crucial nos sistemas democráticos.

Nesse sentido, efeitos inibidores relacionados às capacidades de vigilância do Estado e à liberdade de expressão têm sido estudados e evidenciados há bastante tempo. A ausência de parâmetros legais evidentes e de critérios específicos que orientem as atividades autoridades públicas torna a capacidade de uso dessas ferramentas absolutamente discricionário. Na medida em que esse cenário ocorre, o ambiente democrático já é afetado.

Um ambiente de insegurança coletiva e de desconfiança nas instituições de segurança pública e defesa por sua vez também é nocivo a qualquer democracia moderna, que depende dessas instituições para sua continuidade.

Como consequências, então, da utilização reiterada dessas ferramentas, temos efeitos nocivos ao ambiente democrático, seja pelo impacto na segurança das informações, seja pelo impacto inibidor na liberdade de expressão e

na confiança nas instituições, seja pela possibilidade de usos que rompam com os limites da impessoalidade da Administração Pública. É preciso, portanto, que a gente pense no dever do Estado de proteção desse ambiente informacional.

Em diversos momentos, o Supremo Tribunal Federal já teve a oportunidade de reforçar esse dever do Estado de não enfraquecer a segurança da comunicação entre seus cidadãos e, assim, assegurar uma infraestrutura democrática no debate público.

Na ADPF 722, de relatoria da Ministra Cármen Lúcia, em seu voto, ela ressaltou que o serviço de segurança do Estado não pode ser desempenhado fora dos estritos limites constitucionais e legais, sob pena de comprometer a democracia em sua instância mais central, que é a de garantia dos direitos fundamentais.

Já na ADPF 403 e na ADI 5.527, ambas julgadas em conjunto, que questionam o art. 12 do Marco Civil na Internet, mas cuja questão de fundo é a utilização de criptografia de ponta a ponta, votos importantes já foram emitidos no sentido de que existe um dever do Estado de proteção de um ambiente informacional e de comunicação entre seus cidadãos.

No voto da então Ministra, Rosa Weber, ela afirmou que o Estado não pode compelir o aplicativo a oferecer serviços de forma menos segura,

com o pretexto de usar essa vulnerabilidade para acessar dados e investigações criminais.

Já no voto do Ministro Edson Fachin, ele afirmou ser necessário afastar qualquer interpretação do dispositivo que autorize ordem judicial, que exija acesso excepcional ao conteúdo de mensagem criptografado de ponta a ponta, ou que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações na internet. Fato é que essas ferramentas que discutimos aqui hoje enfraquecem a proteção de aplicações na internet.

Aqui, parto para uma conclusão: nesse sentido, já há inúmeras outras técnicas e ferramentas de investigação menos gravosas que a invasão direta a um dispositivo eletrônico à disposição do Estado.

Diante da profusão de novos meios de obtenção de provas, é possível identificar a autoria de crimes por meios ordinários de investigação, inclusive, por meio de procedimentos menos restritivos de direitos dos que os que estamos mencionando aqui.

Cabe, então, a reflexão sobre se o uso dessas ferramentas poderia ser considerado necessário e proporcional em qualquer caso, diante dos impactos que eles possuem nos sistemas de informação e na própria democracia brasileira, ou se deveriam ser considerados como possuidores de um risco excessivo, levando-

se a dizer que seria, talvez, melhor não termos essas ferramentas em nosso ambiente normativo-institucional.

Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Bárbara Simão!

Passo a palavra agora ao Doutor Pedro José Nasser Saliba, Coordenador de Assimetrias e Poder da Data Privacy Brasil, advogado e sociólogo, mestre em sociologia e antropologia pela PPGSA - UFRJ, pesquisador em intersecção entre proteção de dados pessoais e Poder Público, especialmente na área de segurança e vigilância. Foi pesquisador do Laboratório de Estudos Digitais (LED-UFRJ) e atualmente trabalha como Coordenador de Assimetrias e Poder na Data Privacy Brasil.

Doutor Pedro, tem a palavra.

O SENHOR PEDRO JOSÉ NASSER SALIBA (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA – DATA PRIVACY BRASIL) - Muito obrigado!

Bom dia a todas as pessoas aqui presentes!

Eu gostaria de parabenizar o Supremo Tribunal Federal, na figura do Ministro Cristiano Zanin, pela realização da presente audiência pública, de temática urgente em nosso país.

Agradecemos também a Procuradoria-Geral da República pelo ajuizamento da presente lide, provocando a interpretação constitucional do tema.

Saúdo também os e as colegas presentes aqui na mesa para o debate sobre a interpretação da nossa Constituição frente a novas tecnologias digitais, celebrando a democracia brasileira.

A Data Privacy Brasil é uma organização que nasce da parceria entre uma escola e uma associação, com o objetivo de fomentar a cultura de proteção de dados e de direitos digitais. Contamos com uma equipe multidisciplinar e oferecemos formações, eventos e pesquisas de interesse público e auditorias cívicas. São iniciativas que buscam promover os direitos digitais e direitos fundamentais, além dos valores ligados à justiça social, diante de tecnologias contemporâneas e processos de datificação.

Desde 2020, nós trabalhamos com pesquisas de interesse público sobre o tecnoautoritarismo. Nós analisamos o estado da arte científica no Brasil e no mundo, trabalhando com material de referência, como relatórios técnicos,

vídeos informativos e, inclusive, uma série de reportagens em parceria com veículos de mídia.

Na esfera judicial, nós atuamos como *amicus curiae* na ADI 6649, sobre o decreto que criava o Cadastro Base do Cidadão e regras de compartilhamento de dados no Governo Federal, e na ADI 6387, que questionava o compartilhamento de dados de usuários de telecomunicações com o IBGE.

Conforme o Professor Ingo Sarlet, o tecnoautoritarismo pode ser definido como a utilização cada vez mais massiva de recursos de tecnologia da informação e comunicação digital para o controle de indivíduos e grupos pelo Estado. Não se trata de um fenômeno exclusivo de estados ditatoriais. Tais tecnologias são frequentemente adotadas em diversos países, minando a democracia a partir da confiança que os cidadãos e as cidadãs têm sobre o Estado nacional.

Ao longo desses quatro anos, nós atuamos em diversos episódios que foram decisivos sobre o uso dessas tecnologias no contexto político brasileiro.

No caso Pegasus/Harpia Tech, nós percebemos uma confusão entre *spywares* e *OSINTS*, sendo necessário reforçar essas diferenças entre tais categorias. Enquanto o Pegasus era um *software* capaz de monitorar informações de

celulares em alvos, o Harpia Tech apresentava recursos que coletavam de forma automatizada milhares de informações públicas na internet para a criação de perfis de alvos e monitoramento de seus rastros *on-line*.

O caso da Abin/Denatran, sobre o pedido da agência de CNHs de todo o país, mostrou-nos riscos agudos no uso secundário de dados sem devidos parâmetros constitucionais, ainda que utilizados por agências de inteligência.

Em 2022, no caso Excel, isso nos mostrou riscos ao devido processo na extração de dados de dispositivos. Os fatos apontam para a criação de zonas cinzentas no devido processo, permitindo que autoridades administrativas pudessem decidir sobre a extração de dados em dispositivos sem autorização judicial.

Em conjunto com outras organizações, nós atuamos em inquérito civil exigindo freios e contrapesos aos softwares de extração em dispositivos, além de arranjos institucionais que garantissem os princípios da necessidade, legalidade e proporcionalidade em tais operações.

Mais recentemente, o FirstMile aponta outros cenários de risco. Por ser um software que explora vulnerabilidades em protocolos de telecomunicações, a sua aquisição pelo Estado brasileiro viola não apenas normas constitucionais de privacidade, de proteção de dados e autodeterminação

informativa, mas também normas do setor de telecomunicações, direitos de livre associação, liberdade civis e políticas.

Evidências do uso desse software foram identificadas no Mianmar e no Sudão, culminando, inclusive, em monitoramento massivo e prisões.

Atualmente, nós trabalhamos com o tema de *spywares* na iniciativa de defesa digital, um projeto junto ao Internet Lab, para promover um debate qualificado sobre ferramentas de vigilância, trazendo elementos que possam fortalecer o debate e proteger direitos constitucionalmente garantidos à proliferação, sem controle, dessas ferramentas em nosso país.

O relatório Mercadores da Insegurança, do IP.rec, organização que também estará presente nessa audiência, aponta 209 documentos contratuais relativos a *spywares* na Administração Pública.

Trata-se do material de referência sobre esse tema, e destacamos algum de seus achados aqui nessa tabela. Seu material será referenciado, aqui, em nossa petição, enquanto *amicus curiae*.

Diante dos casos expostos, fica evidente a relevância jurídica do debate de *spywares*. Eles podem ser definidos como programas com capacidades intrusivas de extração de informações e invasão em dispositivos ou sistemas eletrônicos. O seu objetivo é explorar falhas de segurança existentes para a coleta de informações sobre seus alvos, que dificilmente conseguem identificar a invasão.

Na literatura especializada, eles também são conhecidos pelo fenômeno de *hacking* governamental. A sua proliferação é cada vez maior ao redor do mundo, especialmente através da aquisição de ferramentas desenvolvidas e comercializadas por empresas privadas.

Apesar de afirmarem o seu uso lícito, a Relatoria Especial da ONU sobre Contraterrorismo e Direitos Humanos aponta que a proliferação, sem salvaguardas, dessas tecnologias foi utilizada para perseguir jornalistas, ativistas, oposição política e mesmo cidadãs e cidadãos.

Podemos separar as diferentes modalidades de *spywares* a partir de suas características e capacidades, auxiliando a identificar os riscos que cada um promove aos direitos fundamentais, bem como formas de controle necessárias para a ação estatal.

No Brasil nós temos dezenas de exemplos que precisam ser analisados em detalhe, inclusive considerando quais órgãos detêm as ferramentas, ponderando se elas estão de acordo com as suas competências legais.

Com base no extenso levantamento do IP.rec, nós desenvolvemos uma tipologia de análise de impacto a direitos fundamentais.

Eu destaco que essas tipologias que nós vamos apresentar aqui são utilizadas, mais de uma vez, em cada ferramenta. Então, diferentes ferramentas podem ter mais de uma dessas categorias que nós trabalhamos.

A primeira que nós destacamos são softwares de extração de dispositivos que são capazes de extração lógica e física em dispositivos eletrônicos, sejam celulares, computadores, cartões SIM, SD, entre outros. Isso significa que podem extrair todo o sistema de arquivos ou, mesmo, arquivos selecionados de acordo com a aplicação utilizada, como redes sociais, aplicações de mensageria, navegadores, entre outros. Trata-se da maior parte dos contratos localizados pelo IP.rec, sendo utilizados por uma gama de órgãos públicos ao redor do país. Esses dispositivos exigem a presença física do aparelho e precisam de salvaguardas específicas para garantia do devido processo legal, especialmente no que tange à cadeia de custódia.

A segunda categoria que nós trazemos são *spywares* de exploração de infraestrutura, que utilizam a invasão em infraestrutura de redes públicas ou privadas por meio de falhas em protocolos, que deveriam ser compartilhados apenas por operadoras de telecomunicações. Um exemplo dessa categoria é a ferramenta FirstMile, capaz de monitorar a movimentação de até 10 mil alvos. Outro de destaque é o GI2, que é capaz, inclusive, de ativar microfones remotamente e identificar a localização desses alvos. Ambas são da empresa Cognite. E há relato de uso para monitorar autoridades, jornalistas e Ministros do STF.

Um outro exemplo foi a denúncia de monitoramento de servidor do Ibama responsável por ações de combate ao garimpo ilegal na Amazônia.

Nós trazemos, também, software de derrubada de chaves criptográficas que rompem os mecanismos de defesa de dispositivo. Outro também sobre infração de informações deletadas que recuperam arquivos que foram deletados em dispositivos. Extração de sistemas em comunicação em nuvem que são capazes de extrair dados de ferramentas como Facebook, Google, iCloud.

E outro também que nós destacamos é uma categoria que extrai informações por inferência. Essas ferramentas têm um grau invasivo altíssimo. Elas são capazes de processar dados, gerando informações novas em análises complexas a partir das informações coletadas nos dispositivos. Elas podem reconhecer padrões em mensagens de aplicação e mesmo fotos, reconhecendo pessoas, frequências de encontros e contatos, além de unificar seus bancos de dados. Seus critérios são opacos e podem criar enviesamentos nas investigações, além de automatizar ainda mais a vigilância de indivíduos e grupos sociais. Pode ser especialmente perigoso para a perseguição por motivação política ou outros marcadores sociais. Nos casos de reconhecimento facial, a literatura recente demonstra que existem vieses incorrigíveis nos códigos capazes de perpetuar crimes raciais a partir da tecnologia. São as ditas tecnologias mais avançadas, mas com risco altíssimo na sua utilização e controle.

Além da tipologia apresentada, nós destacamos três categorias importantes para análise: *spywares* de análise física, remota e esse de inferências. Nas análises físicas, as pessoas investigadas muitas vezes têm conhecimento da apreensão, cabendo maior controle da atividade estatal. Isso não acontece em invasões remotas, quase indetectáveis. Por fim, as inferências, como eu trouxe anteriormente, criam uma camada adicional de inteligência, mas a sua falta de transparência pode levar a interpretações equivocadas.

Diante do exposto, recomendamos à Corte um exame de proporcionalidade e razoabilidade sobre a aquisição, desenvolvimento e uso de *spywares* pelo poder público brasileiro, considerando as competências legais dos órgãos, capacidades técnicas das ferramentas e o reconhecimento das múltiplas violações de direitos fundamentais que podem trazer. A apresentação da tipologia tem como objetivo balizar o debate, apontando a gradação de riscos considerados no potencial de invasão massiva de direitos dessas ferramentas, especialmente no protocolo de comunicação e extração remota de informações.

Eu agradeço e até a próxima.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Pedro José Nasser Saliba.

Eu convido agora a Doutora Raquel Saraiva para fazer uso da palavra. A Doutora Raquel Saraiva é presidente do Instituto de Pesquisa em Direito

e Tecnologia do Recife, IP.rec, é presidente e fundadora do IP.rec, é graduada em Direito pela Universidade Católica de Pernambuco, Mestre em Ciência da Computação pela Universidade Federal de Pernambuco. No IP.rec, atua principalmente nas áreas de privacidade e vigilância, com foco no Observatório da Criptografia e regulação de plataformas digitais, mas também se interessa pelas discussões sobre gênero e tecnologia.

A Doutora Raquel Saraiva tem a palavra.

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) - Muito obrigada, Ministro Cristiano Zanin.

Bom dia a todas e todos.

Cumprimento as autoridades aqui presentes na pessoa do Excelentíssimo Ministro Cristiano Zanin, Relator desta ADPF, saudando pela iniciativa também de abrir o espaço para ouvir os representantes da sociedade civil, interessados e especialistas no tema aqui discutido.

O Instituto de Pesquisa em Direito e Tecnologia do Recife, IP.rec, é uma organização sem fins lucrativos que, desde 2017, atua na realização de pesquisa científica, incidência política, capacitação e comunicação, focado nos impactos sociais, éticos e jurídicos do desenvolvimento tecnológico. Dentre os diversos temas de interesse do IP.rec, estão questões envolvendo privacidade e

vigilância. Buscamos, nesses sete anos de atuação, investigar, partindo de um olhar do sul global e nordestino, temáticas como proteção de dados pessoais, criptografia e a prática do *hacking* governamental, que será o foco desta exposição.

As revelações do Edward Snowden em 2013 apresentaram um cenário alarmante no que tange à corrosão da privacidade e ao poder da vigilância de entes estatais. Como consequência dessas revelações, serviços avançaram na adoção de criptografia de ponta a ponta como forma de proteger seus usuários e ativos contra o poder de vigilância do Estado. Apesar de reforçarem a narrativa de que a criptografia impede a investigação das forças policiais, é importante reforçar que o poder investigativo avançou na mesma proporção.

Assim, defendemos a criptografia como ferramenta essencial para a garantia do direito à privacidade, diante da atual conjuntura de vigilantismo posta, além de fortalecer uma gama de outros direitos humanos, conforme dados reforçados por relatórios da ONU, pesquisas acadêmicas e da sociedade civil e ações de coalisões, como a Global Encryptions Coalition, à qual o IP.rec integra, assim como pelos materiais produzidos pelo Observatório da Criptografia, um projeto conduzido também pelo IP.rec.

No nosso estudo *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil*, já referido aqui anteriormente, buscamos contribuir, com os estudos, para o tema do *hacking* governamental, que conceitualizamos como

a exploração intencional, ou não, por agentes do Estado de vulnerabilidades em sistemas informáticos. Como consequência, forma-se um ecossistema de vulnerabilidades, colocando a segurança cibernética de cidadãos e nações em risco. Empresas surgem, nesse mercado de insegurança, pagando altas quantias para vulnerabilidades descobertas, as quais são posteriormente vendidas para empresas de vigilância ou para Estados ricos que podem explorá-las.

Paralelamente, esses Estados, notadamente no norte global, geralmente detêm também a capacidade de encontrar e desenvolver a exploração de tais vulnerabilidades. Nessa rede, empresas com alto valor, alto poder de intrusividadade e vigilância ganharam notoriedade no debate público, dentre elas a NSO Group, empresa israelense desenvolvedora do *spyware* Pegasus. Esse tem capacidade de infectar dispositivo sem o conhecimento do alvo, transmitindo toda a informação do aparelho do alvo para o espião. Graças ao seu poder, o Pegasus foi adquirido por diversos governos autoritários ao redor do mundo para reprimir e perseguir dissidentes políticos, jornalistas, ativistas e pessoas LGBTQIA+, sendo alvo de denúncias de organizações de direitos humanos, ativistas em privacidade e entes governamentais.

Outro exemplo de ferramenta de vigilância em massa são as produzidas pela Cognyte, responsável por duas ferramentas presentes no Brasil, a GI2 e FirstMile, ambas com capacidade de identificação de geolocalização de alvos.

A última foi o pivô no caso da chamada Abin paralela, no qual autoridades, jornalistas e adversários políticos do governo anterior tiveram sua localização espionada.

O foco excessivo dado no avanço do Pegasus ofuscou a capilaridade de outras ferramentas de diferente poder intrusivo, mas igualmente preocupantes. Hoje, ferramentas de extração de dados em massa de dispositivos informáticos dominam secretarias estaduais, órgãos federais e estão presentes em todos os estados federativos, incluindo órgãos que, a princípio, não teriam competência investigativa, como secretarias da fazenda de alguns estados, conforme aponta também nossa pesquisa.

Dentre essas ferramentas em extração em massa, destacamos o avanço de outra empresa de israelense, a Cellebrite. Essa desenvolveu o UFED Touch, responsável pela extração de dados em massa de dispositivos que estão em posse do usuário da ferramenta. Igualmente as ferramentas anteriores, o Cellebrite está envolvido em controvérsias no que concerne aos direitos humanos e vem sendo o principal fornecedor de soluções para as forças de investigação brasileiras.

Considerando tal similaridade de abuso, de vulnerabilidades e diferença de intrusividade, propomos, no estudo diferenciação do *hacking* governamental remoto e com o dispositivo em mãos. A primeira tipologia envolve a utilização de *spyware* de soluções, na qual o agente de Estado não necessita ter em

mãos o dispositivo para abusar das vulnerabilidades do sistema, como é o caso do Pegasus e do FirstMile. No segundo caso, o agente necessita ter a posse do dispositivo para extrair os dados desejados, como o caso do Cellebrite e outras soluções forenses. Não obstante essa diferenciação, ambas representam erosão na privacidade e na cibersegurança. Um dos pontos de riscos postos foi o da proteção de dados pessoais, que foi elevado a direito fundamental pela Emenda Constitucional nº 115.

A não aplicação da LGPD para fins de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais, conforme o disposto no art. 4º, IV, coloca cidadãos brasileiros em uma zona de incerteza, ainda que haja a salvaguarda da Constituição. Na prática, observa-se uma opacidade generalizada na forma como os dados coletados para fins de investigação utilizando ferramentas de monitoramento remoto e extração em massa estão sendo tratados, abrindo margens para abusos.

Um exemplo nítido de tal situação é o projeto Excel. Criado pela Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública, durante o Governo Bolsonaro. O projeto tinha como objetivo fornecer equipamentos de extração de dados em massa de dispositivos, como o Cellebrite, para as secretarias estaduais. Essas, em troca, enviaram os dados coletados para o Governo Federal. Não há transparência, no que concerne ao uso de tais dados, para

além de campanha publicitárias que indicam o número de crimes combatidos como consequência do projeto.

Consideramos, portanto, como ponto de partida haver necessidade de publicização do nível de capacidade intrusiva presente nos diversos órgãos de segurança no Brasil. Isso fornece ao debate público insumos de como melhor endereçar o tema, tendo em vista que as ferramentas possuem diferentes capacidades de intrusividade. Esse nível de transparência também é fundamental para a compreensão dos riscos que estão postos em nível de soberania nacional.

Terceirizar os serviços de inteligência por meio da aquisição desse tipo de ferramenta coloca a questão sobre quem tem acesso aos dados coletados. Não há garantia de que as empresas fornecedoras não tenham acesso aos dados tratados por suas soluções, o que pode representar um sério risco à soberania nacional visto que informações altamente sensíveis e sigilosas podem vir a ser acessadas por entes privados.

Hoje, tal opacidade se encontra amparada inclusive em dispositivos legais. O § 1º do art. 3º da Lei das Organizações Criminosas dispõe que, havendo necessidade justificada de manter o sigilo sobre a capacidade investigatória, poderá ser dispensada a licitação para serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia

judiciária, para rastreamento e obtenção das provas previstas nos incisos II e V, sendo estes a captação ambiental de sinais eletromagnéticos, óticos ou acústicos e interceptação de comunicações telefônicas e telemáticas.

Ademais, ter ciência das soluções adquiridas pelo Estado brasileiro possibilita que identifiquemos se o dinheiro público está sendo usado para adquirir ferramentas que estão sendo utilizadas para violações de direitos humanos. Algumas das ferramentas em funcionamento do Brasil têm elos conhecidos com regimes autoritários ou com violações de direitos. A Cellebrite está presente nos Estados Unidos e sendo utilizada para reprimir, sobretudo, infrações de menor potencial ofensivo cometidos por populações negras e latinas, além de haver casos de abuso no Paquistão. A Cognite forneceu seus serviços para a repressão no Sudão do Sul. Assim, é incompatível para uma nação democrática que respeita os direitos humanos realizar contratos com empresas que têm seu lucro pautado na opressão e na morte de pessoas.

Todos os pontos expostos aqui demonstram um cenário grave, opaco, que não apenas coloca em risco os direitos humanos, mas a segurança da internet como um todo.

Por tal razão, faz-se necessária a adoção de duas medidas urgentes. Primeiro, a aprovação de uma lei geral de proteção de dados pessoais

aplicável à segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão de infrações penais, cobrindo o vácuo legislativo deixado pela LGPD. E, dois, o banimento do uso dessas ferramentas ou, em ação alternativa, a adoção de medidas extremamente restritivas por meio de salvaguardas legais que garantam a estabilidade dos sistemas e os direitos humanos. Entre essas medidas devem estar a transparência na adoção das ferramentas, incluindo a apresentação periódica de relatórios de transparência que demonstrem como elas estão sendo usadas, a investigação das empresas desenvolvedoras e fornecedoras dessas ferramentas, a apresentação de relatórios de impacto à proteção de dados pessoais e a restrição no uso a tipos penais mais graves. Assim, podemos ter algumas mínimas garantias de que os direitos dos cidadãos e das cidadãs brasileiras estão realmente na centralidade da elaboração de políticas públicas.

Novamente, eu agradeço e me coloco à disposição para eventuais questionamentos. Obrigada.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Raquel Saraiva.

Agora fará uso da palavra o Doutor Hugo Alberto Lazar, que é bacharel em relações internacionais pela Universidade de Brasília, especialista em

política internacional pela Escola de Sociologia e Política de São Paulo, mestre em diplomacia e relações internacionais pela Schiller University, Londres; atuou na Agência Brasileira de Inteligência, Abin; foi coordenador-substituto na Coordenação de Contrainteligência, coordenador de análise de organizações criminosas do Departamento de Contrainteligência, coordenador de análise de segurança pública do Departamento de Inteligência, assistente-técnico do Departamento de Contrainteligência, coordenador da análise de inteligência estrangeira do Departamento de Contrainteligência, coordenador-geral de contraespionagem do Departamento de Contrainteligência, superintendente da Superintendência de Minas Gerais, adido civil de inteligência em Moscou, diretor do Departamento de Inteligência e é presidente da União dos Profissionais de Inteligência do Estado da Abin - Intelis.

Doutor Hugo Alberto Lazar tem a palavra, por gentileza.

O SENHOR HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA AGÊNCIA NACIONAL DE INTELIGÊNCIA - ABIN - INTELIS) - Bom dia, Excelentíssimo Senhor Ministro Cristiano Zanin, Relator da ADPF 1.143, autoridades presentes, Senhoras e Senhores.

Meu nome é Hugo Alberto Lazar e sou o presidente da Intelis, a União dos Profissionais de Inteligência de Estado da Agência Brasileira de Inteligência.

A Intelis vem a público reiterar a importância desta ADPF, que visa a regulamentar o uso de ferramentas de monitoramento de aparelhos eletrônicos por órgãos públicos e estabelecer balizas sistêmicas que afastem o risco de arbitrariedade no uso dessas ferramentas por agentes públicos.

Nesta apresentação, buscarei brevemente explicar o que é a nossa atividade e a importância desta ADPF para proteger as garantias fundamentais da cidadania e para atualizar e garantir a segurança jurídica da atuação legítima dos servidores públicos da Abin.

As relações sociais são cada vez mais fluidas e complexas. A realidade não é azul ou vermelha, preta ou branca. Estamos em um período cinzento ou incerto. Violência urbana em níveis crescentes, extremismo violento de diferentes matizes por todas as partes do mundo, desinformação amplificada pelas conquistas tecnológicas e elevado nível de competitividade entre as nações, impulsionando ações de espionagem e interferência externa são algumas das marcas desse quase um quarto de século.

A atividade de inteligência de Estado busca minimizar essas incertezas, inerentes a cenários complexos, tanto internos quanto externos. É uma

função de Estado que exige profissionalismo, ética e autonomia técnica. Essa atividade é praticada por todos os países democráticos.

No Brasil, cabe aos profissionais da Abin realizar essa complexa missão, desde informações confiáveis às altas autoridades sobre a pandemia à antecipação sobre os atos antidemocráticos de 8 de janeiro de 2023, a identificação e alerta sobre extremistas e terroristas, o acompanhamento e análise da criminalidade organizada, a garantia da confidencialidade dos dados da urna eletrônica, a prevenção e análise de ataques cibernéticos, o esquema de segurança do Concurso Nacional Unificado e a identificação de agentes clandestinos estrangeiros. Edward Snowden, na década passada, já alertava sobre a espionagem sofrida pela Presidente brasileira. Essas são algumas das atribuições e realizações da Abin nos últimos anos.

O Brasil possui uma legislação que regulamenta a atividade de inteligência. No entanto, é necessário aprimoramento para assegurar um controle mais efetivo, maior clareza nas atribuições e limites da atividade de inteligência.

A atividade de inteligência no Brasil não dispõe de um mecanismo de controle judicial prévio para ações operacionais, a exemplo das maiores democracias do mundo. Importa destacar que a inteligência não se confunde com investigação criminal. A polícia atua após a ocorrência de crimes e tem como foco buscar a atribuição da autoria. A inteligência busca antecipar fatos

e situações com potencial impacto à segurança de pessoas e instituições. Como exemplo já citado, a Abin foi uma das poucas instituições que alertou para os ataques de 8 de janeiro, pois possuía a atribuição de prevenir e informar autoridades a respeito dessas ameaças.

Na petição inicial, o Ministério Público Federal requer que o Congresso Nacional seja instado a legislar sobre limites ao emprego de *spyware*, *indicators* e dispositivos ou ferramentas de geolocalização por meio da rede celular.

Em relação às ferramentas tecnológicas em discussão, a Intelis defende a necessidade de melhor compreensão das particularidades das ferramentas, bem como do grau de invasão à privacidade, que são substancialmente distintos.

Inicialmente, cumpre esclarecer que, no âmbito de suas competências legais, a Abin utiliza ferramentas não intrusivas para a coleta de dados em fontes abertas e entende que essas atividades não se devem submeter a reserva de jurisdição. A agência vem aprimorando suas políticas e processos de controle de rastreabilidade para fins de prestação de contas acerca dessas atividades.

Em relação aos *spywares*, a Intelis entende que são programas maliciosos, usados para a coleta de informações e de comunicações privadas. Na atividade de inteligência, essas ferramentas poderiam ser usadas, por exemplo,

para identificar redes de relacionamento de suspeitos de atentados contra instituições democráticas e rastrear a infraestrutura empregada por grupos criminosos cibernéticos.

Em relação aos *IMSI-Catchers*, entendemos que são equipamentos que simulam torres de telefonia para atrair celulares de uma determinada área. Na inicial, o respeitável Ministério Público Federal não fez uma diferenciação importante dessas ferramentas. *IMSI-Catchers* podem ser ativos ou passivos. Os ativos possuem capacidade de quebrar a criptografia das comunicações, sendo invasivo como os *spywares*. O tipo passivo, contudo, apenas captura o identificador do celular, permitindo saber se um celular específico se encontra em determinada área. No caso passivo, um exemplo de uso para a inteligência de Estado está em determinar se existem aparelhos de celular não permitidos em uma área de segurança, como uma reunião de chefes de Estado.

A geolocalização de um alvo de inteligência é uma forma de vigilância eletrônica, realizada por meio do rastreamento de um aparelho celular. Essa vigilância permite identificar em tempo real onde a pessoa está, esteve ou que trajeto utilizou. Essas ferramentas, como a conhecida FirstMile, não capturam as comunicações privadas dos alvos, mas apenas os locais por onde aquele celular circulou. Na atividade de inteligência, a vigilância por geolocalização permitiria

determinar os trajetos, por exemplo, de um suspeito de integrar organização terrorista ou extremista.

No memorial por escrito, a Intelis analisa com maiores detalhes as balizas sugeridas pelo Ministério Público Federal e tece reflexões sobre a sua aplicação na inteligência de Estado. Como é possível proteger o Brasil da espionagem estrangeira, do terrorismo e do extremismo violento, sem executar ações de caráter sigiloso? As principais democracias do mundo organizam e regulam a questão do controle dos limites, das prerrogativas e especificamente do acesso aos dados pessoais de seus próprios cidadãos. Destaque-se que, na maioria dos casos, este controle judicial prévio para operações intrusivas se dá muitas vezes com a definição de juízos ou varas especializadas, como no caso da Espanha e da Argentina. As ferramentas aqui em discussão são essenciais para prevenir ameaças à segurança do Estado e da sociedade. Nossos adversários fazem uso desses sistemas, mas seu uso por agentes públicos deve ser rigorosamente controlado para evitar abusos.

A Intelis acredita que um controle judicial prévio das atividades de inteligência é necessário para garantir a segurança jurídica dos servidores de inteligência e a proteção dos direitos individuais. As leis devem proteger os brasileiros dos abusos, mas sem tornar disfuncional uma atividade essencial para a segurança nacional.

Concluo esta apresentação reforçando que a Intelis considera necessária, conveniente e oportuna a regulamentação do emprego, para fins de inteligência de Estado, de soluções que possam representar riscos aos direitos à privacidade e à inviolabilidade das comunicações. A Intelis considera também necessária a regulamentação da capacidade postulatória específica da Abin para provocar o Poder Judiciário, assim como vê como positiva a eventual criação de juízo especializado para conhecer de temas relativos à atividade de inteligência de Estado, o que induziria à prestação jurisdicional mais robusta e ao controle mais efetivo dos riscos relativos à proteção de direitos e garantias fundamentais.

Agradecemos a oportunidade de apresentar nossas considerações e estamos à disposição para contribuir com o aprimoramento da regulamentação das atividades de inteligência no Brasil.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Hugo Alberto Lazar, que fez agora a sua exposição.

PERGUNTAS AOS EXPOSIDORES

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agora passaremos à abertura para perguntas neste bloco da manhã. Para iniciar esta fase, farei algumas perguntas e depois recorrerei a perguntas feitas, elaboradas, por pessoas que estão aqui presentes.

Começo perguntando ao Doutor Wesley Vaz, do Tribunal de Contas da União.

O Doutor Wesley mencionou aqui, em sua exposição, que o Tribunal de Contas da União já teve a oportunidade de fazer uma análise sobre essas ferramentas de intrusão ou sobre processos de aquisição em cinco processos já encerrados, e pode, a partir disso, a partir dessas análises, estabelecer alguns critérios e também fazer algumas recomendações.

Doutor Wesley, o senhor nos poderia dizer, ainda que sem, evidentemente, abrir qualquer informação que não seja pública, quais foram as ferramentas de intrusão analisadas pelo Tribunal nesses processos de aquisição? É a primeira pergunta.

E o senhor nos poderia informar se os contratos analisados previam a coleta de dados por essas ferramentas e a destinação desses dados? Vale dizer, se a empresa que forneceu a ferramenta de intrusão, de alguma forma, pelo contrato celebrado tinha acesso ou poderia ter acesso aos dados obtidos a partir do uso dessas ferramentas?

O SENHOR WESLEY VAZ (TRIBUNAL DE CONTAS DA UNIÃO - SECRETARIA DE CONTROLE EXTERNO DE GOVERNANÇA, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL DO ESTADO) - Muito obrigado, Excelentíssimo Ministro.

Todos os cinco processos são públicos, portanto, disponíveis a todos no site do Tribunal de Contas da União.

Em relação à primeira pergunta, nós temos licitações, a 3 de 2021, do Ministério da Justiça e Segurança Pública, que tratava do sistema Pegasus. Temos também, no processo que gerou o Acórdão 1.529, de 2022, a contratação do sistema Cortex junto e temos e aberto ainda, como havia dito, a avaliação do sistema Cognite junto à atuação da PRF, se não estou enganado, sob a relatoria do Ministro Antônio Anastasia.

Bom, em todas as representações e na única denúncia já julgada, Ministro, não pôde ser evidenciado nenhum tipo de uso distinto do que foi previsto no contrato pelas empresas. Tenho que dizer que, desses cinco processos, pelo menos um deles não teve sequer essa análise realizada por ter sido uma perda de objeto, por ter sido uma interrupção da contratação.

Em todos os casos analisados, portanto, o que o TCU conseguiu identificar foi eventuais problemas no processo de aquisição e sugestão sobre os controles internos dos próprios órgãos para que eles, enquanto agentes públicos, pudessem usar o sistema e o sistema também fornecer algumas funcionalidades de modo que a gente conseguisse também checar o que cada agente público estava fazendo.

Então, objetivamente respondendo à sua questão, Ministro, o Tribunal de Contas não fez nenhum tipo de evidenciação desse tipo de situação que o senhor descreve nesses processos que já estão encerrados.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) – Perfeito.

Só uma complementação. Vossa Senhoria também afirmou que, na análise feita pelo Tribunal de Contas da União, foram feitas algumas recomendações de controle para o uso dessas ferramentas.

O senhor poderia, de forma mais objetiva, dizer quais seriam basicamente essas recomendações e também se o Tribunal de Contas fez alguma análise sobre as vulnerabilidades dos sistemas de comunicação e, a partir disso, se constatou a existência dessas vulnerabilidades para o uso das ferramentas, quais foram as providências adotadas?

O SENHOR WESLEY VAZ (TRIBUNAL DE CONTAS DA UNIÃO - SECRETARIA DE CONTROLE EXTERNO DE GOVERNANÇA, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL DO ESTADO) - Perfeito, muito obrigado.

De novo, sendo mais objetivo, aqui, nos termos do Acordão 1.331, de 2022, o Tribunal determinou que se fizesse constar do contrato e dos modelos de contrato referente a um ato de resistir preço da contratação do sistema

Pegasus características de segurança e auditabilidade. Então, o que o Tribunal fez foi determinar que o órgão inserisse no contrato jurídico controles que pudessem de algum modo garantir a segurança e a auditabilidade dos sistemas não somente por órgãos contratantes, mas para aqueles que eventualmente pudessem vir a aderir à ata de registro de preço. Isso consta do Acórdão 1.331, de 2022.

No segundo caso, presente no Acórdão 1.529, de 2022, o Tribunal checou que não houve desvio de finalidade e checou que havia controles no sistema que permitissem que se verificasse em alguma medida a auditabilidade do sistema, nesse caso, o sistema Cortex. E também nesse caso algumas recomendações foram feitas para melhorar esses controles.

É preciso dizer, senhores e senhoras, que existem dois processos em aberto e esses processos em aberto podem vir, a depender da sua análise, gerar um conjunto de recomendações e determinações, com base nos casos concretos ainda não apreciados.

Mas, de novo, para ser objetivo, excelentíssimo Ministro, esses dois casos, do Acórdão 1.529, de 2022, público, e do Acórdão 1.331, também de 2022, público, são aqueles que determinam e recomendam de maneira objetiva a criação de controles de auditabilidade nesses sistemas.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - agradeço ao Doutor Wesley Vaz e também, antes de passar para as perguntas feitas

aqui pelos presentes, gostaria de perguntar ao Doutor Hugo Alberto Lazar, na sua experiência na Agência Brasileira de Inteligência, quais foram as ferramentas de intrusão usadas, ou que são usadas para os fins que Vossa Senhoria expôs aqui durante a sua fala?

O SENHOR HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA ABIN – INTELIS) - Bom dia, Ministro! Como representante da associação, eu não tenho acesso a essas ferramentas. Enquanto funcionário, servidor da agência, eu também não tive, porque muitas das minhas áreas estavam envolvidas na área de análise. Então, eu não tenho conhecimento.

Na área de inteligência, é muito forte a questão do compartilhamento, o que uma área sabe, a outra não sabe. Então, isso é muito forte na área inteligência. Então, eu pessoalmente, eu não nunca tive acesso às ferramentas.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Eu vou então passar aqui a primeira pergunta, que é dirigida ao Doutor Wesley, do Tribunal de Contas da União. A pergunta é: o Tribunal de Contas da União tem alguma previsão de publicação de orientações específicas para a compra dessas ferramentas de monitoramento ou intrusão?

O SENHOR WESLEY VAZ (TRIBUNAL DE CONTAS DA UNIÃO - SECRETARIA DE CONTROLE EXTERNO DE GOVERNANÇA, INOVAÇÃO E TRANSFORMAÇÃO DIGITAL DO ESTADO) - Eu não sei quem perguntou, mas a resposta objetiva é que não, não há previsão. O que o Tribunal de Contas normalmente faz, a partir dos seus julgados, a partir das suas recomendações, é informar ao mercado, informar à sociedade que tipo de controle é absolutamente necessário nesse tipo de contratação. Então, objetivamente, a resposta é não, ainda não há esse tipo de previsão específica para esse regramento.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois não. Obrigado, Doutor Wesley.

Aqui a pergunta do Senhor Guilherme Portela, que é da Casa Civil, é analista e coordenador. E a pergunta é para o Doutor Hugo Lazar, que é da Intelis. A pergunta é: o Senhor poderia citar um exemplo de país democrático em que tais ferramentas são empregadas para fins de inteligência?

O SENHOR HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA ABIN – INTELIS) - Obrigado pela pergunta. A lista que eu trouxe aqui para apresentação são de países democráticos inicialmente. Mas me chama muita a atenção o modelo espanhol. No modelo espanhol, a Suprema Corte espanhola designa um juiz para avaliar os casos de inteligência, um juiz específico.

No caso canadense, por exemplo, também existe uma normatização de que o próprio diretor do Canadian Security Intelligence Service pode acionar o Tribunal Superior Canadense para delimitar as ações operacionais da atividade de inteligência. São dois casos que chamam muita atenção.

Um terceiro caso interessante também é na Suécia. Na Suécia, as agências de inteligência podem acionar o Poder Judiciário, e o Poder Judiciário tem a assistência de especialistas em direitos dos cidadãos, em direito privado, em regulação da cidadania para apoiar esse juiz especializado na decisão.

São os três casos que mais chamam a minha atenção.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Hugo Lazar!

A Doutora Rebeca Azevedo, advogada, pergunta à Doutora Laura Mendes: a OAB mencionou a necessidade de regulamentação específica sobre o tema. Quais são os critérios propostos?

A SENHORA LAURA SCHERTEL MENDES (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL – COMISSÃO DE DIREITO DIGITAL) - Obrigada, Ministro! Obrigada pela pergunta!

Bom, o mais importante é que haja uma dada reserva legal, que tenha uma legislação com inúmeros requisitos. Nós, no memorial, citamos cerca de

oito ou nove requisitos. Vou passar para o Alisson, que vai especificar pelo menos seis principais que a gente considera fundamentais.

O SENHOR ALISSON ALEXSANDRO POSSA (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL – COMISSÃO DE DIREITO DIGITAL) - Obrigado pela pergunta!

Cabe ressaltar que os requisitos são apontados já na doutrina brasileira sobre a necessidade da reserva legal para o uso desses softwares. Nós identificamos aqui os seis que entendemos os principais.

Primeiro requisito: a necessidade de autorização judicial devidamente fundamentada com a observância da adequação, necessidade e proporcionalidade, em sentido estrito, do uso dessas ferramentas no caso concreto, e não em uma situação abstrata.

Segundo requisito: hipóteses fechadas e restritas dos tipos penais em que o uso do *malware* deve ser permitido, devendo possuir ainda a pertinência entre o crime e a medida adotada.

Terceiro requisito: estabelecimento de procedimentos com tipos e dispositivos maliciosos permitidos, tipos de dados que podem ser com coletados, reversibilidade de medida, entre outros mecanismos voltados à segurança, entendendo-se a confidencialidade e a integridade desses sistemas informacionais,

até porque esses softwares podem modificar em alguns casos, como alguns expositores mencionaram, as barreiras de segurança informacionais.

Quarto requisito: determinação de um período para a utilização dos softwares e a limitação de renovações.

Quinto requisito: previsão de formas para garantir a proteção de conteúdos íntimos ou sensíveis encontrados com o uso da ferramenta que não tenham relevância para a investigação ou pertinência com ela. Aqui eu remeto à fala do Doutor Turbay, no sentido que ele mencionou, de que esses softwares, quando adentram o dispositivo para garantir acesso a uma totalidade dos dados armazenados e das comunicações, fica muito difícil de fazer uma seleção, muitas vezes, do que se está tendo acesso e pode haver ali dados que envolvem a vida privada e extremamente íntimos.

Sexto requisito: mecanismos de supervisão e controle, seja para o controle por autoridade competente, seja também por parte do acusado e dos investigados.

Então, esses são os requisitos que nós extraímos da doutrina e que entendemos que seriam necessários na elaboração da reserva legal.

Muito obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Alisson.

A próxima pergunta foi feita pelo Senhor Guilherme Portela, que é da Casa Civil da Presidência da República, e se destina à Doutora Samara Castro. A pergunta é: estados democráticos, como os Estados Unidos e nações europeias, empregam tais ferramentas para fins de inteligência? Quais são os mecanismos de controle aplicáveis e proporcionais na visão de Vossa Senhoria?

A SENHORA SAMARA CASTRO (PRESIDÊNCIA DA REPÚBLICA – SECRETARIA DE POLÍTICAS DIGITAIS DA SECRETARIA DE COMUNICAÇÃO SOCIAL) - Obrigada pela pergunta.

Nós entendemos - e acho que haverá ainda, ao longo do dia, várias contribuições de diversas áreas e setores do governo - que é muito importante a nossa contribuição na defesa dos jornalistas. Nesse sentido, por toda a exposição que eu já coloquei, especialmente para os jornalistas, nós entendemos que nenhuma hipótese do uso dessas ferramentas é cabível, justamente porque o custo-benefício no sentido do potencial de dano que pode ter o uso dessas ferramentas em relação aos jornalistas, ele não compensa quando a gente tem que sopesar valores. E, nesse sentido, não faria nenhum bem para a nossa sociedade

que elas fossem viabilizadas, mesmo que isso tivesse parâmetros ou regulamentações específicas.

Aqui, nós estamos falando especificamente de um público, e é óbvio que tem vários desafios quando a gente aponta isso, inclusive a própria compreensão de quem seriam, quem se enquadraria nessa categoria. Mas, de toda forma, nós entendemos que a reflexão que deve ser feita para esse público, em específico, é de nenhum tipo de uso. Ainda que, em outros países, esse seja um debate um pouco mais acalorado, também é importante lembrar que esses países, eles têm abordagens diferentes para a preservação da liberdade de expressão e de imprensa do que nós temos aqui no Brasil.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutora Samara.

Uma outra pergunta do Doutor Guilherme Portela, da Casa Civil, da Presidência da República. Pelo que eu compreendi, é para o doutor Hugo Lazar.

Como estados democráticos, em especial nações com o porte e a relevância do Brasil no cenário internacional, regulam o uso de ferramentas tecnológicas intrusivas por parte dos serviços de inteligência? Quais são os controles *ex ante* aplicáveis?

Eu acredito que, aqui, na verdade, o Doutor Hugo já falou sobre isso, mas se quiser desenvolver um pouco mais a questão, eu concedo a palavra a Vossa Senhoria.

O SENHOR HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA ABIN-INTELIS) - Ministro Zanin, quero aproveitar a pergunta também para avançar nas ideias que nós colocamos aqui. Nós fizemos muita referência aos países democráticos por conta dessa similaridade com o Brasil. Eles são países também que estão na defesa da democracia. E nesses países, o que a gente nota é essa situação de uma vara especializada, um juizado especializado que permita um controle judicial prévio.

No Brasil, quando foi criada a Abin e o Sistema Brasileiro de Inteligência, criou-se também um controle parlamentar, mas que, na verdade, é um controle posterior.

A Comissão de Controle da Atividade e Inteligência do Congresso Nacional, seis deputados, seis senadores, se reúne muito pouco, infelizmente, mas faz um controle posterior. Ela basicamente trabalha nas crises. E o que nós propomos, aqui, em linha com o mundo - nós estamos atrasados nesse ponto - é que possamos ter um controle prévio, um controle das atividades de inteligência, sejam operacionais, ou com ferramentas intrusivas ou não intrusivas, que esse controle seja eficiente e eficaz e no momento oportuno.

É essa defesa da linha que nós propomos, aqui, hoje.

Muito obrigado pela palavra.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Hugo.

Enquanto aguardamos eventuais outras perguntas, eu faço uma pergunta à Doutora Laura Mendes. Vossa senhoria fez referência a um julgado do Tribunal Constitucional Alemão que tratou sobre as ferramentas de intrusão. Esse julgado, ele tratou sobre alguma ferramenta específica ou foi de forma mais genérica sobre as ferramentas de intrusão? E se Vossa Senhoria poderia também nos dar quais foram as conclusões e os encaminhamentos dados pelo Tribunal Constitucional Alemão.

Muito obrigado.

A SENHORA LAURA SCHERTEL MENDES (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL - COMISSÃO DE DIREITO DIGITAL) - Muito obrigada pela pergunta, Ministro Zanin.

Bom, a decisão era de 2008, então até imagino que as ferramentas são um pouco diferentes das que a gente tem hoje, talvez menos poderosas, mas ele não trata de uma ferramenta específica, mas eles chamam de softwares espiões, cavalos de troia, é a expressão que o Tribunal usa. E, na época, esse estado específico alemão, Nordrhein-Westfalen, tinha autorizado o órgão

estadual, inclusive, de inteligência a utilizar essas ferramentas. Então, não apenas há, digamos, o órgão que cuida da inteligência nacional. Então, acho que esse é um ponto importante.

E então, não há uma ferramenta específica, mas é esse tipo de intrusão que estava sendo debatido. A intrusão não apenas para telecomunicações, mas para toda a esfera virtual da pessoa. Então, é interessante que, na ocasião, o Tribunal acabou entendendo que apenas o direito à determinação informativa não era suficiente e que era preciso avançar ainda mais, tamanho o risco para a esfera privada. Então eles avançaram, criando quase, não criando um novo direito, mas uma nova dimensão daquele direito já, hoje previsto na Carta alemã, que é esse direito ligado a um sistema, como se todos os sistemas pessoais, *notebooks*, telefones, estivessem protegidos, no sentido - aqui muito acho que trazido pelos colegas da mesa - de que nós precisamos confiar nesses sistemas, na sua integridade, na sua confidencialidade, porque, de certa forma, toda a nossa vida hoje está armazenada nesses sistemas. Portanto, é quase como se fosse um direito fundamental ligado a esse sistema.

E no fim, ele também traz as limitações, como todo direito fundamental, pode haver sim uma limitação, só que essa limitação precisa estar, digamos, amparada em uma legislação específica baseada em uma autorização judicial, mas um elemento talvez mais importante que a gente trouxe também aqui

nos memoriais, Ministro, foi o fato de que é preciso avaliar um perigo concreto, é preciso ter um perigo concreto para a vida e para outros bens jurídicos máximos. Ou seja, deixando claro que é preciso ter uma proporcionalidade, já que essas ferramentas causam um risco tão grande aqui - como acho que os colegas muito bem trouxeram -, em tantas esferas, e o que está em jogo de fato é, ao fim e ao cabo, a nossa democracia. É fundamental que apenas em hipóteses muito restritas seja realmente necessária a utilização dessas ferramentas. Então, no fim, a decisão traz esses elementos.

Eu acho que um elemento muito importante também que a decisão traz é o fato de que a gente sabe que essas ferramentas vão acabar encontrando elementos muito íntimos das pessoas. Como eu disse, talvez nem uma câmera dentro da nossa casa traria isso. E aí a lei traz essa necessidade de que as ferramentas possam eventualmente separar, ou uma obrigação de que a autoridade policial consiga separar essas informações e não utilize essas informações íntimas, que certamente não serão necessárias para a investigação, que haja alguma garantia de como essas ferramentas, de como o núcleo essencial da nossa intimidade poderá ser protegido mesmo a partir do uso dessas tecnologias.

Então eu acho que esse seria, digamos, um passo a passo para que a gente consiga ter uma maior proporcionalidade no uso dessas ferramentas. Obrigada pela pergunta.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Laura Mendes.

Antes de ler a próxima pergunta, eu também gostaria de formular uma nova pergunta ao Doutor Hugo Lazar. A partir da sua *expertise* nessa área, Vossa Senhoria tem conhecimento do uso privado dessas ferramentas? Ou seja, essas ferramentas são destinadas e adquiridas apenas por entes estatais, no Brasil e no mundo, ou também há o uso privado dessas ferramentas a partir de uma comercialização daqueles que fabricam para entidades privadas? Ou até mesmo se há algum conhecimento de Vossa Senhoria da cessão da ferramenta adquirida por um órgão público para um ente privado.

O SENHOR HUGO ALBERTO LAZAR (UNIÃO NACIONAL DOS PROFISSIONAIS DE INTELIGÊNCIA DE ESTADO DA ABIN - INTELIS) - Ministro, eu não tenho conhecimento da passagem do controle da ferramenta de órgão público para um órgão privado. Mas, no plano internacional, eu não duvido que organizações criminosas ou terroristas, em algum momento, possam ter acesso a esse tipo de ferramenta, seja no mercado primário, seja no mercado secundário. Isso eu acho cabível, que algumas entidades privadas ou organizações privadas possam ter esse acesso. No caso brasileiro, eu desconheço que haja a venda para o mercado privado. O que se sabe é mais para o mercado público.

Voltando um pouquinho à pergunta que o Senhor fez inicialmente, sobre se eu tinha conhecimento de uso de ferramentas pela Abin, o Senhor chegou a ler o meu currículo por completo e o Senhor pôde notar que eu estive em Moscou, na Rússia. Então, eu tenho quase certeza de que eu fui alvo de ferramenta tecnológica, quando da minha estada na Rússia, por um governo autocrático. E o que a gente defende aqui é que, na nossa democracia, a gente possa defender a nossa democracia. Acho que isso é importante passar para essa audiência pública. Muito obrigado, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado mais uma vez, Doutor Hugo Lazar. Eu indago à Doutora Elizeta Paiva Ramos se Vossa Excelência tem alguma pergunta para fazer aos nossos convidados.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Agradeço, nenhuma pergunta.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Também pergunto ao Doutor Marcelo Turbay, que representa o Conselho Federal da Ordem dos Advogados do Brasil, se teria alguma pergunta dirigida aos nossos expositores.

O SENHOR MARCELO TURBAY (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL) - Obrigado, Ministro. Na realidade, eu

até fiz uso aqui do QR code, prestigiando o cerimonial, para fazer uma pergunta endereçada à Doutora Raquel Saraiva, do IP.rec.

A Doutora Raquel mencionou que eles conseguiram apurar a aquisição, ou pelo menos tentativa de aquisição, de software por diversos estados, incluindo secretarias de fazenda estaduais.

A pergunta é se também foi possível identificar essa aquisição por parte de órgãos do Ministério Público estadual, mais especificamente os extintos Gaecos?

A SENHORA SAMARA CASTRO (PRESIDÊNCIA DA REPÚBLICA – SECRETARIA DE POLÍTICAS DIGITAIS DA SECRETARIA DE COMUNICAÇÃO SOCIAL) - Obrigada pela pergunta, Doutor Marcelo.

Eu não tenho, de memória, a referência se especificamente os extintos Gaecos fizeram uso ou contrataram esse tipo de ferramenta. Mas, na nossa pesquisa, pudemos constatar que todos os estados e diversos órgãos públicos de estados têm contratos vigentes com essas ferramentas.

Nós fizemos uma busca, via pedido de lei, dessa sua informação. As 27 secretarias estaduais responsáveis pelas atividades de segurança pública, incluindo a do Distrito Federal; 27 Ministérios Públicos estaduais, incluindo o do Distrito Federal; o Ministério Público Federal e a Polícia Federal, através do Ministério da Justiça e Segurança Pública; o comando do Exército; o comando da

Marinha e o Ministério da Defesa e o Gabinete de Segurança Institucional. Também foi realizada a pesquisa nos portais de transparência dos 26 estados, do Distrito Federal e do Governo Federal. No recorte temporal, entre 2015 e 2021, o resultado foi o levantamento de 209 documentos contratuais no âmbito estadual e federal, compreendendo compra, treinamento de funcionários, termos aditivos, atualização de software e outros atos administrativos comprovando que as ferramentas de *hacking* estão, ou estiveram, em uso no país.

É um cenário em que podemos constatar, de fato, que essas ferramentas estão intrinsecamente utilizadas no Estado brasileiro, em todas as esferas federativas.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Doutora Raquel, uma complementação à pergunta do Doutor Marcelo Turbay. Vossa Senhoria mencionou que, nesses casos de contratos feitos por agentes públicos, eventualmente com órgãos do Ministério Público, há conhecimento se os dados obtidos, a partir do uso dessas ferramentas, de alguma forma, podem ser acessados pelos fabricantes ou representantes que comercializam essas ferramentas?

A SENHORA SAMARA CASTRO (PRESIDÊNCIA DA REPÚBLICA – SECRETARIA DE POLÍTICAS DIGITAIS DA SECRETARIA DE COMUNICAÇÃO SOCIAL) - Não temos como precisar se as empresas estão tendo

acesso a esses dados. Justamente por isso, achamos muito perigoso, porque não há transparência sobre as cláusulas desses contratos, no que se refere ao acesso das empresas fornecedoras e dos fabricantes, porque, em geral, são empresas diferentes. As fabricantes contratam representantes no Brasil para fazer a venda aos entes estatais. Logo, não temos como precisar se de fato elas estão tendo acesso aos dados, ou não. Justamente por essa razão reside o perigo, porque não temos transparência sobre isso.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Raquel Saraiva.

Uma pergunta do Senhor Cleberson Alves dirigida ao Doutor Pedro José Nasser: Em relação aos sistemas operacionais dos dispositivos móveis, há diferença, em grau de dificuldade de intrusão, em relação ao ecossistema Android ou iOS?

O SENHOR PEDRO JOSÉ NASSER SALIBA (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA – DATA PRIVACY BRASIL) - Cada um dos sistemas tem uma ferramenta diferente. Então, por serem sistemas diferentes, são aplicações diferentes.

Nesse relatório do IP.rec, vemos que existem, por exemplo, ferramentas de extração de dispositivos. Aí, existe um complemento para aquela ferramenta de extração de dispositivos específico para o Android ou para o iOS.

Além dessas categorias que estamos criando se sobreporem - uma ferramenta tem mais de uma categoria -, vemos também que, nesse mercado das vulnerabilidades, existem complementações específicas para cada tipo de cliente, para cada tipo de necessidade das pessoas que contratam. Então, existe, sim, essa diferença.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Pedro Nasser.

A próxima pergunta também é para o Doutor Pedro, que foi feita pela Larah Brahim, representante do Centro de Pesquisa e Extensão em Ciências Criminais. A pergunta é: quais órgãos públicos, na visão e conhecimento de vossa senhora, têm mais adquirido as ferramentas de intrusão que estamos tratando nesta audiência?

O SENHOR PEDRO JOSÉ NASSER SALIBA (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA – DATA PRIVACY BRASIL) - Eu não tenho de cabeça agora quais são essas ferramentas, quais são esses órgãos que contrataram essas ferramentas. A gente sabe, pelo relatório do IP.rec novamente, que a maioria das contratações é de extração de dispositivos, mas lá nesse relatório *Mercadores da Insegurança* tem esse detalhamento.

E o que eu destaco, que eu acho que é o que mais nos chamou a atenção durante a pesquisa, era que ferramentas altamente intrusivas estavam

sendo contratadas, por exemplo, tanto pelo Exército quanto por secretarias estaduais de segurança. Então, isso nos chama muito a atenção, essa falta de controle, porque não só a competência legal desses órgãos, mas também o nível de intrusão à privacidade e as diferentes competências federativas mesmo. Eu acho que isso precisa ser muito bem delimitado. E esse é um risco muito grande que a gente está debatendo aqui nesta audiência e nessa ADPF exatamente pela falta de controle a respeito sobre quem pode adquirir, qual ferramenta pode adquirir e em quais momentos isso pode ser feito.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado.

Nessa linha, eu também complemento a pergunta para a Doutora Raquel Saraiva. Se eu entendi durante a exposição de Vossa Senhoria, há notícia da aquisição dessas ferramentas até por secretarias de fazenda de estados, é isso, Doutora Raquel?

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) - Sim, isso foi uma coisa muito preocupante que a gente encontrou na pesquisa, órgãos que não têm, a princípio, competência investigativa estavam contratando esse tipo de ferramenta. Então, a gente pôde constatar, por exemplo, uma secretaria de fazenda de um

estado, mas também a gente pôde constatar o próprio Cade contratando esse tipo de ferramenta, o que nos levanta um questionamento de para que estão sendo utilizadas essas ferramentas em órgãos que não têm esse tipo de competência.

Então, a falta de transparência no uso dessas ferramentas causa inclusive esse tipo de questionamento, porque a falta de controle dessas contratações faz com que a secretaria de fazenda de um estado contrate essa ferramenta, ela não tem competência investigativa, mas ela está usando para quê? Então, acho que a gente precisa de um nível de transparência muito maior.

Com o Cade também, acho que o Cade é um outro grande exemplo disso. Na nossa pesquisa, foi encontrado um contrato do Cade em relação a essas ferramentas também. Então, acho que a gente precisa de um nível de transparência muito maior para que esse tipo de prática não ocorra mais.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Só complementando, nas pesquisas a que a Vossa Senhoria teve acesso, há notícia também do uso dessas ferramentas por entidades privadas? Eu já fiz a pergunta ao Doutor Hugo Lazar, mas também faço a Vossa Senhoria.

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) - Excelência, o uso por entidades privadas não foi objeto na nossa pesquisa. Ela se limitou a buscar as

ferramentas em órgãos públicos, então eu não tenho essa informação. Mas, como disse o Doutor Hugo Lazar, eu realmente não duvido que isso esteja sendo utilizado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Doutora Elizeta Paiva Ramos gostaria de fazer uma pergunta.

A SENHORA ELIZETA PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Eu tenho uma pergunta para a Doutora Raquel Saraiva.

Quantas dessas ferramentas catalogadas pelo Instituto se referem a ferramentas de acesso remoto a dispositivos? Porque a minha assessoria está chamando muito bem a atenção, os procuradores são preparados para isso, pois se precisa fazer uma diferenciação entre o objeto da audiência pública e as outras ferramentas tecnológicas utilizadas pelo Estado para a extração de dados de aparelhos apreendidos, como o Cellebrite, e ferramentas de análise de dados que foram extraídos em outra ocasião.

Então, a pergunta é essa.

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) - A senhora pode repetir, por favor?

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Sumiu.

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) – Desculpa.

A SENHORA CAROLINA SANTOS LIMA (JUÍZA INSTRUTORA DO GABINETE DO MINISTRO CRISTIANO ZANIN) - Doutora Raquel, a pergunta é se essas ferramentas que nós estamos discutindo na audiência pública se referem à intrusão remota nos dispositivos móveis ou se são aquelas, se essa pesquisa contemplou aquelas que os entes, os órgãos públicos utilizam para extrair dados de equipamentos apreendidos, por exemplo. É que haveria essa distinção.

A SENHORA RAQUEL SARAIVA (INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE – IP.REC) - A pesquisa contemplou as duas, os dois tipos de ferramenta, tanto a extração de dados em massa local com o acesso ao dispositivo quanto o acesso remoto. Mas, é ... Enfim, acho que as de extração... É... A pergunta da senhora se referiu à da extração em massa de dados, não é? Eu acho que era minoria, nesse caso, dos achados da nossa pesquisa, eu acho que era minoria, se eu me recordo bem. Mas, de toda forma, nós vamos submeter os memoriais porque, como o IP.rec é *amicus curiae*, nós vamos submeter os memoriais com todos esses dados também nos autos do processo.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Alguma pergunta mais?

Bom, então, eu agradeço aos nossos expositores da parte da manhã pelas relevantes contribuições que trouxeram para esta Arguição de Descumprimento de Preceito Fundamental 1.143.

Agora, vamos fazer um intervalo para o almoço e voltaremos às 14h com um novo bloco de expositores.

Muito obrigado e bom almoço a todos!

DIA 10/7/2024 – TARDE

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Boa tarde a todos!

Renovo meus cumprimentos à Doutora Elizeta Maria de Paiva Ramos, Subprocuradora-Geral da República, ao Doutor Marcelo Turbay, à Doutora Caroline, ao Doutor Lucas, a todos que hoje, agora na parte da tarde, farão suas exposições e a todos aqui presentes ou que nos assistem pelo canal do YouTube.

Conforme já expus pela manhã, o objetivo desta audiência é instruir o processo com informações de todos os segmentos da sociedade, seja por meio de órgãos públicos, seja por representantes da sociedade civil, especialistas

ou interessados que possuam experiência e autoridade no tema aqui discutido, que, mais precisamente, trata dos limites e possibilidades da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, também chamadas ferramentas de monitoramento secreto de aparelhos de comunicação pessoal.

Na parte da manhã, tivemos já exposições de especialistas e representantes da sociedade civil. Daremos, agora, continuidade.

O primeiro a falar será o Doutor Sauvei Lai, Promotor de Justiça do Ministério Público do Estado do Rio de Janeiro, professor, autor de obras jurídicas, membro do Grupo de Trabalho da Sub-relatoria de Revisão do Código de Processo Penal na Câmara dos Deputados, autor também do Anteprojeto de Lei nº 4.939/2020, que trata sobre provas digitais e outros assuntos.

Concedo a palavra ao Doutor Sauvei, para fazer sua exposição, reforçando que o tempo de exposição foi dividido em dez minutos para cada expositor, com a possibilidade, ao final, de abrirmos um tempo para perguntas e outras colocações complementares.

O Doutor Sauvei tem a palavra para a sua exposição.

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - Boa tarde a todos, boa tarde

a todas! Excelentíssimo Senhor Ministro-Relator, Doutor Cristiano Zanin, Excelentíssima Senhora Subprocuradora-Geral da República, Doutora Elizeta Ramos. Rendo minhas homenagens também ao Conselheiro Federal da OAB, Doutor Marcelo Turbay e aos Juízes Instrutores Doutora Caroline Lima e Doutor Lucas Sales.

Tenho uma apresentação para passar e temos alguns tópicos para serem abordados basicamente. O primeiro item, sem dúvida, é o aumento de cybercrimes, da criminalidade cibernética. Acompanhamos isso no mundo inteiro.

Quanto à questão da criminalidade cibernética no Brasil especificamente, temos dados da ONG Safernet, que arrecada e coleta as principais denúncias de crimes praticados no ambiente virtual. Só em relação ao crime de pedofilia, exploração sexual infantil, foram mais de 100 mil denúncias no ano passado, reportadas com imagens, incluindo filmagens de crianças em situação de exploração sexual.

Não podemos esquecer também que o legislador se encontra atento. De 2022 para cá, tivemos diversas alterações no Código Penal: Lei nº 14.155, que introduziu a fraude eletrônica, o furto eletrônico; Lei nº 14.478, que cuida das pirâmides financeiras com ativos virtuais, com as criptomoedas; recentemente, Lei

nº 14.811, que tipifica o *cyberbullying*, a perseguição sistemática, especialmente contra as crianças, mas não só.

A parte mais nefasta do uso da tecnologia não apenas visa à potencialização da prática do crime, mas também ao uso de ferramentas antiforenses, ao uso de ferramentas de medidas pela criminalidade, especialmente a criminalidade organizada, para ofuscar, dificultar, a persecução criminal.

Temos, hoje, dispositivos eletrônicos cujos aplicativos de mensagens se utilizam de criptografia ponta a ponta. Isso certamente torna todas as medidas atuais obsoletas. A interceptação telefônica hoje está fadada ao fracasso. Nas nossas investigações, as pessoas não usam mais o telefone para se comunicar; usam, sim, o aplicativo, com essa criptografia ponta a ponta. Recentemente, por sinal, as grandes organizações criminosas mundo afora, inclusive, já usam o próprio sistema de comunicação, com dispositivos adquiridos no mercado negro, com modificações de sua configuração de fábrica e sem a intermediação de empresas de tecnologia como WhatsApp, Signal e Telegram.

Tivemos, em 2020, uma operação europeia, EncroChat, na Bélgica. Tivemos também, em 2021, como está no eslaide, uma operação do FBI, a polícia federal norte-americana, com o sistema Anom, ou seja, sistemas envolvidos por organizações criminosas, sistemas próprios de comunicação, sem

intermediação de empresas de tecnologia, com criptografia própria, de ponta a ponta. Tudo isso nos força a criar novas ferramentas, não só tecnológicas, mas jurídicas, para a persecução criminal de crimes digitais. Em Portugal, na Europa, no mundo afora, como veremos daqui a pouco, chamam-se de novos meios ocultos - têm essa característica sub-reptícia - de investigação em ambiente digital. O Professor Pérez, professor espanhol, diz que a investigação atualmente ou é tecnológica ou simplesmente não é investigação. Nesse ponto, é muito importante diferenciar - às vezes, existe confusão e até um certo preconceito em chamar de *spyware*, de programa espião. Cada país tem sua terminologia. Na Alemanha, chama-se *durchsuchung online*, quer dizer, busca *on-line*; nos Estados Unidos, *remote forensics*; na França, *captation des données informatiques*. Mas, hoje, existe um consenso: diferenciamos o GovWare, que é governo e software, ou seja, é um programa estatal para infectar, com vírus, dispositivos de alvos para monitorar, em tempo real, todas as atividades, por conta justamente da criptografia ponta a ponta - temos que saber, enquanto esse alvo digita, o que ele está enviando de mensagem, porque, a partir do momento que ele clica no botão enviar, toda a mensagem fica codificada. E não é só isso, há um segundo objetivo, como os expositores afirmaram mais cedo: a possibilidade de acionar o sistema de vídeo e o sistema de áudio, transformando aquele dispositivo eletrônico, sobretudo o dispositivo móvel, em verdadeiro instrumento, ferramenta, de gravação ambiental.

O GovWare, o nome já está dizendo, é um programa de Estado, de Governo, que tem dois módulos. Há duas espécies, dependendo da finalidade. Se o objetivo é investigar um crime, chamamos de software policial, Policia Ware, mas se o objetivo é coletar informações sensíveis, ou seja, de inteligência, aí sim chamamos de *spyware*. Parece que está havendo essa confusão.

O software policial já vem sendo usado no mundo inteiro. Coloquei até uma cronologia: desde 1999, nos Estados Unidos; nos principais países continentais da Europa: Espanha, em 2015, Alemanha, em 2017 - a colega Laura Mendes citou a inconstitucionalidade em 2008, mas com base nessa decisão, o legislador mudou o STPO, o Código de Processo Penal alemão, em 2017, está em vigor a possibilidade desse Policia Ware, desde que respeitadas as balizas legais -, Itália, na sequência, em 2017, recentemente, a França, em 2019. No Brasil, por sua vez, temos o projeto de lei do Senado, apresentado recentemente, de autoria do Senador Alessandro Vieira, que tenta regulamentar o GovWare, tanto no aspecto do Policia Ware quanto no aspecto de inteligência, de espionagem, a questão do *spyware*.

Tenho um livro que será publicado, no mês que vem, exatamente sobre esse tema. Analiso como está sendo regulamentado na Alemanha, em 2017, sempre para determinados crimes; na Alemanha, chama-se inclusive de crimes especialmente graves. São crimes praticados por organizações

criminosas: terrorismo, tráfico de seres humanos - algo muito recorrente na Europa -, tráfico de drogas e, obviamente, crimes com violência física e grave ameaça. Na França, temos o respeito ao princípio da proporcionalidade nos seus três aspectos: que essa intrusão seja, além de adequada, necessária e proporcional, em sentido estrito - a França expressamente prevê a possibilidade de acionamento à distância do sistema de câmera e de áudio. No Brasil, existe uma proposta, que está no livro, que justamente visa a balizar o uso do Policia Ware, definindo-se os crimes - obviamente respeitando-se os princípios da proporcionalidade. Como disse, o âmbito de aplicação do Policia Ware, basicamente, são os crimes especialmente graves, obviamente sempre com requerimento prévio do Ministério Público, com a devida autorização judicial - ao contrário da Espanha, onde é possível a decretação de ofício do Policia Ware.

Temos também a delimitação subjetiva dos alvos, grande preocupação inclusive na Europa. No caso Big Brother Watch *vs.* Inglaterra, em 2018, o Tribunal Europeu de Direitos Humanos proíbe o uso do Policia Ware contra jornalistas. Existe inclusive meio tecnológico para prevenir isso. Por exemplo, já é tecnicamente impossível usar o Policia Ware em um canal de jornal, Globo, ao citar todo o *e-mail,* @globo.com. Existem meios tecnológicos para se adotar previamente medidas para evitar esse tipo, por exemplo, contra advogados, contra aqueles que têm dever de sigilo profissional. E claro, existem outros requisitos.

O tempo é curto, o material está à disposição. Existe inclusive um livro que entregarei à Vossa Excelência posteriormente.

A Associação Nacional do Ministério Público - CONAMP encerra pedindo que se declare a inconstitucionalidade por omissão e que se fixem balizas para o devido uso do Policia Ware.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Sauvei Lai, pela exposição.

Passo a palavra, agora, para o Doutor Lauro Moraes Rego, advogado do Diretório Nacional do Partido Verde, Bacharel em Direito pelo IDP. Obteve experiências profissionais na Secretaria de Políticas para Mulheres da Presidência da República, na Secretaria Judiciária do Supremo Tribunal Federal. Tem atuação no Congresso Nacional especialmente voltada à defesa de interesses de partidos políticos, parlamentares, frentes parlamentares, especialmente na Câmara dos Deputados. Tem experiência acadêmica como professor voluntário na UnB, na área de sociologia jurídica.

Doutor Lauro, tem a palavra.

O SENHOR LAURO RODRIGUES DE MORAES RÊGO JÚNIOR (PARTIDO VERDE) - Primeiramente, queria cumprimentar todos,

especialmente na pessoa do excelentíssimo Senhor Ministro-Relator, Ministro Cristiano Zanin, a quem cumprimento efusivamente pela coragem de convocar audiência pública para debater um tema que nos é tão caro e tão difícil a todos nós. Cumprimentar também, como não poderia deixar, a Doutora Elizeta Maria de Paiva Ramos pela visão aguçada e acurada em propor esta inconstitucionalidade por omissão que, do ponto de vista político-partidário, de fato há.

Eu inicio minha exposição recordando como ponto de partida o art. 45-D, da *Grundgesetz*, a Constituição da República Federal da Alemanha, que trata especificamente de atividades de inteligência de Estado e assim diz a *Grundgesetz:* o Parlamento nomeará um comitê para controlar as atividades de inteligência federais. Este ponto me parece importante de ser salientado porque chamou-nos a atenção do pedido constante da inicial: concessão de medida para o fim de determinar a aplicação provisória da fixação de dispensável autorização judicial prévia, portanto a reserva jurisdicional, à utilização por quaisquer órgãos públicos, inclusive as ações de inteligência, forças armadas, forças policiais, bem como parâmetros e balizas fixados pelo Supremo, até ulterior provisão legislativa. Portanto, em nossa leitura, o pedido contempla tanto o aspecto de segurança pública, que é aspecto de persecução criminal, portanto reunindo os requisitos previstos no Código de Processo Penal e no Código Penal, que são afetos à questão da coletividade, ao correto deslinde da persecução criminal.

Mas também, no mesmo pedido, insere-se a questão da inteligência do Estado. E este ponto é objeto de nossa preocupação de forma específica, porque envolve não uma intervenção antecipada da Corte em relação à matéria, mas uma intervenção da Corte em relação a fatos pretéritos, em relação a fatos presentes e em relação a fatos futuros. Por quê? No caso das atividades de inteligência, seja aquela inteligência desenvolvida pelo Estado, como manifestou-se a Associação da Inteligência Brasileira, a Abin, mais cedo, seja a inteligência erroneamente usada por particulares, caso que não se sabe qual o limite exato desse alcance.

No caso de direito parlamentar, existe uma série de inviolabilidades que o próprio Texto Constitucional traz para o exercício da atividade legiferante. Chama-nos a atenção a necessária incidência do art. 53 nesta discussão, porque, em combinação com o art. 5º, X e XII, que são claramente abordados na inicial, precisa ser contemplada, no futuro reconhecimento de omissão por parte do Supremo, a necessidade de articular essa omissão com as garantias parlamentares, inclusive porque o art. 53, da Constituição, traz essas inviolabilidades civil e penalmente.

E digo mais, os incisos VI, VII e VIII, também do art. 53, referem-se a imunidades parlamentares. E diz a Constituição Federal: as imunidades de

deputados ou senadores subsistiram inclusive durante o estado de sítio, de tal maneira que a nós nos parece que, ainda que sobrevindo uma regulamentação para os mecanismos de intrusão, parece-me que esses mecanismos são totalmente imprestáveis se aplicados contra parlamentares no exercício do mandato, exceto por decisão do Supremo Tribunal Federal, porque precisamos, juridicamente, pensar também em exceções, e o Tribunal tem visitado princípios da proteção democrática no caso, por exemplo, da abolição violenta do Estado Democrático de Direito. Se há, como último *ratio*, a necessidade de lançar-se mão do mecanismo de intrusão, parece-me que o valor democrático e republicano é mais importante doravante do que a garantia parlamentar, mas em casos excepcionais.

Então, eu queria abordar esses pontos e dizer que o direito à vida e à segurança são, nos termos da jurisprudência, não apenas de dimensão negativa, mas também de dimensão positiva, constituindo a exigência de que o Estado construa políticas de segurança e controle de violência armada, pelo que nos parece haver aqui na matéria uma correlação com a ADI 6.680, Relatora a Ministra Rosa Weber, e com a ADI 6.446, Relator o Ministro Edson Fachin, no ponto de que fomenta-se a dimensão positiva da questão da segurança pública, marcando, entretanto, o caráter excepcional dos mecanismos de intrusão, a exigência de demonstração e comprovação de necessidade concreta (este ponto já foi salientado mais cedo inclusive pela Ordem dos Advogados do Brasil) e vedando-se

expressamente as chamadas necessidades presumidas, termo que consta da jurisprudência.

Portanto, todo esse sistema precisa estar voltado a contemplar o interesse público, e aqui nos alinhamos também à ideia de reserva de jurisdição, prévia e exaustiva motivação e controle de legalidade, sobretudo pelo Poder Judiciário. Agora retomo as palavras do sempre Decano Ministro Celso de Mello: até para que haja a impossibilidade de conversão dos mecanismos de intrusão em instrumentos de busca generalizada e devassa indiscriminada, aspas, estou citando Sua Excelência, o HC 84.758, relatoria do Ministro Celso, até para que fique muito clara a finalidade do mecanismo de intrusão, preservada a imunidade do Poder Legislativo, a inviolabilidade parlamentar que ocorre *ratione muneris* e é indisponível. O parlamentar, inclusive, não pode dispor de suas faculdades, de suas prerrogativas parlamentares.

Portanto, e aqui finalizo relembrando que o próprio Supremo já definiu regras limitadoras de processamento parlamentar e proibição de prisão de parlamentar. Portanto, não é exótico o entendimento que se traz à baila nesta audiência pública, senão porque referendado pela jurisprudência.

Eu vou evitar citar muito precedentes, mas farei juntada de memorial por escrito nos autos, porque entendo que poderá facilitar, e penso que estes pontos resumem o principal da matéria a ser abordada.

Agradeço, novamente, a Sua Excelência o Ministro-Relator, renovo os cumprimentos a Vossa Excelência Subprocuradora-Geral da República pela coragem de propor esta reflexão e também aos colegas que falaram mais cedo e falaram doravante.

Obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Lauro Moraes Rêgo. E agora passo a palavra para o Doutor André Cyrino, que é Professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro, Mestre e Doutor em Direito Público pela Universidade do Estado do Rio de Janeiro. E também tem *Master of Laws* pela Yale Law School dos Estados Unidos.

Doutor André Cyrino tem a palavra, por gentileza.

O SENHOR ANDRÉ CYRINO (CONEXIS BRASIL DIGITAL - SINDICATO NACIONAL DAS EMPRESAS DE TELEFONIA E DE SERVIÇO MÓVEL CELULAR E PESSOAL) - Muito obrigado! Boa tarde a todas e a todos!

Excelentíssimo Ministro-Relator Cristiano Zanin, muito obrigado pela oportunidade, em nome de quem saúdo todos os demais membros da Mesa, em especial a Doutora Elizeta Ramos, subscritora da petição inicial desta ação.

Meu nome é André Cyrino, sou professor, falo como advogado da Conexis Brasil Digital, entidade que reúne as empresas de telecomunicações do Brasil, desde concessionárias de serviço fixo, autorizatárias de serviços móvel, empresas prestadoras de serviço de comunicação multimídia e serviço de acesso condicionado.

Ficamos honrados com a oportunidade de poder contribuir com tema tão relevante, em relação ao qual buscamos trazer nesta tribuna elementos tanto técnicos quanto jurídicos e, posteriormente, em memorial, como *amicus curiae*. Assim, trago elementos tanto de ordem técnica quanto jurídica que delineiam uma grande preocupação no setor de telecomunicações com essa discussão.

Em primeiro lugar, as associadas da Conexis, empresas de telecomunicações que são, não dispõem de ferramentas e pessoal capazes de realizar o monitoramento de dispositivos de usuários, tal como parecem fazer esses softwares espiões. Monitoramento pressupõe o acesso remoto de equipamentos e aplicações fora do escopo dos serviços dessas empresas. Isso por uma razão simples: na forma da Lei Geral de Telecomunicações, Lei nº 9.472, as associadas da Conexis não têm acesso às estações de telecomunicações e aplicações necessárias, entendidas como equipamentos, aparelhos, terminais e demais dispositivos, notadamente telefones celulares e *smartphone*s, na forma do art. 60, § 2º, da LGT.

O negócio das empresas que compõem a Conexis, como define o art. 60 da LGT, não é o dispositivo do usuário, os softwares nele instalados. Seu negócio é garantir a segurança, a qualidade e o conjunto de atividades que possibilita a oferta de telecomunicações, entendida na forma da lei como "a transmissão, a emissão ou recepção por fio, rádio, eletricidade, meios óticos ou qualquer outro processo eletromagnético de símbolos, caracteres, sinais, escritos imagens, sons ou informações de qualquer natureza." Esse é o limite de suas outorgas.

O foco das associadas da Conexis sempre foi, sem jamais deixar de cumprir as normas em vigor, Ministro Zanin, proteger meios de rede e serviços contratados por seus usuários, estes detentores dos aparelhos de telecomunicações, com a criação de sistemas que resguardem a privacidade, o sigilo e a segurança das comunicações, direito que já decorria do texto original da Constituição, art. 5º, X e XII, reafirmado recentemente no inciso LXXIX do art. 5º.

Por tudo isso, as associadas, que ora represento, jamais trabalharam para espionagem ou qualquer flexibilização dessa privacidade. Elas trabalham, muito pelo contrário, para a segurança do sistema. Monitorar usuários fora da interação comunicativa é a antítese do empenho que sempre tiveram as associadas da Conexis, um esforço absolutamente incompatível com as ferramentas que ora se discutem. Isso traz graves riscos porque, do ponto de vista técnico - e já

se foi dito aqui -, não se sabe com exatidão como funcionam essas ferramentas. Há dúvidas e há algumas opacidades muito graves. Logo, é impossível saber de antemão quais as dificuldades e impossibilidades técnicas, quanto à infraestrutura de telecomunicações, que adviriam do uso desses meios.

Não se trata, para fazer a comparação mitológica, de cavalos de asas, Pégaso, mas de cavalos de Troia, que, uma vez instalados, perde-se o controle. Não se sabe quando eles vão sair, como eles vão ser colocados - verdadeiras armadilhas. Uma vez dentro do sistema, seu controlador pode muito, para não dizer que pode tudo, o que traz riscos aos usuários, aos sistemas de telecomunicações e a terceiros que nada têm a ver com aquele que está sendo objeto de espionagem.

Vou falar um pouquinho dos riscos quanto a esses três grupos.

Primeiro, quanto aos sistemas de telecomunicações. Aqui foi muito bem falado, na parte da manhã, sobre o risco de que se incentive a criação de um mercado de vulnerabilidade.

Como se sabe, esses softwares precisam de portas, precisam de falhas no sistema. Tratar disso significa incentivar, de alguma forma - porque esses sistemas não são baratos -, economicamente, que se busquem mais falhas e que se

incentivem esses furos, o que não é buscado pela legislação e por todas as associadas da Conexis.

Há um risco também, obviamente, aos usuários de telecomunicações. O problema aqui é porque não há meios seguros de espionagem. Aliás, espionagem e segurança é quase uma contradição em termos. Não há garantia de que o operador da ferramenta cessará o uso quando expirado o prazo ou revogada a ordem judicial. Não há garantia de que o operador da ferramenta limitará o uso à finalidade da decisão judicial.

Disso decorre um risco para terceiros, pessoas que não têm nada a ver com a investigação. Fala-se aqui de soluções que permitem que se ligue a câmera, que se ligue o microfone, que se escute tudo o que está acontecendo ao redor, em espaços em que pode haver crianças, pode haver pessoas que não têm nada a ver com aquilo, que são absolutamente inocentes, que vão ter sua privacidade rasgada, enfim.

A Conexis, entretanto, ciente de todos esses problemas, não nega que o legislador pode criar meios de investigação que envolvam a coleta de dados. Ela tem absoluta consciência da sofisticação da criminalidade, o que exige também uma atualização das forças de segurança. Aliás, as suas associadas contribuem

efetivamente com investigações, fornecendo inúmeras informações, quando demandadas.

No entanto, o que se busca aqui é muito mais do que a interceptação telefônica, muito mais do que simples busca e apreensão de informações. Busca-se uma devassa, como foi dito pelo Doutor Marcelo Turbay, verdadeiras *fisher expeditions*, com monitoramento permanente e abrangente de tudo o que acontece ao redor de um aparelho celular.

Esse é um passo que, com todas as vênias, parece que vai na contramão do empenho do legislador de fazer valer o art. 5º, LXXIX, da Constituição, como se observa do Marco Civil da Internet, da chamada Lei Carolina Dieckmann, da Lei Geral de Proteção de Dados e da própria Lei Geral de Telecomunicações, estatutos que ilustram o esforço legislativo em atendimento à proteção e à confiabilidade dos sistemas. Daí a preocupação, preocupação com limites técnicos, éticos e jurídicos sobre o tipo de Estado de Direito que imaginamos para este país. Um Estado de Direito em que a eficácia bloqueadora de direitos fundamentais precisa ser efetiva, que é diversa de um Estado-espião - para usar a expressão que o Ministro Gilmar Mendes usou certa vez -, o modelo de Estado-espião mais agressivo do que o estado policial que não respeitava o asilo inviolável, mas que não dispunha de meios tecnológicos, para citar George Orwell, para

monitorar cada passo, cada som, cada imagem de cidadãos, um estado de coisas em que o segredo foi banido. Citando novamente *1984*, um estado em que, se você quer manter um segredo, você deve escondê-lo de si mesmo.

Parece-nos que esse ambiente pode aproximar-se não da lógica autorizada no art. 5º, incisos XII e LXXIX, mas da racionalidade do art. 139 da Constituição. Esse, sim, que, ao regular o estado de sítio, prevê a possibilidade maior de flexibilização de direitos comunicativos, esse, sim, relativo a um estado de exceção, uma situação necessariamente temporária e pontual, diversa de um excepcionalismo permanente, de um modelo de espionagem que remete assustadoramente a outro Giorgio, Giorgio Agamben, que tem alertado, em seus estudos, como o medo e a busca por segurança são cada vez mais utilizados para justificar ações de exceção.

Em conclusão, espera-se que essas complexidades para todo o sistema aqui trazidas sensibilizem esta Corte para que se conclua que o desenvolvimento das soluções tratadas nesta ação, que não estão ao alcance das associadas da Conexis, traz riscos reais aos serviços de telecomunicações e ao Estado de Direito. Um risco que precisa ser delineado e aprofundado com cuidado.

Excelentíssimo Ministro-Relator, muito obrigado! Boa tarde a todos!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor André Cyrino pelas colocações e passo a palavra para o Doutor Vinícius Vasconcelos, Vice-Presidente do Instituto Brasileiro de Direito Processual Penal. É advogado, doutor em Direito pela USP, com período na Universidad Complutense de Madrid, e pós-doutoramento na UFRJ, editor-chefe da *Revista Brasileira de Processo Penal*, professor doutor efetivo da Universidade Estadual de Goiás, também professor de PPGs em Direito do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa e da Universidade Católica de Brasília.

Doutor Vinícius, tem a palavra, por gentileza.

O SENHOR VINICIUS GOMES DE VASCONCELLOS (INSTITUTO BRASILEIRO DE DIREITO PROCESSUAL PENAL - IBRASPP E REVISTA BRASILEIRA DE DIREITO PROCESSUAL PENAL - RBDPP) - Excelentíssimo Senhor Ministro Cristiano Zanin, muito obrigado por essa oportunidade de fala! Cumprimento sua assessoria, em nome da Doutora Caroline e do Doutor Lucas, e demais servidores deste Supremo Tribunal. Cumprimento, igualmente, a Doutora Elizeta e o Doutor Marcelo Turbay, por acompanharem esta audiência e por toda essa abertura tão importante ao debate.

Falo aqui em nome do Instituto Brasileiro de Direito Processual Penal e, especialmente, como editor-chefe da *Revista Brasileira de Direito Processual Penal*. Trata-se de uma revista de acesso aberto, uma revista científica, com ampla

produção, que se tem consolidado como uma das principais fontes científicas no âmbito do Direito Processual Penal. Por isso, no debate entre inteligência e persecução penal, foco minha fala somente nos aspectos relacionados à persecução penal e ao uso dos aplicativos espiões na persecução penal.

Destacarei aqui algumas contribuições já produzidas na *Revista*, em alguns artigos, e cito três deles que vão embasar minha fala.

O primeiro, produzido por Luís Greco e Orlandino Gleizer, sobre o sistema alemão. Luís Greco, professor brasileiro, professor titular da Alemanha, trata muito bem, nessa exposição já mencionada aqui, de alguns aspectos das decisões do Judiciário alemão.

Depois, falarei um pouquinho sobre um artigo de Francesco Caprioli, sobre captador informático na Itália.

Por fim, algumas questões relacionadas ao papel dos tribunais constitucionais, tendo em vista que editamos um dossiê sobre esse tema, *O papel dos tribunais constitucionais no mundo na formação do devido processo penal*.

Existe um artigo de uma autora da Polônia que se chama Michalina Marcia sobre a importância da atuação dos tribunais constitucionais na limitação das novas tecnologias no processo penal.

Falarei uma mistura de todos os três para três pontos fundamentais.

Primeiro, ressalto a importância de respeito à legalidade. Destaco que, no cenário atual brasileiro, do mesmo modo que houve na Alemanha, não há uma normativa específica e o que temos, ainda que possa ser utilizado como uma colcha de retalhos, não seria suficiente.

Por fim, proponho ou sugiro alguns critérios, alguns parâmetros especialmente desenvolvidos na Itália e na Alemanha por esses artigos e pelas decisões, lá, dos tribunais.

Quanto ao primeiro ponto, é fundamental, como se tem desenvolvido e como já foi exposto, ressaltar a importância da legalidade para legitimar essas medidas invasivas. Temos aqui medidas invasivas que destoam do que existe até o momento.

Como já foi exposto, existem, no ordenamento brasileiro, algumas disposições esparsas, que têm avançado com legislações recentes, sobre infiltração *on-line* de agentes, sobre utilização, compartilhamento de dados e diversos outros aspectos, mas não há nada que regule, de modo específico e claro, uma medida invasiva que vai permitir, como no *hacking* governamental, a utilização dos próprios celulares como captação ambiental, captação de vídeo, rastreamento de GPS.

Na discussão da Alemanha, isso foi bastante claro. Nas decisões que começaram a surgir a partir de 2007 e 2008 e que foram reforçadas em 2016 até

a surgir a legislação, em 2017, mais ou menos, ressaltou-se a importância de traçar limites e estabelecer que o juízo de proporcionalidade, a ponderação de proporcionalidade, deve ser feita *a posteriori*. É necessário que, primeiro, exista uma autorização normativa para que depois, no caso concreto, a partir dos parâmetros de proporcionalidade, estabeleça-se se ela é justificada ou não. Como foi feito na Alemanha e em outros países, é necessário estabelecer como condição invariável que exista normativa específica para autorizar essas medidas. O IBRASPP se manifesta no sentido de que, como primeira opção, essas medidas invasivas de *hacking* governamental devem ser vedadas até que surja uma legislação específica.

Parece algo bastante grave, contudo, o Supremo Tribunal Federal já fez algo semelhante em relação à interceptação telefônica. Tudo bem que, na Constituição de 1988, havia uma normativa de eficácia limitada, que dependia expressamente de legislação, mas, até 1996, no HC 73.351, este STF vedou as interceptações telefônicas até que surgiu a lei em 1996. Óbvio que é algo bastante grave fazer uma vedação abstrata, mas é algo que já foi feito tanto no Brasil quanto no cenário internacional.

Passando para a segunda parte da fala, existem normativas internacionais e existe todo um debate internacional sobre parâmetros para isso. No ponto, a gente percebe que a segunda parte da fala, que vai propor alguns parâmetros, ressalta a primeira. Os parâmetros assumem uma complexidade tão

grande que talvez demonstrem a importância de que esse debate deve ser feito na esfera legislativa com maior tempo de digestão, com maior tempo de participação popular.

Temos no artigo *O papel das cortes constitucionais em reduzir os impactos negativos das novas tecnologias*, de Michalina Marcia, uma exposição de como os tribunais constitucionais têm feito, alguns deles, leituras dessas novas tecnologias a partir de precedentes antigos, e que isso tem resultado em uma proteção deficiente; e dá outros exemplos de tribunais constitucionais, como o Tribunal Constitucional da Alemanha, que, inclusive, como já foi falado pela manhã, estruturou um novo direito fundamental ou uma nova perspectiva de direito fundamental, e que aí sim têm avançado um pouco mais nessa limitação das novas tecnologias para a utilização de um módulo legítimo. O artigo conclui que precedentes antigos podem guiar a discussão, mas não podem orientar a limitação necessária dessas novas tecnologias.

Passo, a partir dos três artigos, a propor ou sugerir alguns aspectos de limitação. Primeiro - antes de passar para eles -, se este Tribunal entender que as medidas são legítimas de um modo excepcional, sustentamos que é necessário estabelecer um prazo para que o Congresso legisle. Isso existe em uma produção de tese de doutorado de Gustavo Soares, tese específica sobre o respeito

à legalidade das novas tecnologias no processo penal. Se houver a excepcionalidade de admissão dessas medidas, alguns parâmetros precisam ser estabelecidos.

Primeiro, reserva de jurisdição. É necessário estabelecer que essas medidas somente se legitimam com prévio controle judicial, a partir de uma justificativa em elementos concretos de investigação.

Segundo, subsidiariedade. Por analogia, é possível utilizar a legislação da interceptação telefônica, a legislação do agente infiltrado digital, que determina que essas medidas devem ser as últimas, somente se as outras não forem suficientes.

Terceiro, vinculação finalística. É necessário que a decisão judicial estabeleça o motivo dessa utilização, o motivo dessa captação de dados e que a sua utilização seja limitada a esse motivo.

Quarto, auditabilidade. É necessário estruturar mecanismos para permitir o respeito à cadeia de custódia. Esse é um tema em que se tem avançado bastante na jurisprudência deste Tribunal e do STJ. Em provas digitais, o respeito à cadeia de custódia, na posição majoritária da doutrina, acarreta uma consequência mais grave ainda do que nas provas físicas, diante da sua volatilidade.

Depois, fiscalização. Do mesmo modo que a legislação prevê, para agentes infiltrados, que o agente infiltrado deve fornecer um relatório

periódico para que as autoridades independentes façam uma verificação, também aqui sustentamos que as medidas de *hacking* governamental pressupõem uma fiscalização durante a execução da medida, a partir de relatórios mensais que podem ser oferecidos para algum outro órgão de controle, que pode ser independente daquele que tem feito, que está fazendo a medida. Fiscalização durante a execução, informação ao detentor de informação. Percebe-se que a legislação quanto à LGPD, que não se aplica diretamente à matéria penal, pauta-se muito na ideia de consentimento e informação.

Em matéria penal, temos algumas dificuldades, tendo em vista que, se a pessoa investigada for avisada, a medida vai perder sentido. Contudo, a partir do momento em que não haja mais risco para a execução da medida, pensamos, e é um critério importante, que se estabeleça um dever de informação à pessoa que foi investigada e que teve seus dados captados, para que ela possa saber o que foi captado, eventualmente exercer algum contraditório, inclusive ter alguma previsão sobre a exclusão desses dados de bancos de dados.

Por fim, algumas limitações. Limitação temporal da invasão. É necessário traçar um prazo máximo em relação à decisão judicial - e aqui podemos pegar por analogia a infiltração digital, que prevê 180 dias, renovável até um máximo total de 720 dias -, limitação temática temporal - os dados obtidos somente podem ser buscados e captados se vinculados ao período de investigação e ao

objeto investigação -, limitação subjetiva com relação à proteção de direitos de terceiros e limitação quanto ao cabimento em relação à proporcionalidade, estabelecendo quais crimes têm gravidade necessária para justificar essas medidas.

No geral, a partir desses dez parâmetros, sustentamos que esse tema é extremamente complexo, e isso só reforça a importância desse debate e a importância de que se avance na delimitação de parâmetros claros para proteger os direitos fundamentais no processo penal.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Vinicius Vasconcelos.

Agora, ouviremos, por videoconferência, o Doutor Vinicius Valentim, doutor em Ciência Política pela UFRGS e mestre em Direitos Humanos pela Universidade de Glasgow.

O SENHOR VINICIUS VALENTIN RADUAN MIGUEL (UNIVERSIDADE FEDERAL DE RONDÔNIA) - Boa tarde a todos os participantes!

Irei começar com uma brevíssima audiodescrição. Sou Vinicius, um homem de pele de cor clara, uso barba e cabelo castanho, tenho um óculos com armação preta, estou vestindo um *blazer* de cor acinzentada, com uma camisa branca, e o meu sinal de libras é este (sinaliza com a mão).

Falo do Grupo de Pesquisa e Intervenção em Direitos Humanos - Mapinguari, da Universidade Federal de Rondônia. Tentarei ser o mais preciso e pontual, dentro do tempo permitido, agradecendo mais uma vez a Sua Excelência o Ministro Cristiano Zanin e todos os demais partícipes da Mesa pela, eu chamaria, ousadia jurídica de proporcionar esse debate tão importante e crucial em tempos de tantos avanços e retrocessos em direitos fundamentais, sobretudo mediados pela tecnologia.

Sendo extremamente pontual, precisamos acenar que não se trata de mecanismos de intrusão remota, de possibilidade de *hacking* governamental, de um paralelo com aquilo que foi, em tempos outros, e ainda hoje transborda nesta Corte Constitucional, a discussão sobre escutas telefônicas. Esses novos mecanismos de intrusão virtual, remota, chamemos como quiser, são infinitamente superiores à mera escuta telefônica, conforme mencionado por outros expositores que falaram antes de mim. Mesmo na escuta telefônica, com todos os critérios e requisitos, controle externo da autoridade policial, vemos excessos e abusos. Inclusive tivemos abusos muito recentes, não somente com escuta telefônica de forma ilegal, interceptando gravações de escritórios de advocacia, de jornalistas, mas com discussões sobre quebra de sigilo de fontes de pessoas ligadas a profissionais da imprensa. Chegou também aqui outro tema de direitos fundamentais, a ADPF ajuizada pelo Partido Rede Sustentabilidade, com

relação ao chamado Dossiê de Antifascistas. Nesse momento, esta Corte deliberou não poder o Estado, por meio de qualquer de seus agentes, sob qualquer forma de justificativa, ainda que acessando dados públicos abertos de redes sociais de indivíduos, alimentados por eles próprios, fazer esse tipo de monitoramento, *a priori*, dos indivíduos, sem qualquer observância da reserva jurisdicional.

O primeiro paradigma que precisamos entender: esses *spyware*s, cavalos de Tróia, todos os softwares são algo que proporcionam e possibilitam uma devassa sem precedentes, incomparável com o que era a escuta telefônica. Podem possibilitar o acesso de informações que nada têm a ver com qualquer investigação, como por exemplo o acesso de gostos e preferências até mesmo de caráter sexual de um indivíduo, ou de suas compras nas redes sociais, ou do seu uso de qualquer dispositivo telemático. É uma verdadeira devassa, sem qualquer precedente até então encontrado.

Além disso, existem os chamados efeitos intimidatórios, os *chilling effects*. Os usos desses softwares monitorando jornalistas resultarão claramente em um efeito intimidatório significativo. Jornalistas ou outros profissionais da imprensa não poderão resguardar a segurança de suas fontes de qualquer maneira. Não teremos como resguardar, mediante a presença de uma vigilância massiva, formas de autocensura. Os próprios jornalistas evitarão cobrir

assuntos sensíveis ou politicamente delicados para proteger não só suas fontes, mas também a si próprios.

Com isso, chegamos a um outro paradigma que passa a ser objeto de ameaça: a própria confiança do público na imprensa passa a ser erodida ao saber que os jornalistas podem estar sendo, a qualquer tempo, monitorados.

Temos - não poderia deixar de falar aqui nessa segunda parte - uma série de riscos e implicações para os direitos humanos, não de uma forma somente abstrata e teórica, mas para a vida e segurança de ativistas e profissionais de direitos humanos em sentido mais amplo.

Esses softwares, como o FirstMile, Pegasus, entre outros, permitem a coleta de dados pessoais sensíveis, sem o conhecimento ou consentimento dos envolvidos, violando não só dispositivos telemáticos, mas também normas de telecomunicações e a intimidade e privacidade dessas pessoas.

Temos inúmeros registros, para usarmos uma ciência política e jurídica comparada, de casos que documentam que esses *spywares* foram empregados para invadir e espionar defensores de direitos humanos, ativistas e dissidentes políticos, resultando em detenções e mais represálias. Vários governos de caráter tecno-autoritário têm utilizado esses equipamentos, essas tecnologias e essas ferramentas para suprimir a oposição política e silenciar vozes críticas.

Há uma total falta de transparência sobre o funcionamento desses dispositivos, desses softwares. Não há uma regulamentação que facilite o controle social e o controle externo, mesmo quando submetido ao crivo da reserva de jurisdição, que responsabilize ou permita responsabilizar os perpetradores dessas violações, inclusive de forma transfronteiriça, uma vez que poderíamos facilmente ter agentes de outro Estado usando esses softwares aqui, em território nacional, contra terceiros, nacionais ou não, em qualquer lugar do mundo. Assim, temos uma erosão da confiança pública, temos uma ameaça à liberdade de expressão e à própria liberdade de associação.

Em democracias emergentes ou frágeis, essas ferramentas de vigilância vêm sendo utilizadas para suprimir a dissidência e consolidar regimes autoritários.

Peço agora que o cerimonial faça exposição do quadro que enviei com antecedência sobre os registros recentes de invasão por um único software específico que, entre 2018 e 2022, foi utilizado contra inúmeros jornalistas e ativistas de direitos humanos nos mais variados países.

Não sei se a apresentação está sendo feita

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Já está na tela. Está na tela a apresentação.

O SENHOR VINICIUS VALENTIN RADUAN MIGUEL (UNIVERSIDADE FEDERAL DE RONDÔNIA) - Perfeito, muito obrigado!

Vemos claramente que não existe um critério geográfico. Em todos os continentes tivemos casos de espionagem, sempre com a justificativa de possibilidade de controle pela segurança pública, pela segurança nacional ou pela segurança interna.

Passo agora, portanto, após todos esses pontos, a algumas recomendações e apontamentos gerais.

São indispensáveis a colaboração internacional e a conscientização pública para proteger direitos individuais e liberdades públicas, preservando as estruturas democráticas em um mundo cada vez mais digitalizado e, por isso, ainda mais sujeito às formas de tecno-vigilância.

É necessário que a Suprema Corte possa, ao final do julgamento desta ADPF, impor um embargo imediato sobre a venda, exportação, transferência e qualquer uso de tecnologias de vigilância que possam impor riscos aos direitos humanos fundamentais. Além disso, devem ser divulgados todos os contratos existentes e o uso de tal tecnologia por qualquer secretaria, autarquia, órgão público ou agente estatal, assim como estabelecido de forma clara quem é o responsável por controlar o controlador, quem vigia o fiscal. Também é importante a aplicação

de sanções a essas empresas. Foge do escopo desta ADPF, mas essas empresas devem ser objeto de investigação e ter suspensa qualquer possibilidade de realização de contratos com o poder público brasileiro até que demonstrem mudanças políticas que cessem os abusos e violações de direitos humanos em todos os países do mundo.

Era minha exposição. Muito obrigado! Mais uma vez, agradeço enormemente a oportunidade.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Vinicius Valentin pela exposição.

Agora, passo a palavra ao Doutor Renato Blum, que também fará sua exposição por videoconferência. O Doutor Renato Blum é advogado, economista, árbitro e professor, patrono regente do curso de Direito Digital, Proteção de Dados e Inteligência Artificial da Ebradi, mestre pela Florida Christian University, conselheiro da EuroPrivacy e membro da Associação Europeia de Privacidade. É presidente da Comissão de Estudos de Novas Tecnologias, Neurodireitos e Inteligência Artificial do Instituto dos Advogados de São Paulo. Escreveu e participou de diversas obras relacionadas ao tema de Direito, Tecnologia e Proteção de Dados.

Doutor Renato Blum tem a palavra, por gentileza.

O SENHOR RENATO OPICE BLUM (ESCOLA BRASILEIRA DE DIREITO - EBRADI) - Excelentíssimo Senhor Ministro Cristiano Zanin, Subprocuradora Elizeta Ramos, Doutor Marcelo Turbay. Agradeço o convite e a oportunidade de debater esse assunto tão relevante, que envolve nossas vidas tecnológicas e digital.

O primeiro ponto que gostaria de destacar e refletir envolve a questão da percepção de todos nós, e, aqui, sem exceção, sobre a evolução tecnológica. Quando falamos em interceptação, em uso de dados, fica cada vez mais difícil compreender onde estão esses dados e se esses dados estão ou não protegidos, do ponto de vista técnico, legal e jurídico.

Existem hoje, conforme já foi debatido aqui, vários aplicativos, várias soluções, vários programas de computador que possibilitam de forma aberta, portanto, sem interceptação, que é o que a lei hoje notadamente restringe, a obtenção de dados - dados de geolocalização, dados cadastrais (em parte previstos no Marco Civil da Internet), dados que revelam perfis, preferências e gostos, dados sensíveis em algumas situações (nem todas, até em função da Lei Geral de Proteção de Dados).

Entretanto, é nesse ponto que quero fazer o meu realce em relação a essas novidades tecnológicas, difíceis de serem compreendidas pela sociedade. Isso vai piorar. Cada vez mais, teremos dificuldade de compreender

isso. Essas aplicações de forma aberta, portanto, dentro de uma lacuna jurídica, podem propiciar o "uso legítimo" - bem entre aspas -, pelo menos do ponto de vista penal, especialmente em um momento em que se discute de forma tão intensa a inteligência artificial, que cresce a cada três meses e meio - no caso do ChatGPT, por exemplo, praticamente dobra. Fica cada vez mais difícil compreender essa evolução. É algo para se colocar nessa reflexão, até como proposta. Sabemos que já existem projetos, inclusive um deles, 2.338, deve ir à pauta na próxima quarta-feira no Senado, mas isso não afasta nossa discussão aqui, que envolve notadamente a questão penal.

Neste primeiro momento, então, queria trazer esse alerta sobre nossa dificuldade de percepção.

Qual é a consequência disso, quando a sociedade tem dificuldade de perceber o que é aberto, o que é fechado, quais são as soluções, onde estão esses dados - independentemente da questão penal, que deixo para o final?

A consequência é adotar ou dotar a sociedade, a partir da legislação, de mecanismos de alerta ou até de restrição quando ficar difícil de ter a expectativa de privacidade - a questão dos termos de uso: todo mundo clica, mas ninguém lê. No caso da proteção de dados, tanto a GDPR europeia quanto a LGBT brasileira, o próprio modelo chinês e de outros países trazem a figura do *Privacy by Default*. Não é o *By Design*, quando há a obrigação de incorporar proteções técnicas;

no *Default*, essas aplicações devem ser ativadas automaticamente. Invertemos a lógica se, por conta e risco próprio, o usuário quiser desativar. Ele desativa, mas vamos supor que ele tenha um mínimo de conhecimento para desativar aquilo que já vem pré-ativado. É uma inversão da lógica que temos hoje.

Lembrei uns minutos atrás, para fazer uma retrospectiva rápida, da invasão do painel do Senado em 2001, em que houve manipulação do programa e acesso ao resultado de uma votação. Na época, uma das figuras jurídicas interpretadas foi a do crime impossível, depois revertida pela Lei nº 9.983, e nós tivemos a figura da manipulação - arts. 313-A e B do Código Penal. Isso foi evoluindo e hoje temos a Lei nº 9.296 falando sobre fluxo da interceptação - assim é o reflexo penal -, fluxo das comunicações; quando houver fluxo - é importante isso -, aí sim é ilicitude. Temos também uma questão curiosa na própria nº 9.296, no art. 10-A, que trata da captação de sinais eletromagnéticos e que traz inclusive a figura sobre a possibilidade (por parte não da polícia, polícia só com ordem judicial), sem ordem judicial, de alguém que esteja participando de determinada circunstância.

O que é um sinal eletromagnético hoje? O que será daqui a seis meses? Não posso deixar de falar, de fazer uma conexão, com os chamados neurodireitos, figura jurídica nova, que traz muitas preocupações.

Temos registros históricos de algumas questões técnicas. O conceito de sistema aberto, protocolo SS7, por exemplo, possibilitava, no passado - não que seja 100% garantido, mas foi corrigido em parte -, a identificação de um telefone, as ligações que recebemos no nosso próprio número, por meio da manipulação de sistemas de mensagens automáticas. Isso deve ser considerado dentro do conceito de dados abertos ou de questões técnicas do próprio acesso à internet, do conteúdo, da telecomunicação etc. A figura do *Steam Grey* foi inclusive julgada, em 2012, nos Estados Unidos. O que é o *Steam Grey*? É quando há a emulação de uma estação de rádio-base próxima da verdadeira estação de rádio base. É mais ou menos o seguinte: eu uso o meu telefone celular para se conectar com a torre da operadora. Aparece o nome da operadora, mas, do ponto de vista de eventual ilicitude, pode haver a instalação de uma minitorre, com a mesma identificação. Aí a figura jurídica seria outra, não a interceptação em si, de uma minitorre, emulando conexão com o mesmo nome. Não teremos diretamente a interceptação, mas o uso daquele canal de comunicação a partir de um ardil. Foi julgado como ilegal nos Estados Unidos, caso Estados Unidos contra Graham, em 2012.

Dentro do que foi abordado aqui, para chegar já no final, o foco principal é o *Privacy by Default* dentro da questão de percepção *versus* inteligência artificial e a própria produção da evidência. Para não gerar nenhum tipo de

confusão com respeito à cadeia de custódia, cada vez mais profunda, prevista no Código Penal, com relação e alusão a normas técnicas, temos aqui dois, três exemplos rápidos. Sobre a utilização de telas de WhatsApp Web - o WhatsApp Web é uma emulação do WhatsApp nativo nos nossos dispositivos -, em que a estrutura de software é diferente, ela permite alguns acessos que não temos nos nossos aplicativos. Isso já foi analisado pelo STJ inclusive e, na terceira decisão, a primeira e a segunda foram revertidas. Não é o fato de o WhatsApp Web ser mais inseguro que vai levar à invalidade da produção da prova.

Temos também a questão das portas lógicas. O Marco Civil fala em guarda de IP, data e hora, mas agora temos uma jurisprudência majoritária determinando a guarda da porta lógica - números que servem para identificar a origem da conexão por força da mudança do IPv4 para o IPv6. O IPv4 é aquele número antigo de conexão à internet, de domínio. Esses domínios se esgotaram e migramos para o IPv6, que é quase infinito, só que ainda existem sistemas que compartilham. Em uma hipótese de investigação criminal, em uma ação de quebra de sigilo, por exemplo, posso ter, no resultado da quebra, trinta suspeitos. Obviamente, não será feita a busca e apreensão desses trinta suspeitos.

Por fim, tentando amarrar todos esses conceitos, minha finalização, em síntese, seria a seguinte: a dificuldade de percepção vai piorar.

Sobre a evolução tecnológica, cada vez mais rápida, sobre a dificuldade de percepção *versus* evolução tecnológica, teremos - teremos, eu digo, a sociedade, os órgãos de percepção penal, o Judiciário, todos nós - cada vez mais dificuldade em identificar se os dados são acessíveis, são abertos ou fechados, se são legítimos e a sua própria origem. E nem discutimos aqui a questão da competência, da jurisdição, institutos que por si só agravam o efeito prático do que está sendo debatido aqui.

Por fim, dada essa dificuldade toda - terceira vez que vou mencionar uma sugestão -, privacidade por *default* como regra e interpretação dentro do princípio da reserva legal. É assim no nosso sistema jurídico. Se determinada conduta não está tipificada, como, por exemplo, uma invasão, citando aqui inclusive o art. 154 do Código Penal, ou a interceptação de fluxo, com base na Lei nº 9.296, temos duas soluções possíveis. A primeira solução é a absolvição, e, aí, vamos questionar como fica a percepção e admissão da sociedade; a segunda solução seria a evolução legislativa.

O último ponto a que faço menção direta é sobre a mudança dessa evolução legislativa, que deve ser dinâmica. Falamos na mudança de estrutura de desenvolvimento de uma lei. As leis ordinárias podem não ter mais efeito ante a rápida evolução tecnológica. Temos que achar uma outra forma.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutor Renato Blum, pela exposição e passo a palavra à Doutora Estela Aranha, advogada, membro do Conselho Consultivo de Alto Nível da ONU para Inteligência Artificial, ex-secretária de Direitos Digitais do Ministério da Justiça e Segurança Pública e ex-presidente da Comissão Especial de Proteção de Dados do Conselho Federal da Ordem dos Advogados do Brasil.

Doutora Estela Aranha, tenha a palavra, por gentileza.

A SENHORA ESTELA ARANHA (CONSELHO CONSULTIVO DE ALTO NÍVEL DA ONU PARA INTELIGÊNCIA ARTIFICIAL) - Boa tarde, excelentíssimo Ministro Cristiano Zanin, excelentíssimos Doutora Eliseta Maria, Doutor Marcelo Turbay, Doutor Lucas Salles, Doutora Carolina Lima, todos os meus colegas que estão expondo e assistindo aqui.

Nas exposições aqui, hoje, se falou de diversos tipos de dispositivo. Eu vou me ater aos programas de intrusão virtual remota, de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, como é o tema desta audiência, que são os chamados *spywares*, que fazem a interceptação e são disponibilizados hoje no mercado internacional, aí o que a gente está discutindo. A natureza técnica desses dispositivos é essencial nessa discussão, porque as características técnicas acabam sendo determinantes para a avaliação jurídica.

Como até deixou claro na primeira parte a Doutora Raquel, do IP.rec, entre outros que me antecederam também falaram isso, uma característica fundamental desse dispositivo é que ele funciona a partir da exploração de vulnerabilidades da infraestrutura de redes de telefonia ou de infraestruturas críticas, sistemas operacionais dos aparelhos. Como por exemplo, tem uma ação da Apple contra o sistema Pegasus nos Estados Unidos ou, então, do WhatsApp contra esse mesmo sistema que busca *backdoor* nas suas criptografias. São *hackers* notórios, como são falados aí.

Existe, para isso, um mercado sobre conhecimento de vulnerabilidades em sistema de software, que é negociado diretamente entre partes ou facilitado por corretores. Esse mercado inclui uma série de intervenientes não estatais e, obviamente, organizações criminosas.

Tem um excelente trabalho de uma ONG canadense, Citizen Lab, que mostra leilões dentro da internet para pagamento de *hackers*, buscando achar esse tipo de vulnerabilidade. Inclusive tem denúncias de ex-funcionários, por exemplo, dessa empresa que eu falei, que tem esse sistema, a NSO, que roubou o código fonte da empresa para vender dentro dos *insiders* da indústria.

Eu vou trazer um pouco da discussão que eu tinha bastante, enquanto eu era assessora especial no Ministério da Justiça e, depois, secretária de direitos digitais, e a gente trazia essa questão como fundamental do nosso trabalho.

Um exemplo, que a gente intensificou o debate, é até o sistema FirstMile que está dentro do Inquérito 4.781, aqui, no STF, que é do sistema Cognite, que tem vários produtos vendendo aqui para esse tipo de intrusão.

Essa empresa, por exemplo, ela explora a vulnerabilidade da rede de telefonia brasileira, como mostraram diversas matérias de jornal. Inclusive, pelo que saiu na imprensa, o uso de equipamentos teve que ficar suspenso por alguns dias, não se pode usar porque a TIM, acho que foi a TIM, uma telefonia conseguiu localizar e fechar essa porta de vulnerabilidade, inclusive, fizeram um aditivo de contrato, oferecendo mais uso depois justamente porque tiveram que buscar outras vulnerabilidades para continuar trabalhando.

Então, essa vulnerabilidade quando você abre, você pode pegar qualquer dado. Você abre uma vulnerabilidade em que você vai expor dados confidenciais, informações, registros financeiros, registros de saúde, leva a roubo de identidade, fraude, mas também questões em relação à própria segurança nacional, a cybersegurança, de modo geral, há questões de geopolítica internacional, até porque grande parte desse mercado são softwares fabricados fora do Brasil e em alguns poucos países.

Existe até um parecer técnico da Polícia Federal, dentro desse inquérito, eu sei em linhas gerais, porque ele está em segredo de Justiça. Então, eu não sei se esse segredo da Justiça poderia ser aberto, mas se pudesse ia instruir

muito o debate dessa ação aqui, porque mostra justamente como esse tipo de software funciona aí pelo que nós ouvimos falar pela imprensa.

Então são importantes algumas coisas. Em primeiro lugar, a exploração dessa vulnerabilidade afeta interesses fundamentais de segurança nacional, de política externa. Os riscos dessas tecnologias emergentes podem representar para as instituições, para todo o pessoal, informações do próprio Brasil, por exemplo, permite que o governo ou outros atores hostis se infiltrem, indivíduos organizações e governo, sem conhecimento nenhum ou consentimento. Nós sabemos que, por exemplo, num cenário de guerra, tivemos membros do governo com seus próprios celulares infiltrados, neste caso, justamente nessa discussão geopolítica.

Em segundo lugar, que dessa forma é impossível garantir que a tecnologia desenvolvida neste mercado privado seja implantada, governada de acordo com os direitos fundamentais, com o Estado do Direito, com a autorização legal, com salvaguardas, supervisões apropriadas, de modo que apoie e não prejudique a democracia e os direitos civis e a liberdade civis e também a própria segurança pública.

Além de tudo, esses *spywares* comercializados ameaçam o livre fluxo de dados de comunicação e, sobretudo, o que a gente chama a confiança. Os

Estados Unidos, por exemplo, colocaram grandes salvaguardas em relação ao uso da maioria desses softwares comerciais.

Em terceiro lugar, já foi também explorado pelos expositores, há um impacto geral na sociedade pela capacidade desses dispositivos. Eu dou o exemplo do Pegasus, que tem maior literatura, mas ele acessa remotamente dados e comunicações confidenciais no dispositivo móvel, rastreia comunicação e suas atividades, coletam dados de todos os tipos, mensagens, fotos vídeos, localizações, senhas e assume o controle do dispositivo.

E ele pode manipular as funções do dispositivo como ligar, desligar microfone, câmera. A gente já falou sobre excluir arquivos, mudar aplicativos e também tem módulos de autodestruição responsável por remover seus vestígios de quando ele foi invadido, ou para não se detectado por nenhum sistema de segurança.

Além dessas vulnerabilidades gerais, têm duas vulnerabilidades específicas: essa possibilidade de manipular dados, ela traz um grande risco para a cybersegurança, para confiabilidade de todos os sistemas de infraestrutura crítica, quando você acessa um sistema de telefonia, você acaba tendo essa integridade que você pode usar para qualquer coisa, não só para espiar, mas para fazer qualquer vulnerabilidade e também você pode alterar qualquer coisa em qualquer dispositivo e alterar sem vestígios.

Então, eu quero trazer um outro problema. É que a gente fala muito sobre a integridade da informação de modo geral e também no devido processo legal. A gente um pouco antes de discutir *deep fake* e outros conteúdos sintéticos e aí a gente também tem esse uso de *spyware*, que pode modificar qualquer conteúdo e acabar com a confiança de qualquer ambiente digital, inclusive na cadeia de custódia das provas digitais, que é uma garantia de natureza constitucional, ela não é uma mera consequência lógica do sistema de preservação do corpo de delito digital e ela afeta, então, os direitos fundamentais, a confidencialidade e a garantia de integridade dos sistemas de tecnologia de informação.

Enfim, há várias coisas aqui, mas eu queria remeter a alguns problemas que nós temos quando a gente fala em regular esses softwares. A gente viu a ideia do uso generalizado desses softwares. A proposta que está no Senado, por exemplo, autoriza para qualquer membro de forças policiais - membros e entidades -, secretarias estaduais, serviços nacionais de inteligência, que imagino que sejam Abin, Receita, Coaf, Polícia Rodoviária Federal, Polícia Penal, Senasp, Forças Armadas e seus membros.

Então, a gente está imaginando aqui que, assim como há o guardião, todos os presídios, todos os batalhões de PM, bombeiros, comandos militares, todo lugar terá o seu *spyware* com essa capacidade, com essa potência,

cujo risco foi, inclusive, mostrado anteriormente, que é um risco imenso e é um risco irreversível, se nós autorizarmos, porque a potência disse é muito grande. Nós não temos nenhum tipo de rastreabilidade, de auditabilidade, de controle e de poder de supervisão, com esse enorme poder de intrusão.

Nessas discussões que nós tivemos no Ministério da Justiça, a Polícia Federal trabalha - inclusive a Diretoria de Inteligência da Polícia Federal - com o uso parecido com o que funciona hoje com a interceptação de telefone. A partir do momento em que você consegue ter as mesmas informações necessárias para a investigação criminal e para a persecução penal, quando as companhias telefônicas sejam obrigadas, assim como elas são na interceptação, a passar os dados, as polícias simplesmente vão trabalhar os dados no mesmo modelo da interceptação.

Eles já fizeram testes em relação ao uso disso, basta também a Anatel junto. Já há conversa com a Anatel - e seria importante a Polícia Federal para conversar aqui. Existem outros meios que não o uso de *spyware*, que não tem controle nenhum, para que sejam feitas a persecução penal e a investigação criminal com todas as devidas garantias, rastreabilidade, supervisão e confiança nos sistemas computacionais.

Então, o meu encaminhamento é nesse sentido de vedar o uso de *spyware* de modo geral, inclusive com a possibilidade de criminalizar esse uso, justamente para não se espalhar, e a partir daí você trabalhar com um sistema parecido hoje, que é o da interceptação telefônica, que é absolutamente possível e que vai permitir a persecução penal e a investigação criminal do mesmo modo.

Obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Estela Aranha pela exposição.

Agora, passo a palavra ao Doutor João Ataíde, especialista em inteligência artificial e servidor público federal do Superior Tribunal de Justiça.

O Doutor João Ataíde tem se dedicado à capacitação de gestores e líderes no âmbito do serviço público e empresas corporativas, atuando como instrutor na ação de desenvolvimento gerencial. É especialista em criação de GPTs, engenharia de *prompts* e criação de agentes com inteligência artificial.

Doutor João Ataíde, tem a palavra, por gentileza.

O SENHOR JOÃO FELIPE ATAÍDE DA CUNHA RÊGO (GESTOR PÚBLICO) - Muito obrigado, Ministro Cristiano Zanin, na pessoa de quem cumprimento todos, a excelentíssima Procuradora, todos os Juízes Auxiliares e o representante da OAB, Doutor Marcelo.

Eu sou o João Ataíde e sou entusiasta de inteligência artificial já há dois anos, quando começou a questão do GPTs, que explodiram de uma forma muito, digamos assim, até sem controle do que está acontecendo.

Eu quero trazer essa clareza, porque isso, no caso, é uma forma de expandir a velocidade do que está acontecendo com relação à captura de dados. Hoje, as *big corps* estão investindo bilhões, chegam a ser bilhões, na captura de dados e esses dados vão valer ouro, vão ser o novo petróleo.

Vídeos que nós estamos fazendo aqui neste momento, por exemplo, no YouTube, valem ouro. Uma IA consegue extrair o que está sendo falado aqui hoje, gerar propostas, gerar soluções, com base, inclusive, no arquétipo que Vossa Excelência tem como essência, que é, digamos, o mais grave. É, digamos assim, uma espionagem mais agressiva e a comunicação mais intensa, nesse sentido.

Eu quero trazer, aqui, essa questão de que há necessidade - eu li a petição inicial da excelentíssima Procuradora - da necessidade imediata de uma regulação, porque os dados não estão sendo capturados. Eles foram capturados já. Esse é o ponto. Eles não estão sendo, já estão capturados. E o que vai ser feito com isso? Nós não temos noção do impacto que vai acontecer.

No marketing digital - Vossa Excelência perguntou mais cedo ao outro colega sobre a questão do uso nas empresas privadas - isso é utilizado em massa, porque uma empresa privada, ela usa um sistema de espionagem da outra, que é o chamado *bitmarketing*. Ou seja, isso simplesmente transferiu para o serviço público e nas mãos de pessoas que se não tiverem uma intencionalidade correta, vai ser algo devastador. Por quê? Quem tem os dados, tem o quê? Poder. Não é isso? Tem o - como é que chama -, tem, como diz, aqui, o Yuval Harari, no seu livro *21 lições para o século 21*, ele fala o seguinte: os algoritmos poderão nos conhecer melhor do que nós mesmos, prevendo nossos desejos e manipulando nossas escolhas.

Então, quantas vezes alguns dos senhores, aqui, já compraram algo que não necessariamente queriam? Por quê? Porque simplesmente a mensagem tocou no seu arquétipo, no seu eneagrama, na forma como você comunica, na forma como você age. E isso é o grande ponto que eu quero trazer aqui.

E imagina isso na mão de políticos que querem literalmente dominar a massa, que dominam a massa já, hoje, mas esse canhão, essa potência nas suas mãos, de forma irregular, de uma forma que não seja controlada, como diz a Procuradora aqui.

Estamos, aqui, então, diante dessa ação, ADI por omissão parcial, como existe, aqui, algumas normas anteriores e tal, que já regula alguma coisa, mas, na verdade, estamos diante de uma grande - eu falo assim - bomba atômica de que está acontecendo com a IA, porque a IA, ela come o marketing digital no café da manhã, porque ela não multiplica, ela duplica semanalmente.

Recentemente a GPT, eles abriram a loja do OpenAI para softwares, ali, que você pode criar com base em dados que você tem, ou que são capturados de forma irregular, gerando outros sistemas que estão sendo vendidos já. Isso de forma gratuita. E isso sem regulação nenhuma, entendeu? Por que eu estou trazendo a IA? Porque ela é o potencializador do que a gente está discutindo aqui. E eu vejo a importância dessa discussão principalmente pelo fato de que isso, aqui, vai ser, digamos, até o marco inicial da regulamentação também da IA. Por quê? Porque uma coisa está ligada à outra.

Eu vejo, eu tenho essa percepção, porque estamos, aqui, diante de princípios, que são a segurança, verdade, justiça, segurança nacional, principalmente.

Eu, como servidor do STJ, os processos do STJ são armazenados na nuvem, Microsoft, e isso a gente não sabe, nem tem noção que ponto, que pode acontecer, de que vasos passem, transpassem para outro governo, para outro país, que domine o nosso país. A gente não tem essa clareza. E pelo que falam, questão

do regulamento, lá, existem muitas exceções. Não existe segurança. Onde tem um cadeado, existe uma chave, entendeu? Então, assim, se essa chave existe, ela tem que ser muito bem trancada, ela tem que ser muito bem regulada, ela tem que estar muito bem delimitada.

E com base, por exemplo, na questão da gerente de *prompt* no GPT. O que é um *prompt*? É o comando. No seu comando, ele existe o quê? Um contexto e um exemplo. Então, aproveitando esse conceito de *prompt* básico para avançado, é que nós temos, aqui, o seguinte: dentro desse contexto que nós estamos vivendo aqui hoje, dentro dos exemplos que temos aqui hoje, tanto de Direito Comparado, como os outros colegas, aqui, expuseram já mais cedo, quanto ao que vai acontecer, muito em breve, temos, aqui, a oportunidade de lançar, como uma nação pioneira, talvez, uma regulação imediata dos dados, porque você não tem mais acesso à privacidade. Essa é a verdade. Nós estamos sem privacidade. Inclusive o Mark Zuckerberg, dono do Facebook, ele, quando se posiciona na frente do computador dele, ele tampa a câmara do computador, porque ele não garante, ele não tem garantia nenhuma de que não está sendo filmado. Isso é o grande perigo.

E a gente também não tem noção. Eu, debruçando-me sobre esse tema aqui, comecei a ficar muito mais receoso de estar perto do meu celular em determinadas situações, porque você está sendo gravado, seus dados estão sendo

gerados, e não tem almoço grátis. Os dados, nós somos reféns dos sistemas. Gmail, por exemplo, está tudo lá, seus dados estão lá, sua vida está lá. Ele sabe como é que você pensa, como é que você age, sabe o que você quer, sabe o que você não quer. Então, se você gerou dados e teve recompensa, que é o uso de ferramentas que nós temos hoje, o GPT é uma ferramenta que está sendo disponibilizada de forma gratuita. Não, não é gratuita. Então eu chego à conclusão de que, se não houver uma regulamentação nisso - e essa oportunidade de hoje trazer clareza nisso -, essa questão da privacidade, que já, a meu ver, não existe, no nível que deveria existir, no nível mínimo de segurança, simplesmente, cada vez mais, como diz Yuval, nós seremos ali como se fosse gado no pasto. A tecnologia não nos servirá mais, mas sim nós serviremos à tecnologia. Esse é o ponto que eu quero trazer aqui e deixar bem registrado, também com mais detalhes nos memoriais enviados ao gabinete.

Muito obrigado, Doutor.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor João Ataíde.

PERGUNTAS AOS EXPOSIDORES

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Chegaram já algumas perguntas. Eu começo, na verdade, fazendo uma pergunta ao Doutor Sauvei Lai.

Doutor Sauvei, Vossa Excelência mencionou, durante a sua exposição, sobre a necessidade de novos meios ocultos de investigação. Vossa Excelência sabe dizer se já existem decisões judiciais que autorizaram o uso desses novos meios? E quais foram as ferramentas autorizadas, na hipótese de a resposta à primeira pergunta ser positiva?

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - Boa tarde, Excelência, obrigado pela pergunta. Sim, no eslaide que nós vimos, não só houve autorização dessas cortes em solo europeu, mas também por conta do uso desses programas de invasão, de infecção de vírus em dispositivos eletrônicos do suspeito - é claro que a gente fala de dispositivo móvel, mas pode ser um dispositivo fixo também -, por conta desse uso, a jurisprudência europeia foi forçada a se debruçar nas questões. Como a Professora Laura Mendes destacou, algumas cortes, no início, consideraram inconstitucionais por falta de parâmetros, mas, na sequência, ajustando as decisões dessas cortes, o legislador europeu começou a regulamentar. Então nós temos, como eu disse, no *StPO*, o Código de Processo Penal da Alemanha, está especificamente no art. 100, eles chamam de *on-line-Durchsuchung*, que é busca *on-line*. Nos próprios Códigos de Processo Penal espanhol e italiano foi muito mais interessante, porque, ao contrário da corte alemã, que declarou a inconstitucionalidade no início, forçando o legislador alemão a regulamentar, as

cortes espanhola e italiana aceitaram o uso desses programas e, na sequência, houve uma disciplina legislativa. Então nós temos sim não só decisões favoráveis nos Estados Unidos, que foi o pioneiro em 1999. A corte de New Jersey, no caso da máfia novaiorquina, autorizou, em 1999. O Brasil está atrasado nesse assunto. Em 1999, já temos decisões norte-americanas. No início de 2000, temos decisões nas cortes europeias. E na década de 2010, temos regulamentação expressa na legislação.

O que me causou muita surpresa é que nós temos também uma regulamentação, que eles chamam de Hipcar, a Harmonia dos Países Caribenhos. Em 2013, eles regulamentaram o uso do que eles chamam de *remote forensic*. Então, é uma busca remota forense, é uma infecção à distância para que possibilite o uso desses programas, até porque, repito, ao contrário de muitos aqui que sustentaram, hoje, outros meios tradicionais estão fadados ao fracasso, até porque foram meios que foram planejados por uma outra era tecnológica.

Hoje não se usa mais interceptação telefônica. Eu sou promotor de justiça há 25 anos. Os meus bandidos do Rio de Janeiro não usam mais o telefone, não usam nem mais o WhatsApp, porque o WhatsApp ainda coopera com a Justiça brasileira. Eles estão usando já Signal, Telegram. E lá fora, como a gente explicou, o caso EncroChat, da Aeropol, o caso Anom, que foi do FBI, houve infecção. Eu esqueci de falar isso na minha sustentação. Esses sistemas internos de comunicação

dessas criminalidades organizadas internacionais só foram desbaratados com o uso tradicional de colaboração premiada: o diretor de tecnologia de informação dessas organizações que permitiu infectar os dispositivos.

No ano passado, nós tivemos outro caso, o do Sky ECC, que me apavorou, porque foi uma grande rede de traficantes internacionais da Europa, mas com dois brasileiros traficantes usando esse sistema interno de telecomunicação. Eles não estão nem usando mais WhatsApp, Telegram ou Signal. Já estão desenvolvendo o próprio sistema de telecomunicação, que a gente só vai conseguir acessar, por causa da criptografia, se houver essa infecção.

É óbvio que essa intrusão estatal viola direito à privacidade, à liberdade de expressão, à autodeterminação informativa, os novos bens jurídicos informáticos, a confidencialidade, a disponibilidade, a integridade. Isso tudo tem que ser parametrizado pela legislação, que o Tribunal Europeu de Direitos Humanos chamou de *quality law*, uma lei de qualidade. É uma lei clara, precisa, compreensível para os cidadãos dos limites dessa intervenção que deve ser sempre proporcional.

Muito obrigado pela pergunta. Espero ter respondido.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Só uma complementação.

Vossa Excelência tem conhecimento de decisões judiciais que tenham autorizado o uso desses novos meios ocultos de investigação no Brasil?

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - Eu desconheço. Nós não temos nenhuma autorização judicial dentro dos tribunais superiores e nem nos tribunais de primeira instância. O que nós temos, recentemente, são as jurisprudências do espelhamento, WhatsApp Web. Inclusive houve uma mudança recente na jurisprudência do STJ, que proibia antemão, mas passou a admitir, e também, mês retrasado, a vedação do uso dos *prints* do WhatsApp, até por violação da cadeia específica - cadeia de custódia - das evidências digitais.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Sauvei.

Doutora Elizeta, alguma pergunta? Doutor Marcelo Turbay?

O SENHOR MARCELO TURBAY (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL) - Ministro, teria uma pergunta bem breve para a Doutora Estela Aranha.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois não.

O SENHOR MARCELO TURBAY (CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL) - A respeito do caso FirstMile, que ficou

nacionalmente conhecido, inclusive sobre alcunha de Abin paralela. A imprensa veiculou inúmeras notícias sobre esse caso, Estela - e aproveito para cumprimentá-la pela fala e densidade da exposição.

Apenas uma pergunta: quando Vossa Senhoria ocupou a Secretaria de Direitos Digitais, chegou ao conhecimento do governo alguma outra tentativa de utilização, ou mesmo a utilização por algum outro órgão investigativo, ou agência de inteligência, ou mesmo algum ente privado, de um software como o FirstMile ou mesmo o Pegasus? A empresa também noticiou que o Pegasus foi objeto de uma tentativa de licitação, em 2021, que acabou não acontecendo.

Enfim, apenas para trazer mais elementos à discussão, se de fato houve a identificação dessa tentativa, ou efetiva utilização desses programas no Brasil?

A SENHORA ESTELA ARANHA (CONSULTIVO DE ALTO NÍVEL DA ONU PARA INTELIGÊNCIA ARTIFICIAL) - Obrigada, Doutor Marcelo.

Na verdade, temos notícias que estão sob investigação criminal e, aí, com o devido sigilo da Polícia Federal. Não conheço detalhes, né? Temos só a notícias de que outros órgãos poderiam estar usando o próprio FirstMile. Também houve um caso - ficou famoso, saiu na imprensa - sobre o uso pela Polícia Rodoviária Federal, no qual teve uma emboscada, com algumas mortes, justamente

porque soube da localização por um tipo de *spyware.* Nós temos um *spyware* privado e é bem famoso, irei pegar em minhas anotações o nome. Sim, nós temos, e alguns tipos de *spyware* estão sendo vendidos na internet, os quais são colocados no telefone das pessoas para saber de traições e outras questões privadas. E sim, um dos trabalhos que estávamos tentando fazer era em relação a esse mercado privado de venda de tipos de *software* de espionagem.

Enfim, alguns softwares *malware* não usam essa infraestrutura crítica, não têm acesso a essa... você teria que dar um *click* ou teria que saber, mas também a gente vê avançando que você não tem menor notícia, você não consegue ver no seu próprio telefone por meio de infraestrutura telefônica. Isso nós tivemos também notícias e está sob investigação da Polícia Federal, mas tanto que saem na imprensa, tem discussões de modo geral. Mas eu tenho certeza de que, sob a investigação da Polícia Federal, também existe na continuidade desse processo.

E sempre é muito importante destacar isso, o uso desses instrumentos de tal grau de intrusão na Constituição Federal é restrito, já que invade a competência das comunicações telefônicas, telemáticas. De modo geral, ele precisa, obviamente, da previsão legal e é de competência exclusiva das forças de investigação e de persecução penal. Isso não é caso, por exemplo, de atividade de inteligência, que é uma coisa mais ampla; e que não cabe a esses tipos de órgão, como a inteligência de outras polícias ou da polícia militar, esse tipo de uso de

software, porque ele é restrito à polícia judiciária. Obviamente pode-se trabalhar em conjunto, pode-se ter protocolos etc. Mas esse uso é restrito para a polícia judiciária, que vai trabalhar na investigação criminal ou na instrução do processo penal.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado.

Doutora Caroline Santos Lima, juíza instrutora, teria uma pergunta?

A SENHOR CAROLINE LIMA (JUÍZA INSTRUTORA) - Uma pergunta para o Doutor Sauvei Lai, até complementando o que já foi dito. Vossa Senhoria mencionou que a interceptação hoje já não surte os efeitos que tinha há alguns anos, talvez até mais de década. Então, entre 2000 e 2005, ainda era bastante utilizada.

Na prática, a autoridade policial ou o Ministério Público requisitava a interceptação para o juízo; o juízo avaliava uma série de requisitos, expedia um ofício para as operadoras de telefone. A operadoras então mantinham funcionários na área da interceptação, que, durante determinado período, produziam aqueles dados e devolviam para o juízo os dados que haviam sido coletados e que depois eram levados ao conhecimento da autoridade que estava na investigação.

Com relação a esses aplicativos, softwares, hoje em dia, qual é o procedimento que é utilizado nas investigações? Eu queria saber o *iter*, o caminho que é percorrido entre aquele momento em que se detecta a necessidade de utilizar para fins de investigação, como foi colocado na exposição, qual é o caminho percorrido? Quais são as autoridades envolvidas ou os atores que participam desse percurso?

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - Obrigado pela pergunta. Depende do país.

A SENHOR CAROLINE LIMA (JUÍZA INSTRUTORA) - No caso brasileiro.

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - No Brasil, o ideal - porque nós não ainda temos um parâmetro do procedimento; ao contrário, por exemplo, da Espanha, como expus, em que o juiz pode autorizar de ofício -, aqui nós temos uma tradição justamente para que haja uma prévia provocação do juiz, seja mediante requerimento do Ministério Público, seja mediante representação da autoridade policial, que vai ser submetida a um controle jurisdicional bem rigoroso, não só em abstrato, de quais são os crimes especialmente graves que vão comportar esse tipo de meio oculto de investigação e também de uma fundamentação

concreta. Ou seja, diante daquele caso individual, quais são as circunstâncias que realmente justificam a adequação dessa prova; por que essa prova é apta para se descobrir, para se desvendar o crime; por que ela é necessária; por que não existe um outro meio menos gravoso para se obter esse tipo de evidência.

É a chamada proporcionalidade em sentido estrito, ou seja, o sacrifício da privacidade do suspeito tem que ser menor do que o benefício almejado. Não vamos disparar uma bala de canhão para matar uma mosca; investigar, por exemplo, a um crime de menor potencial ofensivo. Mas, no caso, de novo, de pornografia infantil, crimes hediondos, esses, sim, são os crimes especialmente graves.

Depois de autorizado judicialmente, o que a gente percebe na França, na Espanha, na Alemanha é que existe um cadastro nacional não só dos softwares que são adquiridos ou desenvolvidos. A Alemanha desenvolveu o seu próprio software; não comprou, por exemplo, das empresas israelenses, que são as maiores produtoras desses programas. E também esse cadastro nacional é dos operadores, das equipes, dos órgãos estatais, até para uma futura responsabilização do mau uso, do abuso, do arbítrio na utilização do programa de software.

E também a gente discutiu aqui, e eu não tive tempo de esclarecer, por isso que eu agradeço pela pergunta, existem mecanismos tecnológicos, por exemplo, para excluir de antemão terceiros que não podem ser

afetados, como advogados, jornalistas, foi decidido pelo Tribunal Europeu dos Direitos Humanos, no caso do Big Brother Watch *vs*. United Kingdom.

Também temos discussões no pós, relatórios periódicos para o Ministério Público ou para o juiz, relatórios periódicos dos dados que foram capturados, até para analisar se os dados capturados são dados sensíveis que possam revelar alguma preferência religiosa, política, sindical, naquele núcleo essencial do direito privado das pessoas, naquela teoria alemã, europeia, dos três círculos concêntricos.

E depois, como é que vamos destruir essas provas? Então, por exemplo, na Espanha, é depois da sentença condenatória transitada em julgada - na verdade, sentença transitada em julgada, porque pode ser absolutória também - , enquanto, na Alemanha, são 5 anos depois do trânsito e julgado - até porque, na Alemanha e na Áustria, existe uma possibilidade excepcional de uma revisão criminal em favor da sociedade.

Eu não sei se eu consegui esclarecer os pontos, mas, em qualquer dúvida, estou à disposição novamente.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Sauvei.

Doutor Lucas, teria alguma pergunta?

O SENHOR LUCAS SALES DA COSTA (JUIZ INSTRUTOR DO GABINETE DO MINISTRO CRISTIANO ZANIN) - Não, Excelência.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Então, eu passo agora às perguntas que foram apresentadas aqui pelas pessoas que estão nos acompanhando.

A Doutora Adriana Brito, doutoranda da Universidade Federal da Bahia, pergunta ao Doutor André Cyrino quais as providências que as empresas de telefonia tomaram ou podem tomar para ativamente proteger o usuário contra ferramentas de monitoramento remoto.

O SENHOR ANDRÉ CYRINO (CONEXIS BRASIL DIGITAL – SINDICATO NACIONAL DAS EMPRESAS DE TELEFONIA E DE SERVIÇO MÓVEL CELULAR E PESSOAL) - Está ligado. Muito obrigado, Ministro Zanin, muito obrigado à Doutora Adriana Brito pela provocação.

Bom, as operadoras e as empresas de telecomunicações, elas têm setores voltados à cybersegurança e se voltam, o tempo todo, a tentar bloquear quaisquer portas, janelas e falhas no sistema.

Então, essas medidas são tomadas todos os dias, eles se preocupam com isso. O que eu procurei ressaltar na minha fala é que é uma antítese para elas a percepção de que temos que buscar agora onde estão as falhas. Então essas, eu não saberia dizer os nomes técnicos do que é feito, mas existe um setor de

cybersegurança e existem pessoas dedicadas 24x7 em promover essas proteções e fechamento de portas.

Não sei se eu respondi, mas esse é um ponto que nós queremos aprofundar no memorial de *amicus curiae*, que será apresentado oportunamente nos autos.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor André Cyrino.

A próxima pergunta foi formulada pelo Doutor Mateus Parma e é para a Doutora Estela Aranha. Foi citada na apresentação a norma da Casa Branca sobre vedação do uso de *spywares* comerciais. A normativa é alvo de críticas, pois não abarca ferramentas intrusivas desenvolvidas pelo próprio Estado. Naquele país, existem controles *ex ante* para as atividades de inteligência? Vossa Senhoria acha que o modelo americano de autorização judicial prévia para o uso dessas ferramentas para fins de inteligência é adequado à realidade brasileira?

A SENHORA ESTELA ARANHA (CONSULTIVO DE ALTO NÍVEL DA ONU PARA INTELIGÊNCIA ARTIFICIAL) - Então, não, não acho, até porque a legislação é completamente diferente, inclusive eles têm legislações que vieram, enfim, pós o 11 de setembro, que você tem uma, enfim, o trabalho de intrusão deles, tem NSA, entre outras instituições, e as autorizações prévias, elas são genéricas, isso é uma grande discussão lá.

Então, obviamente, eles têm uma proteção em relação aos softwares comerciais, porque a exposição ao risco ao país, à segurança do país é enorme; e não só isso - não é? -, a gente falou muito da proteção dos jornalistas, da proteção dos parlamentares, dos advogados, mas do próprio todo sistema de segurança. Imagina, qualquer um entra no sistema e pode mexer em qualquer coisa.

Portanto, aqui, no Brasil, que a gente tem, infelizmente, por exemplo, o problema do combate ao crime organizado, esse entranhamento dele nas instituições públicas, inclusive de segurança pública. Imagina ter acesso, enfim, a esse tipo de dados. Isso é um problema.

E a nossa Constituição, inclusive, ela é mais restritiva que a Constituição alemã, por exemplo, no caso que autoriza a inteligência a ter acesso a esses dados telefônicos e telemáticos. O sistema de inteligência nosso não, o nosso exclusivamente coloca para a persecução penal, para a investigação criminal. Então, acho que não tem menor similaridade dos sistemas. Eu dei um exemplo de defesa em relação à soberania nacional, mas nós já temos parâmetros da Constituição e nós devemos usá-los para qualquer interpretação, futura legislação ou parâmetros para essa legislação e é a isso que a gente tem que se ater. Ela é bem mais restritiva e a proteção em relação a esses direitos, são bem jurídicos altamente protegidos pela nossa Constituição Federal.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado Doutora Estela Aranha. Agora, a pergunta foi formulada pelo Doutor Pedro Saliba, do Data Privacy Brasil, e é para o Doutor Sauvei Lai.

Por que a distinção entre *policeware* e *spywares* e quais seriam as características entre eles, além dos órgãos que utilizam? Considerando a necessidade de investigações menos intrusivas, quais os critérios utilizados para a adoção dessas ferramentas pelo Ministério Público e salvaguardas adotadas para a restrição de coleta às finalidades das operações?

O SENHOR SAUVEI LAI (ASSOCIAÇÃO NACIONAL DOS MEMBROS DO MINISTÉRIO PÚBLICO – CONAMP) - Boa tarde, obrigado pela pergunta. De novo, a questão é terminológica para a gente distinguir exatamente a finalidade e o objetivo. *Govware* é o gênero, é justamente um software governamental, estatal que, se usado para fins de inteligência, que tem um outro objetivo regido pelo princípio da prevenção, da precaução, para que os órgãos da comunidade de inteligência forneçam uma informação qualificada para a tomada de uma decisão soberana do mandatário, claro que isso não pode se confundir para fins de investigação, quando o princípio já não é mais de prevenção, mas sim o princípio da repressão. Quando o crime já foi cometido, nós temos o inquérito

policial instaurado, já há indícios mínimos de autoria, prova do crime, consequentemente são dois regramentos distintos.

E aqui inclusive aproveito: na Inglaterra, por exemplo, e nos Estados Unidos, para fins de coleta de inteligência, aí sim, *spyware* e não *policeware*, para fins de coleta de informação qualificada, a decisão não é necessariamente do Poder Judiciário. Nós temos inclusive, na Inglaterra, do ministro do interior; e, nos Estados Unidos, existe uma comissão, e o próprio expositor hoje de manhã, da Abin, explica, um juiz próprio para tomar esse tipo de decisão, desse controle de autorização. Nos Estados Unidos isso também acontece. É um comitê de juízes indicados pela Suprema Corte Norte-Americana.

Mas, de novo, isso para o *spyware*, para fins de inteligência de espionagem. Quando nós estamos combatendo um crime já cometido, tentando identificar a autoria desse crime, aí a decisão, o crivo do Poder Judiciário é pelo juiz competente local. Claro, salvo se houver algum foro por prerrogativa de função nos tribunais superiores.

Vou aproveitar o ensejo, Ministro, e só para explicar que, especificamente na Alemanha, Doutora Carolina, eu esqueci, na sua pergunta, de explicar, não existe nem exploração de *backdoors*, de vulnerabilidade. Tanto é que a

Professora Laura Mendes de Manhã explicou, lá eles chamam de cavalo de troia, o *Bundestrojaner*, que é o cavalo de troia federal.

E lá na Alemanha eles optaram por desenvolver um próprio programa, e esse programa na verdade, tanto a legislação alemã quanto na legislação espanhola preveem o dever de colaboração por parte de empresas provedoras, seja de conexão, seja de infraestrutura. E lá o mecanismo foi enviar ao suspeito falsos avisos de atualização do iOS, Android. Então na verdade você não está explorando, você está infectando aqueles golpes que os criminosos fazem com as vítimas. A gente está fazendo o contrário, a gente está aplicando o *fishing*, o engodo contra eles. Então, quando o alvo recebe uma atualização da Apple, por exemplo, ele vai e clica. Ele não só está atualizando o iOS, como está sendo infectado, sem explorar nenhuma vulnerabilidade no sistema.

Então, é uma alternativa, mas, de novo, vários países europeus têm o seu cadastro nacional de softwares que são usados para essa infecção e o cadastro nacional dos operadores, justamente para permitir a responsabilização de todos eles em caso de eventual abuso.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Salvei!

A próxima pergunta foi formulada pelo Doutor Hugo Lazar, que é presidente da Intelis e esteve conosco é hoje pela manhã. É para o Doutor André Cyrino. A pergunta é: recentemente, o portal Canaltech noticiou que, em 17 de abril de 2024, uma empresa operadora de telecomunicações anunciou a venda de um serviço de confirmação da localização de clientes com base no posicionamento do celular em relação às antenas da operadora. A venda seria voltada ao setor financeiro. Quais são os controles a que o setor de telecomunicações está sujeito para negociar esse tipo de dados?

O SENHOR ANDRÉ CYRINO (CONEXIS BRASIL DIGITAL – SINDICATO NACIONAL DAS EMPRESAS DE TELEFONIA E DE SERVIÇO MÓVEL CELULAR E PESSOAL) - Excelência, agradeço a pergunta do Doutor Hugo Lazar, a quem eu ouvi atentamente na parte da manhã.

Eu não conheço exatamente esse produto que está sendo comercializado, eu que represento várias empresas do setor, não conheço exatamente esse caso.

O que eu posso dizer é que informações de geolocalização já são fornecidas pelas operadoras quando solicitadas por decisão judicial. Então, isso, enfim, é o que eu posso dizer sobre o tema, mas eu vou procurar saber o que é isso e até endereçar a questão no âmbito do memorial posteriormente a ser juntado oportunamente. Muito obrigado!

Lamento não poder responder especificamente a essa notícia do dia 17 de abril de 2024.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutor André Cyrino.

Já foram apresentadas todas as questões. Eu agradeço imensamente aos expositores desta tarde pela colaboração, pela participação nesta audiência pública.

E agora faremos um intervalo, e os trabalhos serão retomados em 20 minutos.

Muito obrigado, até já!

INTERVALO

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Boa tarde a todos.

Vamos agora começar o terceiro bloco desta audiência pública, que tem por objetivo instruir esta ADPF com informações de todos os segmentos da sociedade, seja através de órgãos públicos, de representantes da sociedade civil, especialistas ou interessados que possuam experiência e autoridade no tema aqui discutido.

E o tema aqui discutido são os limites e possibilidades da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão

virtual remota e de ferramentas de monitoramento secreto e invasivo de comunicação pessoal.

Eu renovo meus cumprimentos à Doutora Elizeta Maria de Paiva Ramos, Subprocuradora-geral da República. Renovo meus cumprimentos ao Doutor Turbay, que aqui representa o Conselho Federal da Ordem dos Advogados do Brasil; também à Doutora Carolina Santos Lima, ao Doutor Lucas Sales. Cumprimento, aqui, os expositores que participarão deste terceiro bloco e também todos que aqui estão ou que nos acompanham pelo Youtube.

Neste terceiro bloco, nós começaremos com a exposição do Doutor André Ramiro, que fará sua exposição de forma virtual. O Doutor André Ramiro é atualmente *fellow* pesquisador do Digital Civil Society Lab da Universidade de Stanford e membro da rede latino-americana de estudos em vigilância, tecnologia e sociedade. Foi pesquisador visitante no Weizenbaum Institute e no Alexander von Humboldt Institute for Internet and Society, bem como foi coordenador do estudo *Mercadores da Insegurança, Conjuntura e Riscos do Hacking Governamental no Brasil*, pesquisa pioneira na produção de conhecimento teórico e empírico sobre contratos entre o poder público e comerciantes de ferramentas de intrusão digital no Brasil.

Então, eu passo a palavra ao Doutor André Ramiro.

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Olá, boa tarde a todos e todas! Meus cumprimentos a Vossa Excelência, Ministro-Relator, Cristiano Zanin, à Doutora Subprocuradora-Geral da República Elizeta de Paiva Ramos e às demais autoridades públicas, expositores e expositoras aqui presentes.

É uma imensa honra poder expor nossos entendimentos aqui enquanto membros da sociedade civil, acadêmicos do Direito e demais setores da sociedade de interesse nesse tema. Por isso, saúdo a iniciativa de realização de audiência pública por parte desta Corte, iniciativa que efetivamente deve ser elogiada enquanto processo de qualificação da formação do juízo por parte da Corte e que democratiza a interpretação da Constituição, do arranjo legal brasileiro, pelos demais setores da sociedade.

Deixo o meu reconhecimento e saudações à iniciativa.

Minha exposição vai ser, em grande medida, ancorada em resultados de pesquisas feitas junto ao Instituto de Pesquisa em Direito de Tecnologia do Recife - IP.rec, ao Digital Civil Society Lab, da Universidade de Stanford, ao Weizenbaum Institute for the Networked Society e ao Alexander Von Humboldt Institute for Internet and Society, em que venho buscando uma abordagem de direito comparado junto aos modelos jurídicos de países na Europa e na América Latina, investigando precisamente as abordagens legais e os modelos

de prestação de contas para expedientes do que a gente vem chamando durante essa audiência de *hacking* governamental.

Fico muito feliz em ouvir que o estudo do qual tive a oportunidade de participar, *Mercadores da Insegurança*, publicado em 2022, é referenciado aqui nesta audiência. Isso me dá margem para abordar novas frentes desse debate, uma vez que esse estudo já foi suficientemente coberto.

Minha contribuição vai buscar um balanço dos resultados de investigações que venho fazendo junto a essas instituições. Para isso, vou lançar mão de resultados de ações judiciais já sedimentadas, como a Corte Constitucional alemã, já repetidamente citada hoje, e de outras ações que ainda estão em pleno desenvolvimento em outros tribunais de justiça, como, por exemplo, nos Estados Unidos.

Para iniciar, Ministro Zanin, em vez de fazer uso das expressões *hacking*, *hacking* governamental ou intrusão remota, ainda que plenamente cabíveis na minha opinião, vou-me referir à exploração de vulnerabilidades. Essa expressão já foi ressaltada por outras expositoras, o que, na minha opinião, torna o debate ainda mais flexível neste momento de estabelecimento ainda de uma gramática jurídica e de uma tipologia tecnológica mais apropriada para a regulação por vir. Isso nos dá, na minha opinião, uma dimensão ainda mais ampliada da prática e permite análises tanto de ordem econômica desse mercado de vulnerabilidades

quanto de impacto aos direitos fundamentais, seja em sua dimensão coletiva ou individual, seja de ordem procedimental - para me referir aqui a áreas comumente utilizadas nessas ferramentas -, sejam investigações criminais para produção de provas ou para fins de atividades de inteligência.

Estabeleci inicialmente duas diretrizes que a gente pode considerar como importantes bússolas legítimas para avaliar o tema desta audiência. Primeira: se a gente assumir que técnicas de investigação não típicas - aquelas que não estão inicialmente previstas no rol de técnicas investigativas no arranjo processual penal -, seriam inicialmente passíveis de aplicação analógica para parte da doutrina processualista penal no Brasil e para algumas autoridades públicas, isso faria necessária a criação de um procedimento especial suficientemente estabelecido em ordem judicial que justifique tal medida. Por outro lado, a intrusão por parte de uma autoridade pública em dispositivos, plataformas ou redes de fato extrapola exponencialmente a avaliação de impacto a direitos fundamentais e demanda novas metodologias de testes de proporcionalidade se comparados a técnicas tradicionais como, por exemplo, busca e apreensão, interceptação de telecomunicações, disputas ambientais ou infiltrações, sejam elas físicas ou digitais.

A busca e apreensão em domicílio, por exemplo, está longe de se comparar, do ponto de vista de suspensão de direitos, com uma devassa a dados

pessoais de conteúdo de comunicações acessados por meio de um dispositivo celular pessoal, muitíssimo mais revelador da vida privada do indivíduo, seja em sua esfera íntima, seja em suas esferas política, social e econômica. Inclusive revela dados pessoais e associações de natureza bastante sensíveis.

Entendo que estamos diante de uma fronteira de vigilância cuja regulação, caso encontre uma balança de proporcionalidade e necessidade, vai acarretar inevitavelmente na suspensão de uma série de direitos fundamentais diretamente ligados à segurança e integridade dos sistemas informáticos cujas vulnerabilidades estão sendo exploradas. Para embasar esse raciocínio, apoio-me em duas decisões da Corte Constitucional alemã, que vem pautando e atualizando os procedimentos necessários a esse tipo de expedientes e atualizando também a proteção a garantias constitucionais. Muito rapidamente, para oferecer esse balanço e repisar o referencial que já foi feito por outros expositores hoje, em 2008, a Corte, em sede de Reclamação Constitucional nº 307, que pautava precisamente a legalidade de técnicas de intrusão remota, reconheceu o direito fundamental à proteção da integridade e confidencialidade dos sistemas informáticos enquanto extensão contemporânea do direito fundamental à dignidade da pessoa humana e da livre formação da personalidade - peça-chave no desenvolvimento da doutrina de proteção de dados pessoais, seja nacionalmente, seja globalmente.

Entendo que a decisão buscou um contrabalanço necessário para sopesar a necessidade e a proporcionalidade de medidas de intrusão dessa natureza. Se novos desafios se impõem às investigações criminais devido ao avanço tecnológico, com o uso popular de criptografia, por exemplo, e medidas mais intrusivas supostamente seriam necessárias, a gente precisa também atualizar o arranjo de proteção a direitos constitucionais potencialmente afetados dos indivíduos. Seria possível dizer que é um movimento regulatório análogo, na minha opinião, à recente elevação do direito à proteção de dados pessoais ao patamar de direito fundamental na Constituição brasileira, não enquanto um regime que protege em absoluto um direito fundamental, mas como um contraponto forte que qualifica os testes de proporcionalidade e, por fim, vai resultar em um juízo mais qualificado pela autoridade judicial.

Em segundo lugar, em sede de Reclamação Constitucional nº 2.835, de 2017, a Corte Constitucional alemã reconhece a necessidade de atualização dos procedimentos na lei que regula o trabalho das autoridades de inteligência daquele país. Essa lei foi atualizada, porque a Corte julgou necessária uma reforma tanto legal quanto institucional, tendo inclusive como objeto central garantir a liberdade do trabalho jornalístico, como afirmou a Doutora Samara Castro, da Secom. Ademais, Ministro Zanin, essa decisão resultou na criação do *Independent Oversight Council* ou do Conselho Independente de Fiscalização, em uma tradução

livre, que, em conjunto com a comissão do G10, do Parlamento Alemão, com o painel parlamentar de fiscalização e o comissariado para a apropriação de dados pessoais e para a liberdade de informação no país criam um ecossistema de fiscalização robusto, que pode ser absorvido pelo nosso debate. Ressoando exposições já feitas aqui, sugerem a atualização do regime de proteção de dados pessoais no Brasil para também alcançar as atividades de inteligência e investigação.

Para concluir, friso que, no bojo da regulação sobre o uso de ferramentas de exploração de vulnerabilidades, é fundamentalmente importante discutir o ecossistema de fiscalização desses expedientes. Deve ser esse arranjo de fiscalização especializado e suficientemente democrático, e esse é um tema central nos estudos de inteligência tradicionalmente.

Em último lugar, para concluir a minha intervenção, em sede de ação ajuizada pelo WhatsApp, no Tribunal do Distrito Norte da Califórnia, contra o NSO Group, desenvolvedor do Spyware Pegasus, já mencionado nesta audiência repetidas vezes, vem sendo construída a tese jurídica que vem sendo chamada de *Network Trespass Theory of Liability*, ou seja, um regime de responsabilidade derivado da invasão de propriedade em uma rede ou sistema por meio da exploração de uma vulnerabilidade em redes conectadas, sejam elas públicas ou privadas. Ainda que essa ação ainda esteja em trâmite, o Tribunal de Justiça da

Califórnia já ordenou a cessão do código-fonte do Pegasus ao WhatsApp por entender que estamos diante de um caso de invasão de propriedade.

Isso para dizer que, na minha opinião, Ministro Zanin, o art. 154-A do Código Penal, que versa sobre a invasão de dispositivos informáticos, é um instituto que deve ser levado em consideração para que a gente entenda se, em processos administrativos de contratação dessas ferramentas, não está em jogo a legalidade do próprio objeto de contratação. Quer dizer, se não estamos diante de uma violação clara aos princípios basilares da Administração Pública estabelecidos no art. 37 da Constituição Federal. Entendo ser também um referencial jurídico, que pode repercutir nesse nosso mapeamento de fatos políticos, de arranjos regulatórios e de arquiteturas institucionais no Brasil, inclusive em sede de prestação de contas, da qual vai participar os Tribunais de Contas, eventualmente também a Autoridade Nacional de Proteção dos Dados Pessoais e o CNJ.

Fico por aqui, já extrapolando o limite do meu tempo. Agradeço imensamente o espaço para a contribuição e fico à disposição para maiores esclarecimentos.

Obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor André Ramiro!

Agora vamos ouvir a Doutora Carina Quito, mestre em Processo Penal pela Universidade de São Paulo e advogada nas áreas de Direito Penal e Tecnologia.

Doutora Carina Quito, tenha a palavra, por gentileza.

A SENHORA CARINA QUITO (INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS - IBCCRIM) - Muito obrigada!

Boa tarde a todas e a todos!

Cumprimento o excelentíssimo Ministro Cristiano Zanin, a excelentíssima Subprocuradora-geral da República, estendendo as minhas saudações aos demais integrantes da Mesa, aos colegas expositores e às demais pessoas que nos assistem.

Gostaria de iniciar agradecendo aqui a oportunidade que foi concedida ao IBCCrim de participar desta audiência pública, parabenizando o Supremo Tribunal Federal pela iniciativa de promover uma discussão plural sobre um tema que é tão relevante quanto é complexo.

Falo aqui hoje em nome do Instituto Brasileiro de Ciências Criminais, uma entidade que, há mais de 30 anos, atua na promoção das ciências criminais e na defesa dos direitos humanos. Nos últimos anos, o IBCCrim vem se dedicando a estudar e a debater os impactos de novas tecnologias no Direito Penal, no Processo Penal e na segurança pública, sempre com a preocupação de conter os

agravos a direitos fundamentais que advêm de novas formas de vigilância e de controle sobre as pessoas na sociedade da informação.

Sob essa perspectiva, eu inicio esta exposição apontando que o IBCCrim tem a preocupação de que direitos fundamentais, cuja eficácia direta e imediata é reconhecida pelo Texto Constitucional sejam paradoxalmente limitados como resultado de uma ação que foi ajuizada sob a justificativa de proteger esses mesmos direitos.

A análise do tema aqui tratado, a nosso ver, deve partir da compreensão de que o princípio da legalidade opera como um fator de contenção do Estado e de que as intervenções em direitos fundamentais dependem necessariamente de leis que as autorizem.

Como nós já ouvimos aqui de tantos expositores hoje, as intervenções em direitos fundamentais causadas pelo uso de ferramentas de invasão e monitoramento remoto são muito mais intensas do que aquelas causadas pelos meios de obtenção de prova já previstos no nosso ordenamento jurídico.

E isso, especialmente, porque mais do que o acesso a dados, tanto dados em fluxo quanto armazenados, os chamados *spywares* permitem que o Estado interfira nos próprios equipamentos invadidos, o que compromete, como já ouvimos, a confiabilidade e a integridade desses sistemas, trazendo repercussões importantes também para a persecução penal.

Na ausência de lei autorizativa específica para intervenções dessa magnitude, o ordenamento jurídico brasileiro impõe ao Estado hoje uma proibição para o uso dessas ferramentas.

A pretensão veiculada nessa ADPF, que decorre da constatação de que agentes públicos vêm fazendo um uso que é ilegal de ferramentas de *hacking*, é de que o Congresso Nacional ou de que o Poder Judiciário, em caráter provisório, regule a utilização das tecnologias de infiltração e monitoramento, o que implica, obviamente, restringir direitos fundamentais.

A nosso ver, na constância de um dever de abstenção do Estado não existe lesão a preceito fundamental, sendo necessário que as instituições atuem para coibir o uso ilegal e abusivo das tecnologias tratadas na ADPF, se o que se tem por objetivo é protegê-los contra violações.

Muito bem. Para além desse primeiro ponto, relativo à conformação constitucional do tema, o IBCCrim aponta ainda um segundo que está relacionado à separação de poderes. Caso esse egrégio Supremo Tribunal Federal acolha o pedido para fixar balizas, autorizando ainda que provisoriamente a utilização das ferramentas aqui tratadas, o Poder Judiciário invadirá um espaço de atuação exclusiva do Legislativo.

Como dissemos de início, o IBCCrim entende que é muito louvável e oportuna a iniciativa desta Suprema Corte de ouvir os diversos pontos

de vista sobre o uso de softwares espiões pelo Estado. Ainda assim, reputa que é o Congresso Nacional, por sua representatividade popular, o espaço institucional adequado para que amadureça o tão necessário debate democrático que esse tema suscita.

Ainda pelos enormes riscos envolvidos na regulação da matéria, que já foram vistos aqui hoje, o IBCCrim pondera que o momento não é de pressa, mas um momento de extrema cautela, e cautela para que o Congresso Nacional possa amadurecer e dimensionar corretamente os impactos que ferramentas desse tipo podem ter em direitos fundamentais.

Esse dimensionamento, Excelência, é imprescindível para que o parlamento possa definir a natureza, os limites e as condições das intervenções em direitos fundamentais que serão eventualmente admitidas, de forma a editar uma regulação que seja robusta e proporcional, logo altamente restritiva.

Nesse mesmo sentido, o IBCCrim entende que o Poder Legislativo não deve avançar na regulação do uso de *malware* enquanto não editar uma disciplina específica para as provas digitais no processo penal e para o tratamento de dados pessoais na persecução criminal e na segurança pública.

Entendemos que, sem que se estabeleça previamente o ambiente normativo que seja adequado para o uso dessas ferramentas, será verdadeiramente

impossível aprovar um regime para a utilização do *hacking* governamental, com salvaguardas que sejam efetivas.

Agora, passo a palavra ao meu colega Hélder para dar prosseguimento.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutora Carina Quito, que falou pelo IBCCrim.

Então, agora, falará o Doutor Carlos Mendes também pelo IBCCrim. Doutor Carlos Mendes é doutor e mestre em Ciências Criminais pela PUC do Rio Grande do Sul e membro do Departamento de Novas Tecnologias de Direito Penal do IBCCrim.

Com a palavra o Doutor Carlos Mendes.

O SENHOR CARLOS HÉLDER C. FURTADO MENDES (INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS - IBCCRIM) - Boa tarde a todos e todas! Renovo os cumprimentos do Instituto Brasileiro de Ciências Criminais ao eminente Ministro Cristiano Zanin e a todos os demais presentes.

Antes de pensar na possibilidade da utilização do software espião pelo Estado, é preciso entender que os dados são fragmentos da personalidade do sujeito, de modo que, lembrando o que o Professor Stefano Rodotá afirma, o dado é um corpo desentranhado do próprio corpo. Assim, não são apenas os direitos à intimidade, à privacidade e à livre comunicação afetados

por esse método de investigação. Trata-se de direito fundamental à confiabilidade e integridade dos sistemas informáticos e, portanto, não é possível o uso de legislação análoga para justificar a aplicação de instrumentos de investigação como um *malware* pelo Estado.

A confiabilidade, como dito aqui por diversos expositores, é um direito fundamental firmado pelo Tribunal Constitucional alemão e, como afirmado na tese defendida pelo Professor José Guimarães Mendes Neto, é um direito materialmente fundamental. Pela cláusula de abertura prevista na Constituição Federal, portanto, torna-se admissível a incorporação desse direito fundamental no ordenamento jurídico brasileiro.

A experiência alemã pode servir de base para os debates tratados aqui nesta Suprema Corte. A principal delas - e os principais requisitos - é justamente a necessidade de uma legislação própria, com a devida clareza e precisão normativa, além de um controle jurisdicional a partir da proporcionalidade. Nos casos e hipóteses essenciais tratados por aquele tribunal, foi dito haver a necessidade de existência de evidências suficientes de que outros significativos valores fundamentais precisam ser protegidos, tais quais a vida, a integridade de outros cidadãos, os fundamentos do Estado e os valores da humanidade.

Ante isso posto, é lícito afirmar que a autorização acelerada do uso de *malware* espião por parte do Estado brasileiro, em sede de ADPF, impossibilita reflexões necessárias, razão pela qual, como salientado pela Doutora Carina Quito, deve-se oportunizar ao Congresso Nacional avançar nessas reflexões legislativas antes de qualquer autorização, ainda mais em balizas provisórias. É preciso ter em mente que os dispositivos informáticos que conhecemos são marcados pela obsolescência. Uma autorização precária de invasão desses dispositivos vai implantar balizas que digam ter sido permitida a invasão de diversos outros dispositivos informáticos mais modernos, capazes de alcançar o que se pensa, o que se fala, o que se ouve, e isso é muito grave.

É o Legislativo, portanto, que deve impor qual é o rol taxativo de crimes e, mais ainda, estabelecer limites claros para que o uso desses métodos não massifique a pescaria probatória já vedada por esta Suprema Corte, impondo um protocolo de busca mínimo, capaz de determinar ao agente investigador o dever de informar ao magistrado não apenas qual será o dispositivo alvo, mas também a funcionalidade desse dispositivo a ser ativado, bem como quais os indícios e fontes de prova que se pretendem alcançar, um relatório de atividades a ser informado pelo magistrado e, claro, limites mais concretos de temporalidade.

Por fim, já finalizando a minha fala, em matéria de processo penal, seria impossível realizar a auditabilidade das informações alcançadas sem o conhecimento acerca do código-fonte. Mais ainda, sem esse conhecimento do código-fonte, é possível perceber que os próprios órgãos brasileiros que utilizam métodos ocultos de investigação podem ser alvos de espionagem. Se existe um debate entre conflito de interesse privado e conflito de interesse público, o conhecimento desse código-fonte é fundamental para o interesse público.

Nesses termos e na esteira da melhor interpretação constitucional, sustenta o IBCCRIM a necessidade de legislação específica sobre a matéria, cuja competência é do Congresso Nacional, antes ainda que seja avançado o debate fundamental da legislação própria de proteção de dados em matéria penal, que ainda está pendente.

Muito obrigado mais uma vez!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Carlos Mendes, que também falou em nome do IBCCRIM.

Agora falará, pelo Centro de Pesquisas e Extensão em Ciências Criminais da Faculdade de Direito da Universidade de São Paulo, o Doutor Giovanni Diniz.

O Doutor Giovanni Diniz é doutorando em Direito pela USP, mestre em Direito pela Universidade Federal do Paraná, especialista em Direito Penal e Criminologia e membro do Centro de Pesquisas e Extensão em Ciências Criminais da Faculdade de Direito da Universidade de São Paulo.

Também falará, pelo mesmo Centro de Pesquisas da Faculdade da Universidade de São Paulo, a Doutora Larah Brahim, advogada criminalista e mestranda em criminologia pela Universidade de São Paulo.

Com a palavra, inicialmente, a Doutora Larah Brahim.

A SENHORA LARAH BRAHIM (UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO-FD-USP; - CENTRO DE PESQUISA E EXTENSÃO EM CIÊNCIAS CRIMINAIS-CPECC) - Uma boa tarde a todos. Cumprimento inicialmente o excelentíssimo Ministro-Relator Cristiano Zanin, a Subprocuradora-Geral da República, o representante do Conselho Federal da OAB, Doutor Marcelo Turbay, os juízes instrutores, os colegas especialistas e a sociedade civil aqui presente.

O Centro de Pesquisa e Extensão em Ciências Criminais da Faculdade de Direito da Universidade de São Paulo, sob a orientação do Professor Doutor Maurício Dieter, agradece a oportunidade de contribuir como especialista nesta audiência pública e parabeniza a iniciativa do eminente Relator em convocar esta audiência, possibilitando o debate público e o engajamento da sociedade civil

em um tema delicado e preocupante do ponto de vista das garantias constitucionais e processuais penais, que é o uso de softwares espiões para fins de investigação criminal.

A presente ADPF, antiga ADO 84, busca dar contornos de legalidade do uso desses softwares pelo Estado. Nessa busca, a PGR sugere, na inicial, alguns procedimentos que poderiam ser adotados, ainda que provisoriamente, enquanto o Congresso Nacional não legisla sobre a matéria.

No entanto, nosso posicionamento é diverso e assenta-se na impossibilidade de que esta Corte defina, ainda que temporariamente, critérios para essa prática.

Defendemos, de outro modo, que a decisão do Supremo se limite a reconhecer o uso de softwares espiões, de forma que, com esse reconhecimento de ilegalidade, os órgãos persecutórios cessem tais práticas.

Acreditamos que a solução oferecida na inicial, no sentido de que o Supremo fixe parâmetros provisórios, é inconstitucional, uma vez que esta Corte avocar para si função estabelecida pelo Constituinte de 88 como exclusiva do Poder Legislativo é tentar remediar uma inconstitucionalidade produzindo outra.

Em tempos de desmonte do Estado Democrático de Direito, dos graves ataques sofridos pela recente democracia brasileira e do legado autoritário, deixado pela ditadura militar, é obrigação desta Suprema Corte reafirmar o

compromisso democrático de defesa da Constituição. E o caminho, ele é único, não havendo possibilidade de tergiversar.

O respeito à divisão de poderes instituída pelo Constituinte, cabendo a esta Corte realizar, em momento adequado e se for necessário, o controle de constitucionalidade da temática.

Ademais, importante deixar claro que o pedido de regulamentação, por parte da PGR, é uma tentativa de dar uma roupagem legal para ações estatais que são claramente ilegais dentro do ordenamento jurídico brasileiro. Essa conclusão pode ser deduzida a partir de vários campos do Direito. E aqui, nos valemos de três deles em especial.

O primeiro, que eu vou tratar, do constitucional administrativo; o segundo, parte da dogmática processual penal; e o terceiro da dogmática penal material.

No que se refere ao argumento de Direito Administrativo Constitucional, sabe-se que os órgãos estatais somente podem agir em virtude de lei, porque se submetem ao princípio da legalidade estrita, ou seja, na ausência de lei que regulamente uma conduta, ainda que seja uma omissão inconstitucional, não pode a Administração Pública agir. Isso porque os órgãos estatais, polícias, Ministério Público, só podem fazer o que a lei autoriza, todo o resto está proibido. O que significa dizer que o uso de softwares espiões para fins de investigação

criminal, sem uma lei prévia que autorize e regulamente esse uso, é uma ilegalidade e uma afronta à Constituição brasileira.

Eu chamo, agora, o meu colega Doutor Giovanni para continuar e desenvolver os próximos dois argumentos.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutora Larah Brahim.

Agora, o Doutor Giovanni Diniz fará o uso da palavra.

O SENHOR GIOVANNI DINIZ (UNIVERSIDADE DE SÃO PAULO - FACULDADE DE DIREITO-FD-USP; CENTRO DE PESQUISA E EXTENSÃO EM CIÊNCIAS CRIMINAIS - CPECC) - Boa tarde, Ministro! Obrigado pela concessão da palavra.

Retomo os argumentos da Doutora Larah.

A segunda razão pela qual entendemos que esta Corte não pode criar critérios, ainda que provisórios, para o uso dos *malwares*, relaciona-se ao campo do Direito Processual Penal.

Do ponto de vista do processo, o uso de *malwares* deve ser expressamente vedado durante a omissão legislativa porque essa ferramenta é um meio de obtenção de prova atípico, que não está contemplado nem em lei específica, nem na Lei Geral de Proteção de Dados, nem no Marco Civil da Internet, nem na Lei de Interceptação de Dados e Interceptação Telefônica. A excepcionalidade da

matéria, diante da ausência de balizas específicas para discipliná-la, não pode permitir o seu uso pelas autoridades hoje. Os diplomas legais que citei, todos tratam de assuntos diferentes e que não são aplicáveis à realidade dos *malwares*, de sorte que as leis que agora existem não cabem nem por analogia a essa matéria.

Junto à questão da especificidade do tema e da atipicidade do meio de prova em si, deve-se lembrar que o manejo desses softwares espiões é muito mais invasivo aos direitos fundamentais do que os meios de provas típicos que conhecemos, por todas as razões aqui mencionadas no dia de hoje, em razão de toda a capacidade que esses softwares têm, como invasão a dados, senhas, todas as imagens e o que eles possibilitam fazer.

Assim sendo, sendo mais grave, não poderá a lei que versa sobre o meio de prova menos invasivo ser considerada suficiente ao meio de prova mais invasivo. Essa é uma questão lógica e, dessa forma, o *malware* deve ser regulamentado por lei própria, com maiores restrições e controles ao seu uso. Isso com pressupostos autorizados mais rigorosos do que aqueles critérios que já são previstos no dia de hoje para os meios de provas que são típicos. Caso contrário, o que acontecerá - já vem acontecendo, aliás - será a realização de um *bypass* processual. Hoje esse *bypass* se realiza porque, inexistindo qualquer regulamentação, o uso da tecnologia espiã se vai esquivar em pressupostos básicos que se valem para outras medidas, como é o caso da exigência da decisão judicial.

Mas esse *bypass* também se dará caso seja admitido o uso dessas ferramentas mediante outros requisitos autorizadores emprestados analogicamente de outros meios de prova típicos, como se fosse uma colcha de retalhos. Um exemplo disso seria equiparar o *malware* a um incidente, por exemplo, de busca de apreensão, no que toca aos seus pressupostos autorizadores. Veja, são coisas distintas, mas não pode ser feito esse empréstimo em relação aos seus requisitos, porque afinal a invasão do dispositivo pessoal, no que toca a esses requisitos, não será igual a uma busca e apreensão. Aliás, é muito o contrário. Na realidade, o que se tem é apreensão e depois uma busca, porque primeiro você apreende esse material informático, telemático, e depois, somente depois, você realiza uma busca pelo que se deseja encontrar. Dessa forma, corre-se o risco de que essa enorme intervenção aos direitos fundamentais se aproveite de critérios mais frágeis para se atingir resultados mais graves. Por essa razão, é necessário que o legislador tipifique esse meio de prova e estabeleça outros critérios mais robustos em atenção à nova realidade.

Por fim, em terceiro lugar, o uso do *malware* por agentes de persecução penal deve ser vedado porque, analisando objetivamente a conduta da invasão de dispositivos, seja ela por particulares, seja ela pelo Estado, isolando ela descritivamente quanto a uma ação, entendendo também a violação do direito à privacidade como um bem jurídico relevante ao Direito Penal - e tutelado pelo

Direito Penal -, percebemos que essa ação se torna, portanto, típica e, com a pendência dessas regulamentações que devem ser feitas por lei específica, é também antijurídica. Configura, então, o injusto penal, que, aliado à culpabilidade, torna-se um fato, portanto, que, na verdade, é um crime. Ou seja, a rigor, as ações estatais de invadir dispositivos móveis de terceiros por intermédio de softwares espiões, *malwares* ou qualquer que seja a denominação, consubstanciam atualmente um ato penal relevante e ilícito, uma vez que essa ação, espantosamente, e é esse o grande tema, não está hoje abarcada por uma causa excludente de ilicitude. Em outras palavras, não existe uma permissividade a essa conduta que viesse a tornar essa ação então vista primeiro descontextualizada como de um crime para um mero exercício regular de exercício da atividade persecutória do agente em sua profissão. Aqui não é possível argumentar, não é possível se falar em estado de necessidade na atividade de inteligência, tampouco no uso de legítima defesa como argumento retórico que pudesse excluir essa ilicitude. Também não se trata do cumprimento de um dever legal, uma vez que não está posto na lei esse dever ou o exercício regular de um direito que não está regulamentado em termos do próprio uso desses softwares. Sem essa regulamentação e sem a fixação dos limites da atuação dos órgãos públicos, o que se tem para o Direito Penal hoje é somente a violação do bem jurídico da privacidade e da sua tutela.

Por esses motivos, em divergência propositiva, portanto, em redação à inicial colocada pela PGR, concluímos pela impossibilidade da definição desta Corte de critérios para utilização desses *malwares*, ainda que provisórios.

Por enquanto, é isso, neste momento, mas nada impediria um exame propriamente meritório com relação ao controle de constitucionalidade em nível concentrado em uma ação própria.

Entendemos ser o caso, portanto, de a decisão do Supremo, ao reconhecer a ilegalidade do uso dos softwares espiões, dever apenas - apenas já é bastante coisa - determinar que os órgãos persecutórios cessem a prática de uso desses softwares enquanto não houver regulamentação própria pelo Congresso Nacional.

Agradeço a atenção de Vossas Excelências, e colocamos ao debate.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Giovanni Diniz pela exposição.

Agora, falarão, pelo Centro de Ensino e Pesquisa e Inovação da FGV, a Doutora Heloísa Estellita e o Doutor Alexandre Pacheco da Silva.

Doutor Alexandre Pacheco da Silva, que fará o uso da palavra em primeiro lugar, é professor da FGV Direito São Paulo e Coordenador do FGV Cepi; doutor em Política Científica e Tecnológica pela Universidade Estadual de

Campinas - UNICAMP; mestre e bacharel em Direito pela FGV Direito São Paulo; professor dos cursos de graduação e pós-graduação da FGV Direito São Paulo e coordenador do Centro de Ensino e Pesquisa em Inovação da FGV.

Com a palavra o Doutor Alexandre Pacheco da Silva.

O SENHOR ALEXANDRE PACHECO (FGV – DIREITO SP – CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO) - Boa tarde a todas e a todos.

Começamos aqui - estou dividindo a palavra com a Professora Heloísa Estellita - cumprimentando o Supremo Tribunal Federal, na pessoa do excelentíssimo Ministro-Relator, Ministro Cristiano Zanin, pela iniciativa em organizar esta audiência pública, dando oportunidade para apresentação de diversas perspectivas sobre um tema tão complexo como o tratado na ADPF, que nós discutimos hoje.

Aproveitamos a oportunidade também para cumprimentar todas as autoridades aqui presentes e os nossos diversos colegas, que brilhantemente nos antecederam, e reforçar ser um privilégio ocupar esse espaço. É um privilégio pelo aprendizado que o dia nos proporcionou, mas também em razão da complexidade desse tema.

Eu coordeno o Centro de Ensino e Pesquisa em Inovação, um braço da escola de Direito de São Paulo da Fundação Getúlio Vargas e que cuida de projetos envolvendo impactos de novas tecnologias no Direito. O desafio desse

centro de pesquisa é justamente se estruturar a partir de multidisciplinaridade, envolvendo profissionais de diversas áreas. Esse tema, talvez, seja a expressão da necessidade de multidisciplinaridade, não só para se ouvir profissionais de outras áreas, mas também para se traduzir termos cada vez mais complexos na dinâmica de tecnologias na contemporaneidade.

Aqui, eu começo a minha fala, e obviamente será complementada pela fala da Professora Heloísa Estellita, reconhecendo ser comum e justificado, em parte da nossa tradição jurídica, que, em certas situações, a garantia constitucional da privacidade e proteção de dados pessoais seja objeto de intervenções estatais, particularmente no contexto de investigações criminais. Isso é um detalhe interessante e não é deixado de lado por nós na nossa fala, mas o importante é que essas intervenções são sempre parciais e são sempre acompanhadas de uma série de procedimentos - que foram amplamente mencionados aqui por aqueles que me antecederam - e parâmetros que visam justamente preservar o núcleo essencial desses direitos tão importantes para a nossa sociedade.

Não há, portanto, no contexto jurídico brasileiro, uma isenção total, ou, alguns diriam, uma imunidade da aplicação da proteção de dados pessoais na realização de atividades de segurança pública, por mais que tenhamos uma previsão específica dentro da Lei Geral de Proteção de Dados Pessoais que

estabelece, ali, alguns condicionantes relacionados ao que não será aplicado no âmbito da proteção de dados pessoais pela autoridade de segurança pública e nacional.

O direito fundamental à proteção de dados pessoais, presente no art. 5º, LXXIX, exige que o uso de dados pessoais seja realizado com escopo claro e definido. Independentemente da exclusão estabelecida pela Lei Geral de Proteção de Dados Pessoais, essa ideia de clareza, de especificidade que acompanha a proteção de dados pessoais tem que ser garantida aqui. Principalmente nas situações em que não há participação efetiva do titular de dados pessoais, situações em que não há o seu consentimento, em especial, é a regra na matéria penal.

Essa é uma proteção oferecida pela Constituição ao cidadão e é um pré-requisito importante para que seja exercida qualquer tipo intervenção nesse direito fundamental. Qualquer forma de tratamento dos seus dados, em matéria penal, tem que ser precedida de lei. E, para nós, esse é o caso aqui.

É a exigência de escopo definido para o uso de dados pessoais que protege o cidadão contra os usos nefastos de sua informação e também do ponto de vista também de como o procedimento pode ser encaminhado de maneira adequada e correta. Quando estamos diante de uma situação em que não se exige do cidadão o seu consentimento para o tratamento de seus dados pessoais, é necessária a previsão de uma figura que é típica da área de proteção de dados

pessoais, que é a figura da base legal, que justifica e valida o tratamento de dados pessoais, mesmo que nós tenhamos bases legais diferentes do consentimento na esfera penal.

Em uma situação em que os dados são utilizados sem o consentimento do cidadão, sem a participação efetiva do cidadão, tem se dado ali em diferentes países, em primeiro lugar, um espaço para parlamentares versarem sobre o tema, o que foi amplamente discutido aqui anteriormente, como também a previsão de requisitos, inclusive uma discussão interessante se nós aqui no Brasil vamos exigir ou não autorização judicial prévia para concessão desse tipo de tratamento, ao que, particularmente, nós somos favoráveis.

E é precisamente nesse ponto que o uso de ferramentas de monitoramento, ou uso de ferramentas de espionagem, ou até mesmo o uso de ferramentas que criam essa camada de exploração de vulnerabilidades, o uso delas viola diretamente a garantia constitucional de proteção de dados pessoais.

Nesse sentido, um dos aspectos bastante importantes para que a gente possa entender é em termos do risco de gravidade de abuso e também entender a extensão com que essas tecnologias se apresentam a todos nós.

Em primeiro lugar, do ponto de vista de quem pode ser afetado direta ou indiretamente - pensando em candidatos, magistrados, advogados -, até

aqueles que vão fazer parte de um monitoramento indireto - por exemplo, todos aqueles que cercam esse alvo. E nesse sentido, um dos aspectos interessantes, que é pouco trabalhado, é a ideia de que boa parte das empresas apresentadas aqui anteriormente são empresas que fornecem os seus serviços, mas os fornecem a partir de uma perspectiva externa, estrangeira. Eu não vi ou pelo menos eu não conheço nenhuma empresa nacional que tenha oferecido esses serviços.

Nesse sentido, para terminar esse meu argumento, existe um componente de soberania fundamental para pensarmos esse debate. E não achamos que nós devamos criar atalhos sem o profundo amadurecimento institucional necessário para tratar do tema, para lidar com essa questão, olhando tanto o fato de que não localizamos essas empresas quando pensamos a transparência dos aspectos que compõem esse tipo de serviço como também o fato de termos questões relacionadas a como essas ferramentas vão poder ser utilizadas.

Mas paro aqui e agradeço mais uma vez a oportunidade de ocupar esse espaço. Obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutor Alexandre Pacheco da Silva, e passo a palavra à Doutora Heloísa Estelitta, que é professora da Escola de Direito da Fundação Getúlio Vargas e

coordenadora do Núcleo de Pesquisa em Direito Penal e Processual Penal na mesma instituição.

Com a palavra a Doutora Heloísa Estelitta.

A SENHORA HELOISA ESTELITTA (FGV - DIREITO SP - CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO) - Muito obrigada, Excelência. Ecoarei os cumprimentos feitos pelo Alexandre Pacheco, já que estou com o tempo espremido, e os argumentos que foram apresentados hoje pelos nossos colegas aqui com muito brilhantismo. Foi realmente uma iniciativa excelente esta audiência. Amanhã continuamos com ela.

Um dos efeitos da consagração de um direito fundamental é um dever de abstenção. E como lembrou o Vinícius Vasconcelos, esta Corte, esta Turma, pelas palavras do saudoso Ministro Sepúlveda Pertence, reconheceu que a criação de um direito fundamental implica um dever de abstenção justamente no caso das interceptações telefônicas. E eu relembro o HC 75.745, do Ministro Sepúlveda Pertence, votado nesta Turma.

Esse dever de abstenção se impõe ainda com maior força na matéria examinada nesta ADPF, porque trata-se, como nós vimos no decorrer do dia, de uma das intervenções mais graves, extensas e ubíquas que pode existir em matéria de proteção de dados. E ainda que assim não fosse, é indiscutível que, a

partir de 2022, com o acréscimo expresso desse direito na Constituição Federal, há um dever de abstenção nessa matéria que somente pode ser superado por meio de apoio em lei parlamentar proporcional.

É por isso que não se sustenta o argumento às vezes utilizado, Excelência, de que a LGPD, ao excluir da sua incidência justamente a proteção de dados para fins penais, teria com isso criado uma área livre de liberdade de atuação para as autoridades públicas. A exceção estabelecida pela LGPD não se baseava na inaplicabilidade da proteção de dados na matéria penal, mas sim na necessidade de um diploma legal específico, em virtude da maior gravidade dessa intervenção e das peculiaridades. Como, por exemplo, o diferimento do exercício dos direitos de acesso, a intermediação do exercício de muitos desses direitos por uma autoridade nacional de proteção de dados, os limites de eliminação e de confirmação do tratamento pelo titular.

Esses direitos não podem ser exercidos na seara penal como são exercidos na seara extrapenal. Não por outra razão, no ambiente europeu, a legislação para proteção de dados extrapenal foi separada da legislação, não só por essa razão, mas também por essa razão, da legislação de proteção de dados penal. No âmbito extrapenal, ela é tratada pelo Regulamento nº 2016/679; e a proteção de dados em matéria penal é objeto da Diretiva nº 680/2016.

Enquanto nós não tivemos uma LGPD Penal - e há um anteprojeto, inclusive secretariado pela Professora Laura Schertel, não há uma infraestrutura, uma vez que falamos tanto de infraestrutura hoje, não há uma infraestrutura legal para autorizar a utilização de *spywares*.

É por essas razões que nós do CEP recomendamos que seja vedado o uso dessa tecnologia para quaisquer fins, enquanto não for promulgada uma lei disciplinando a matéria de forma clara, expressa e proporcional.

No tempo. Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutora Heloisa Estelitta!

Agora, eu passo a palavra para a Doutora Charlene Nagae, que é do Instituto TornaVoz, Media Defence e Associação Brasileira de Jornalismo Investigativo, Abraji, que fará a sua exposição de forma virtual.

Com a palavra, a Doutora Charlene.

A SENHORA CHARLENE NAGAE (INSTITUTO TORNAVOZ, MEDIA DEFENCE E ASSOCIAÇÃO BRASILEIRA DE JORNALISMO INVESTIGATIVO – ABRAJI) - Boa tarde, Ministro! Eu agradeço e cumprimento os demais integrantes da mesa na sua pessoa. Também cumprimento os meus colegas que me antecederam. Fiquei com essa árdua tarefa de fazer a minha fala, a última

fala do dia. Depois de tantas exposições relevantes que ouvimos hoje sobre esse tema, eu vou buscar ser breve.

Eu falo hoje em nome do Instituto Tornavoz, onde eu ocupo a posição de diretora executiva, e falo também em nome da Associação Brasileira de Jornalismo Investigativa, Abraji, e da organização britânica Media Defence.

Essas três organizações têm um trabalho muito intenso, Excelência, voltado à defesa das liberdades de expressão e de imprensa, e atuou no Brasil em colaboração pela proteção e defesa de jornalistas brasileiros.

Eu tinha uma apresentação que eu não sei se já está sendo visualizada aí na sessão.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Estamos vendo sim, Doutora Charlene. Estamos vendo, ela está na tela.

A SENHORA CHARLENE NAGAE (INSTITUTO TORNAVOZ, MEDIA DEFENCE E ASSOCIAÇÃO BRASILEIRA DE JORNALISMO INVESTIGATIVO – ABRAJI) - Ah, perfeito! Agradeço, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado!

A SENHORA CHARLENE NAGAE (INSTITUTO TORNAVOZ, MEDIA DEFENCE E ASSOCIAÇÃO BRASILEIRA DE JORNALISMO INVESTIGATIVO – ABRAJI) - Eu vou também agradecer à fala da Doutora Samara

Castro, da Secretaria de Políticas Digitais da SECOM, feita hoje, na parte da manhã, e pela enfática defesa do jornalismo que ela fez, porque acho que boa parte das preocupações que ela trouxe são aquelas que afligem o Tornavoz, a Abraji e a Media Defence.

E as informações que a gente gostaria de ressaltar, nesta audiência pública, Excelência, estão muito ligadas aos impactos concretos do uso desse tipo de software, ferramentas intrusivas de vigilância, para a atividade jornalística. E eu digo isso porque, os jornalistas, assim como defensores de direitos humanos, têm sido alvos preferenciais de quem usa software de vigilância.

Gostaria de que focassem, por favor, no eslaide que está - como eu não enxergo daqui -, o eslaide que está na parte que tem um o mapa - o próximo, logo depois desse, por favor. Obrigada!

O consórcio Forbidden Stories fez uma apuração, Excelência, que revelou, em 2021, que pelo menos 180 jornalistas ao redor do mundo constavam em vistas de vigilância do *spyware* Pegasus, que já foi mencionado hoje aqui diversas vezes.

Como a gente pode ver nesse mapa que está reproduzindo essa investigação, esse tipo de vigilância atinge não jornalistas apenas em países autoritários, mas também em democracias muito consolidadas.

Se puderem passar para o próximo eslaide, por favor.

Na América Latina, a gente já tem episódios muito graves do uso ilegal do Pegasus no México e em El Salvador. No México, nós tivemos pelo menos 25 pessoas atingidas, entre jornalistas e defensores de direitos humanos. Em El Salvador, chama muito a atenção a situação do periódico o *El Fado*, em que dois terços dos jornalistas tiveram seus celulares invadidos pelo Pegasus.

Os impactos são devastadores para a atividade jornalística e porque a gente entende que é necessário dar a dimensão do que acontece com os jornalistas quando eles são alvo desse tipo de vigilância. A gente trouxe aqui alguns depoimentos, vou pedir licença também para passar para o próximo eslaide, em que a gente traz o depoimento da jornalista Khadija Ismaylova, que foi e ainda é muito perseguida pelo governo do Azerbaijão. A Corte Europeia de Direitos Humanos já reconheceu em diversas oportunidades, infelizmente, que ela tem sido alvo de perseguição, e ela diz, com um depoimento que nos toca muito, o seguinte: "Passei a noite toda pensando no que fiz com o meu telefone, me sinto culpada pelas mensagens que enviei, me sinto culpada pelas fontes que me enviaram informações, pensando que algumas formas de mensagens criptografadas são seguras e que não sabiam que meu telefone estava infectado. Os membros da minha família também foram vítimas, minhas fontes foram vítimas, as pessoas com quem trabalhei, as pessoas que me contaram seus segredos íntimos foram vítimas."

Cabe aqui ressaltar, Excelência, que além da jornalista, mais de 90 números da sua lista de contatos também foram infectados com o Pegasus. Até o motorista de táxi, sabe aquele motorista de táxi a quem a gente recorre no bairro, que conhece de algum tempo para nos levar de um lugar para o outro? Esse motorista também teve seu aparelho infectado.

Similar ao depoimento da jornalista mexicana Carmen Aristegui, um dos primeiros casos de vigilância pelo Pegasus que foi revelado no México. Também muito preocupada com o quanto essa vigilância atingiu os membros da sua família. E, por fim, o depoimento do Carlos Dada, que é do *El Fado*, que eu já mencionei aqui de El Salvador, que ressalta o prejuízo para a continuidade do trabalho, da redação, porque as fontes simplesmente pararam de falar com os jornalistas depois desse caso de infecção pelo Pegasus. Então, o que a gente trouxe aqui e várias organizações mencionaram ao longo do dia, o prejuízo para o exercício da atividade jornalística é concreto, ele é concreto, ele já foi vislumbrado na experiência de outros países.

Trouxe aqui também um trecho de uma fala da Relatoria Especial sobre a Liberdade de Expressão da ONU, que ressalta que a mera possibilidade da vigilância de jornalistas vai prejudicar a atividade jornalística. Porque se as pessoas acham que os jornalistas estão sendo alvo de vigilância, como

que elas vão se sentir seguras para fazer as suas denúncias sem ter o receio de que a sua identidade venha a ser revelada posteriormente. Então, isso prejudica sobremaneira o trabalho dos jornalistas, dos periódicos.

No Brasil, a gente queria destacar também o papel do jornalismo e o trabalho, além do trabalho incansável da sociedade civil, de institutos de pesquisa, como a gente viu ao longo do dia todo, o jornalismo tem exercido um papel essencial para revelar informações sobre o uso abusivo e ilegal dessas tecnologias intrusivas. Foi por meio da imprensa que a gente tomou conhecimento do uso ilegal do FirstMile pela Abin paralela, que já foi mencionado nessa audiência também, e que veio a público no furo do jornal *O Globo*. Sem a proteção do sigilo de fonte, é possível que hoje a gente não estivesse nem aqui discutindo toda essa temática, porque esse de fato foi um escândalo a que a imprensa toda deu muito destaque no último ano. Então, é a partir do trabalho jornalístico, inclusive, que a gente, paradoxalmente, consegue entender o que está acontecendo no cenário brasileiro com relação ao uso dessas tecnologias.

Eu trago aqui também uma outra matéria da revista *Piauí*, que fez também um amplo panorama de como essas tecnologias estão sendo adquiridas e utilizadas nas várias esferas dos governos estaduais, federal, e ressaltar um risco concreto acontecendo dentro do território nacional, porque a gente fala muito das

experiências internacionais, mas a gente tem risco para a atividade jornalística aqui. Para além da informação de que a lista de pessoas que estavam sob vigilância, com o uso do FirstMile, também envolvia jornalistas, a gente não sabe dizer a extensão e os nomes de todos os jornalistas envolvidos, mas a revista *Piauí* também identificou um caso específico que eu vou ressaltar aqui, que é do Mato Grosso, em que houve a compra do equipamento GI-2, da Cognyte, que é a mesma empresa que fornece o FirstMile. É um equipamento que permite você ouvir as conversas quando se aproxima do celular das pessoas. Então, o uso combinado do FirstMile com o GI-2 é uma forma que a gente acredita que pode estar sendo utilizada para ilegalmente acessar conversas de jornalistas.

Essa matéria revelou que esse equipamento foi adquirido pela Secretaria de Segurança Pública do Mato Grosso sob a justificativa de que ele seria usado para combate a *fake news*. Essa matéria é de dezembro do ano passado. Em fevereiro deste ano, jornalistas do Mato Grosso que vinham divulgando denúncias contra o governador daquele Estado tiveram seus celulares apreendidos numa operação da Polícia Civil que tinha por objetivo apurar crimes contra a honra do governador.

Então, a gente vê aí a gravidade dos problemas que a gente enfrenta já no uso, no mecanismo que tem previsão legal de busca e apreensão, enfim, não sabemos evidentemente se alguma tecnologia como o FirstMile ou o GI-

2 da Cognyte foram utilizados nessa investigação, mas a verdade é que o avanço dessa investigação foi barrado por uma decisão liminar proferida pela Ministra Cármen Lúcia no âmbito de uma reclamação constitucional, dada a sua evidente legalidade. E acho que isso evidencia o quanto a gente não está falando só de hipóteses remotas de vigilância, mas o quanto a gente enfrenta no Brasil uma série de dificuldades, até mesmo com o uso de ferramentas ou de métodos de investigação que já estão previstos legalmente. Se a gente tiver o uso autorizado ou chancelado de alguma maneira de softwares como o Pegasus, por exemplo, a gente vai enfrentar uma situação que corre o risco de afetar gravemente o exercício da liberdade de expressão e a atividade jornalística.

Com isso, eu queria encerrar a minha apresentação e agradecer a Vossa Excelência a oportunidade de trazer essas informações ao Supremo Tribunal Federal.

Obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Charlene Nagae pela exposição.

PERGUNTAS AOS EXPOSIDORES

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - E agora passaremos às perguntas que foram apresentadas.

Eu não sei se o Doutor André Ramiro ainda está conosco.

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Estou presente ainda, Ministro, sim.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Doutor André Ramiro, apenas uma questão. Vossa Senhoria apresentou, foi o coordenador do estudo *Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil*. Esse estudo, segundo eu compreendi, analisou, inclusive do ponto de vista empírico, contratos entre o poder público e comerciantes de ferramentas de intrusão digital no Brasil. Vossa Senhoria poderia fazer uma exposição, ainda que de forma objetiva, quais foram as conclusões a partir dessa análise? Vossa Senhoria e os demais pesquisadores chegaram a analisar os contratos firmados com o poder público brasileiro e os vendedores ou representantes dessas ferramentas de intrusão digital?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Sim, Ministro Zanin, posso fazer um balanço mais abreviado do estudo. O estudo tem mais de 60 páginas, então, eu convido todos a fazer uma leitura na íntegra, porque tem muitos detalhes, e a nossa própria metodologia também encontrou uma série de desafios em razão de um regime de sigilo que impera sobre os processos administrativos, tanto na seara da investigação criminal, como, sobretudo, da inteligência.

Então, nossas duas abordagens foram implementares, tanto fizemos pedidos via lei de acesso à informação a todas as Secretarias de Segurança Pública do Brasil, incluindo o Distrito Federal, ao Ministério de Justiça, aos Ministérios Públicos dos estados, todos os estados mais o Distrito Federal, ao MPF e ao Gabinete de Segurança Institucional da Presidência da República, a fim de coletar evidências empíricas sobre isso.

Em paralelo, também fizemos uso massivo dos portais de transparência de todos os estados. Então, isso foi um desafio, porque os portais de transparência não são padronizados. Isso envolveu um aprendizado contínuo sobre cada portal de transparência para entender como é que a gente conseguiria coletar cada contrato, e também do Poder Federal.

De saída, eu diria que os contratos ou os termos administrativos que nós encontramos nem sempre davam um padrão de informações para gente. Às vezes, a gente conseguia um anexo, que era um aditivo de contrato; às vezes, já conseguíamos a minuta inicial do contrato; às vezes, nós conseguíamos o valor também; às vezes, não conseguíamos o valor.

Então, havia uma despadronização em relação à política de transparência sobre os contratos entre o poder público e os fornecedores de ferramentas de *hacking*, que são baseados tanto no Brasil como internacionalmente. Mas nós fomos felizes o suficiente para conseguir encontrar 209 diferentes contratos

que estiveram ou ainda estavam em vigência no intervalo entre 2015 e 2021. Então, nós tivemos esse recorte temporal.

E uma das conclusões foi que todos os estados, incluindo todas as Secretarias de Segurança Pública dos estados possuíam, ou ainda possuem, ferramentas de *hacking*. E nós conceituamos as ferramentas de *hacking* como tanto aquelas de intrusão remota, como aquelas de intrusão com os celulares em mão. Então, isso foi uma decisão terminológica que nós adotamos para poder abarcar esses dois tipos de ferramentas de natureza diferentes. Então, nem todas são remotas e nem todas são apenas com celulares em mão. Nós resolvemos pegar todos os tipos de ferramenta que nós entendemos que exploram vulnerabilidades.

Isso porque o debate no Brasil ainda se encontrava no estágio muito inicial e a nossa pretensão era justamente lançar uma rede, fazer algo um pouco mais abrangente realmente, para coletar dados empíricos e assim gerar uma agenda de pesquisa que fosse mais especializada e também gerar uma agenda política para iniciar um debate regulatório em nível nacional. Então, essa foi nossa ambição no nosso estudo.

Inclusive, eu acho que um ponto pouco explorado, ainda que em sede de audiência, mas que que merece destaque, e nós fazemos essa abordagem no estudo, é sobre o mercado. A Professora Estela já mencionou isso brevemente,

mas eu acho que merece ainda mais aprofundamento, sobre o mercado de vulnerabilidades que acontece globalmente.

Então, não é porque o poder público no Brasil ou em qualquer outro país compra uma ferramenta que explora vulnerabilidade que ela se torna automaticamente, por um passe de mágica, legítima. Não, por trás, digamos, a arqueologia dessas ferramentas, ela envolve uma transação contínua de informações sobre vulnerabilidades que não são informadas aos fabricantes originais, seja o Google, seja Apple, Microsoft, Meta etc., não são comunicadas para que esses produtos, que são de uso popular, sejam atualizados e assim a gente consiga avançar em termos de cibersegurança para coletividade dos cidadãos. Mas não, essas informações sobre vulnerabilidades são vendidas para intermediários no mercado que, por sua vez, comercializam aos fabricantes de *spywares* ou de ferramentas de *hacking* de maneira geral.

Então, nós também pretendemos explorar, ainda que de uma maneira passageira, esse mercado de vulnerabilidades que o poder público termina por legitimar quando compra uma ferramenta que tem natureza de *hacking*, tem natureza de intrusão remota, tem natureza de exploração de vulnerabilidades.

Então, eu acho que esse é um debate também que deve ser levado em consideração, porque eu tenho percebido também que essa audiência tem um recorte especial, ela trata especialmente das ferramentas que são

comercialmente disponíveis, ou seja, aqueles acordos comerciais entre o poder público e os fabricantes de *spywares*, ferramentas de intrusão remota, como a gente queira nomear.

Mas um outro recorte desse debate seriam as ferramentas que estão desenvolvidas pelo próprio Estado. Então uma interrogação, uma pergunta que também deve ser feita às autoridades públicas, seja de investigação, seja de inteligência no Brasil, é se nós também, enquanto país, nós também temos capacidade de desenvolver ferramentas de intrusão remota. E não se referindo mais a esse circuito comercial, mas, sim, a própria capacidade do país em desenvolver ferramentas de intrusão remota.

Então, esse é um debate que também tem que ser levado em consideração quando a gente for ensaiar o que seria essa arquitetura regulatória para o uso de ferramentas de intrusão remota.

Não sei se eu fui o suficientemente claro, mas realmente o escopo do estudo é realmente amplo.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Foi bastante claro, Doutor André Ramiro.

Apenas para verificar se eu bem compreendi, esse estudo feito sob a coordenação de Vossa Senhoria chegou a analisar 209 contratos que foram

firmados entre o poder público brasileiro, seja na esfera estadual, seja na federal, e comerciantes de ferramentas de intrusão digital? É isso?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Perfeito, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - E esses 209 contratos que foram analisados, preponderantemente, eram na esfera estadual ou na esfera federal?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Preponderantemente na esfera estadual.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois, não.

E foi possível verificar nesse estudo, Doutor André Ramiro, se as empresas que fazem a venda ou a representação dessas ferramentas de intrusão digital, a partir do momento em que é efetuada a venda para o poder público, continuam participando do processo, ou seja, se elas recebem dados ou, de alguma forma, participam da implementação dessas ferramentas, ou se elas têm atuação limitada ao momento da venda, ou da transferência da ferramenta de intrusão?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Ministro, é variada a participação desses fornecedores de ferramentas. Na grande maioria, a gente pode dizer, com segurança, que apenas fornecem e quem faz o uso - os executivos, digamos - seria autoridade pública, mas, em uma diversidade de casos, essas empresas também participam, por meio de termos aditivos, para estender o termo do contrato e para fornecer também treinamentos a funcionários públicos sobre como usar as ferramentas.

No leque de serviços oferecidos, por exemplo, pela Cellebrite, que foi uma empresa que teve uma participação preponderante em nosso estudo e que tem a maioria dos contratos com as secretarias de segurança pública, existe um serviço de transferência de um dispositivo que uma autoridade pública não conseguiria ter acesso aos dados, porque encriptado, seguro, e que a Cellebrite forneceria essa alternativa de levar o dispositivo à sua sede, em Israel, e decriptar e ter acesso àqueles dados pessoais em uma sede de investigação ou atividade de inteligência. Esse era um serviço que preocupava especialmente a gente.

Agora não vou lembrar de cabeça, mas isto está no nosso relatório, na nossa tabela, qual foi a secretaria de segurança pública que contratou esse serviço, mas, sim, existia a possibilidade de transferência de um dispositivo

pessoal para a sede da Cellebrite, para que eles conseguissem decriptar e, então, retornar aqueles dados de forma plena, de forma legível, à autoridade pública em questão. De fato, é uma preocupação adicional.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois, não. Esses contratos, Vossa Senhoria fez referência a que, preponderantemente, foram firmados com o poder público estadual. É possível saber se apenas no âmbito da segurança pública ou também em outras esferas, por exemplo, secretarias de fazenda?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Isso, exatamente. Como eu venho acompanhando a audiência desde manhã, Ministro, eu acho que a Raquel já mencionou isso, que secretarias de fazenda em pelo menos dois estados chegaram a contratar ferramentas de extração de dados pessoais, assim como o Conselho Administrativo de Defesa Econômica, o Cade.

Para a gente, é muito estranho e nos soa muito suspeito, muito sem uma finalidade legítima, a princípio. Nós chegamos a fazer perguntas já a essas entidades, mas não obtivemos resposta. Então, é seguro dizer que a obtenção, a compra, a aquisição dessas ferramentas extrapolam, inclusive, os setores de segurança pública.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Apenas para finalizar as minhas perguntas, aqui na petição inicial, há referência a ferramentas tecnológicas invasivas do tipo *cell-site simulator*, IMSI *catchers*, e me parece que essas duas modalidades que contemplariam o Pegasus dentre outras ferramentas. Nesse estudo, nesses 209 contratos que foram analisados por vossa senhoria e pelos demais pesquisadores, é possível identificar ou sabemos quais eram as ferramentas e qual era o tipo de ferramenta de intrusão que estava sendo comercializada com os poderes públicos estaduais e federal?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Absolutamente. A princípio, nós não identificamos as usabilidades citadas na petição inicial da PGR, mas nós fazemos uma tabela a parte no nosso estudo, identificando quais são os fornecedores comerciais de cada ferramenta, quais são as ferramentas que foram negociadas e quais são as usabilidades de cada ferramenta.

Então, entramos realmente em uma seara bastante técnica para entender qual é o grau de intrusividade e de ameaça ao ecossistema de segurança cibernética que uma autoridade pública estava se aproximando. Mas, é isso.

Para concluir, nós não identificamos especificamente os que o Senhor citou, na petição inicial, mas identificamos outros e descrevemos com

bastante detalhes as ferramentas negociadas, assim como seus provedores e as autoridades que as contrataram.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutor André Ramiro.

Indago à Doutora Elizeta Paiva Ramos, se tem alguma questão? Indago ao Doutor Marcelo Turbay, se tem alguma questão?

O SENHOR MARCELO TURBAY (ORDEM DOS ADVOGADOS DO BRASIL) - Ministro, apenas um questionamento complementar, muito breve também ao Doutor André Ramiro: se no âmbito da pesquisa, se eles identificaram contratos firmados pelo Ministério Público, sobretudo do Ministério Público Estadual e também órgãos da Polícia Judiciária e Polícia Militar.

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Sim, doutor. Encontramos contratos relativos aos Ministérios Públicos, sim, tanto em nível estadual quanto em nível federal, assim como pelas polícias militares.

Agora de cabeça, não vou me lembrar de quais estados, mas falo com segurança que polícias militares também faziam contratos. Ainda que não seja de sua atribuição fazer esse tipo de atividade de inteligência e de monitoramento, algumas polícias militares também chegaram a adquirir ferramentas de extração de vulnerabilidades, especificamente as de extração de dados.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor André Ramiro.

E aqui, uma questão formulada pela doutora Maíra Fernandes, que é coordenadora do IBCCrim, à doutora Heloisa Estelitta.

Doutora Heloisa Estelitta, a questão é a seguinte: uma das preocupações com o uso de softwares espiões é com a serendipidade. O pedido do MPF, nesta ADPF, é que a autoridade descarte o material de pessoas que não estejam sendo investigadas eventualmente acessado pelo software. Essa recomendação, na visão de vossa senhoria, é suficiente para a proteção dos direitos fundamentais? Vossa senhoria vê alguma dificuldade na implementação da fiscalização desse descarte?

A SENHORA HELOISA ESTELITTA (FGV – DIREITO SP – CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO) - Obrigada, Excelência. Obrigada, Maíra.

A legislação alemã foi citada aqui várias vezes, se não às vezes diretamente, mas era a ela que se fazia referência, e ela tem medidas para cuidar. Essa é uma outra dívida que nós temos no Brasil com a prova digital. É regular o encontro fortuito de provas, que antes era uma exceção, agora passa a ser uma regra. E veja que, mesmo com a previsão da eliminação de dados inúteis no âmbito da lei de interceptações telefônicas, eu desconheço um só incidente de eliminação

dos dados de interceptações telefônicas. Essa é a nossa cultura: é não eliminar esses dados.

Então eu vejo bastante perigo nesse tipo de prova, evidentemente, não só pela privacidade, mas pela investigação de insuspeitos. E, obrigado até pela pergunta, mas para reforçar meu último argumento, que é na verdade um eco do que várias pessoas aqui disseram, num ambiente sem uma LGPD Penal, por exemplo, não é obrigatório, como não é no âmbito das interceptações telefônicas, que tratam de dados pessoais, notificar as pessoas afetadas, para que elas saibam que os dados pessoais foram tratados e eventualmente serão eliminados. Porque até isso o titular de direitos de dados pessoais tem direito a saber e controlar. Isso é o controle informacional ao qual os titulares dos dados têm direito. Obrigada.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutora Heloisa Estelitta. Deixei de perguntar à Doutora Caroline se tem alguma questão. Doutor Lucas?

O SENHOR LUCAS SALES DA COSTA (JUIZ AUXILIAR) - Poderia fazer um acréscimo, Ministro Zanin, se Vossa Excelência me permitir?

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois não. Doutor Lucas Sales, Juiz Instrutor.

O SENHOR LUCAS SALES DA COSTA (JUIZ AUXILIAR) - Eu gostaria de fazer um pequeno questionamento a um termo que foi utilizado pelo Doutor Alexandre e pela Doutora Heloisa, que particularmente eu apreciei. Os senhores falaram sobre amadurecimento institucional, então vou fazer apenas uma reflexão, Ministro Zanin, porque eu vi que os senhores, os senhores podem me corrigir se eu estiver equivocado, atestaram uma necessidade de base legislativa que seria, *a priori*, inviável, impossível - a Doutora Heloisa e o Doutor Alexandre falaram - qualquer tipo de apreciação do Supremo Tribunal Federal a respeito de uma decisão nesta ADPF sem que houvesse algum tipo de base legislativa. Mas a gente sabe, eu creio que seja um pouco incontroverso, Doutor Alexandre, que a sociedade e os fatos geralmente antecedem o Direito. As leis são muito menos velozes do que a realidade fática consegue desenvolver.

Então, nessa inação à qual alguns dos senhores fizeram referência, inação legislativa de não atuar, de não deliberar, de que forma o Supremo Tribunal Federal poderia enfrentar isso? Não seria mais razoável atestar algum tipo de deliberação, algum tipo de fixação, como a PGR mencionou, Doutora Elizeta, na petição inicial, lá na página 56, parâmetros e balizas provisórias de fixação indispensável até que, escreveu a PGR, o legislador estabeleça alguma norma. Como a gente harmonizaria essa suposta inação legislativa às quais os senhores fizeram referência, um termo que os senhores utilizaram, com a

apreciação, eventualmente, por decisão judicial, desse tema tão complexo? E eu aproveito para parabenizar também as explanações dos senhores.

Obrigado, Ministro Zanin.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Obrigado, Doutor Lucas.

A SENHORA HELOISA ESTELITTA (FGV – DIREITO SP – CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO) - No nosso entendimento, não há inação legislativa. O direito está posto. É um dever de abstenção do Estado. O âmbito total, vamos dizer assim, desse direito está protegido hoje pela Constituição Federal. E uma autorização para intervenção é possível só com o consentimento dos titulares dos dados, nós - isso não acontece na área penal, onde é uma exceção o consentimento -, ou por consentimento dos nossos representantes legais, que são os parlamentares.

O SENHOR ALEXANDRE PACHECO (FGV – DIREITO SP – CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO) - Apenas para complementar muito rapidamente, eu acho que a gente precisa fazer uma diferenciação entre o apetite na aquisição de tecnologias disponíveis e o quadro constitucional que está posto para nós, e o quadro legal que está posto para nós. Não apenas porque existe um espaço para discussão de condicionantes, que é o Legislativo justamente que está tratando disso, a LGPD Penal é um exemplo disso,

mas, quando a gente fala em amadurecimento institucional, uma das coisas que a gente tem que pensar é: será que não existe o espaço adequado com participação ampla do ponto de vista da sociedade para debater um tema complexo? Esse é um problema.

E outro problema diferente desse é a ideia de que olhamos autoridades públicas adquirindo uma tecnologia que, por várias razões expostas aqui, hoje, não encontra respaldo dentro de normas específicas que poderiam condicionar o seu uso. Nesse sentido, a primeira medida que nos vem à mente e nós nos deparamos é refrear esse apetite. Refrear por quê? O ordenamento não recebe esse apetite e refrear do ponto de vista dos riscos que a adoção dessa tecnologia, nas condições atuais, representa sem uma discussão ampla da sociedade sobre os impactos dessas ferramentas, tendo em vista os exemplos internacionais que a gente viu até então.

Uma discussão que eu acho absolutamente válida é: não deveríamos pensar em localizar as informações e impedir que informações relacionadas a investigações criminais saiam do país? Essa é uma discussão fundamental para termos. E essa é uma discussão que não aparece quando a gente vai pensar, vamos dizer assim, em medidas que aceleram uma tomada de decisão, nem que seja para o estabelecimento de requisitos preliminares.

Então, nesse sentido - e aí corroborando a fala da Heloisa -, a nossa primeira impressão e o nosso reflexo aqui é pensar nesse dever de abstenção.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Alexandre Pacheco pela exposição.

Tenho aqui uma pergunta para o Doutor André Ramiro, feita pelo Doutor Hugo Lazar, Presidente da Intelis.

Não sei se o Doutor André Ramiro ainda está nos ouvindo.

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Estou presente, Senhor Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - A pergunta é: na sua experiência em Direito comparado, como estados europeus têm regulado e controlado o uso desses softwares espiões para fins de inteligência de Estado? Há diferenças em relação à regulação e controle para fins de persecução criminal?

O SENHOR ANDRÉ RAMIRO (UNIVERSIDADE DE STANFORD - DIGITAL CIVIL SOCIETY LAB) - Sim, há diferenças.

No meu caso, olhei atentamente para o regime legal alemão e para as decisões da Corte Constitucional alemã que vêm sendo proferidas nos últimos de 20 anos.

A abordagem da corte foi não somente, de início, estabelecer a inconstitucionalidade de normas que previam a exploração de vulnerabilidade, seja para fins de inteligência ou para fim de investigação, mas criar um direito autônomo que conseguisse sopesar os testes de proporcionalidade e necessidade para decisões futuras. E isso aconteceu. Entre 2017 e 2018, a corte reconheceu estar dentro das atividades legítimas, tanto para os setores de inteligência como para os de investigação, a exploração de vulnerabilidade, desde que fossem estabelecidos requisitos *ex antes e ex post* de fiscalização e de obedecimento a princípios procedimentais.

O que nos é mais valioso - e aqui ressoo a opinião dos colegas do IBCCrim - é que o Brasil se encontra em um estágio em que uma série de reformas devem interceder esse debate para que consigamos ter uma conversa mais bem informada e mais qualificada sobre se seria constitucional, ou não, uma atividade de exploração de vulnerabilidades. Por exemplo, o nosso Sistema Brasileiro de Inteligência - SISBIN, há muito tempo, historicamente, não é reformado. Ainda que tenhamos evidências de uso de ferramentas de exploração de vulnerabilidade por parte da Abin, isso não está procedimentalizado e tipificado enquanto prerrogativa da Abin na lei que regula o Sistema Brasileiro de Inteligência.

Diferentemente da Alemanha, por exemplo, que já tem um sistema mais qualificado, inclusive uma subdivisão entre duas agências. Uma agência voltada para a vigilância doméstica, a inteligência doméstica, e uma agência voltada para a vigilância e inteligência internacional. Cada uma dessas agências já conta um diploma legal que estabelece seus direitos e deveres e, além disso, a própria lei de proteção de dados pessoais alemã, tanto no nível regional europeu, quanto no federal, também conta com pré-requisitos e atribuições para que a autoridade de proteção de dados pessoais alemão tenha também prerrogativas de realizar auditoria na sede das agências nacionais de inteligência na Alemanha. Isso, nós ainda não vemos acontecendo no Brasil. Então, acho que é uma experiência positiva, uma experiência interessante para que a gente leve em consideração.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor André Ramiro.

Não havendo mais perguntas, eu agradeço a todos os expositores deste terceiro painel; agradeço a todos que hoje estiveram aqui conosco, aos expositores dos três blocos e também a todos que nos acompanharam presencialmente ou pelo YouTube. Agradeço à Doutora Elizeta Maria de Paiva Ramos, Subprocuradora-Geral da República; ao Doutor Marcelo Tubay,

representando o Conselho Federal da Ordem dos Advogados do Brasil; e agradeço a todos que estiveram aqui conosco.

A audiência pública será retomada amanhã, às 9h30 da manhã, e teremos a presença de representantes do Ministério da Justiça e Segurança Pública, da Polícia Federal e da Agência Nacional de Telecomunicações, a Anatel.

Então, com isso, dou por encerrada esta audiência pública, desejando um boa noite a todos.

DIA 11/7/2024

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito bom dia a todos!

Quero cumprimentar todos aqui presentes. Inicialmente, a Doutora Elizeta Maria Paiva Ramos, Subprocuradora-Geral da República que subscreveu a petição inicial desta ADPF de que estamos tratando na presente audiência pública. Também cumprimento o Doutor Leonardo Magalhães, Defensor Público-Geral Federal. Cumprimento, aqui na Mesa, a Doutora Caroline Santos Lima, Juíza Instrutora, e o Doutor Lucas Sales, Juiz Instrutor. Cumprimento todas as autoridades presentes na pessoa do Brigadeiro do Ar Reginaldo Pontirolli, Chefe da Assessoria Parlamentar e de Relações Institucionais do Comando da

Aeronáutica. Cumprimento todos os presentes e todos os que nos acompanham pelo YouTube.

Nós vamos dar sequência, na data de hoje, à audiência pública iniciada ontem, na parte da manhã, da qual já tivemos três blocos de exposição durante o dia de ontem.

Esta audiência pública tem por objetivo instruir esta ADPF de que estamos aqui a tratar, com informações de todos os segmentos da sociedade, por meio de órgãos públicos, de representantes da sociedade civil, de especialistas ou de interessados que possuem experiência e autoridade no tema discutido, qual seja, os limites e possibilidades da regulamentação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal.

Para facilitar os trabalhos e dar a oportunidade de exposição a todos, eu dividi o tempo de cada expositor em 10 minutos, sem prejuízo da possibilidade, depois, de serem formuladas perguntas para a complementação das respectivas exposições.

Eu começo, então, os nossos trabalhos de hoje, dando a palavra ao Doutor Victor Cravo. O Doutor Victor Cravo é do Ministério da Justiça e Segurança Pública, é consultor jurídico, é doutor e mestre em Direito pela

Universidade de Brasília, possui especialização em regulação das telecomunicações pela Fundação Instituto Nacional de Telecomunicações, graduação em Direito pela Universidade Federal de Pernambuco, foi procurador-geral da Anatel, entre 2011 e 2016, é procurador federal, atualmente exercendo o cargo de procurador jurídico no Ministério da Justiça e Segurança Pública desde 2023.

Doutor Victor Cravo tem a palavra, por gentileza.

O SENHOR VICTOR EPITÁCIO CRAVO TEIXEIRA (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA) - Excelentíssimo Senhor Ministro Cristiano Zanin; Excelentíssima Senhora Elizeta Ramos, Subprocuradora Geral da República; Excelentíssimo Senhor Leonardo Magalhães, Defensor-Geral Federal. Bom dia a todos.

É uma honra estar aqui hoje representando o Ministério da Justiça e Segurança Pública nesse debate tão importante para a sociedade. Essa ADPF 1.143 visa tratar da constitucionalidade do uso das ferramentas de intrusão e monitoramento remotos. E gostaria de pautar a minha contribuição pela abordagem das seguintes perguntas objeto da ADPF: Quem pode usar? Quais ferramentas? Para quê e como? Do começo ao fim, a Constituição Federal, no nosso entendimento, é a resposta a essas perguntas. E sempre entendendo que só é possível legislar nos limites estritos da Constituição.

Então, vou começar a minha fala a partir do quadro legal que trata da suspensão legítima do sigilo das comunicações; depois, uma breve visão sobre as ferramentas principais de que estamos tratando; e, depois, um apanhado do futuro da suspensão legítima do sigilo das comunicações.

Então, como mencionei, no nosso entendimento, tudo está pautado pela Constituição, no art. 5º, XII, que trata do sigilo das comunicações, da inviolabilidade do sigilo das comunicações.

É importante notar que a inviolabilidade do sigilo das telecomunicações abarca não apenas as chamadas de telefone celular, mas também dados transmitidos via internet, quaisquer sinais de dados transmitidos, e sua quebra tem que ser feita por ordem judicial e para fins de investigação criminal e instrução processual penal. É muito importante salientar esse ponto, porque é sempre necessário, para que o sigilo seja legitimamente suspenso, que haja um indício de crime.

Portanto, é possível depreender que a violação ao sigilo é proibida, então, para qualquer outro fim que não seja instrução criminal ou instrução processual penal. A exceção a isso está na própria Constituição, na decretação dos estados de sítio e de defesa, que é onde se trata da soberania nacional e das questões relacionadas à instabilidade das instituições.

Outro ponto ainda imprescindível é na forma da lei. Afinal de contas temos uma lei para tratar disso, que é a Lei nº 9.296, de 1996. E ela diz que a interceptação das telecomunicações é de qualquer natureza, inclusive o fluxo de comunicações em sistemas de informática e telemática, ou seja, os dados transmitidos na internet. E a lei também prescreve - isso é um ponto importantíssimo - o apoio técnico especializado das prestadoras de serviços de telecomunicações.

Para dar concretude a isso, temos a regulação da Anatel já estabelecida, que diz que as tecnologias necessárias à suspensão do sigilo devem integrar a plataforma da prestadora. E a Anatel deve estabelecer, por meio de suas regulamentações, as condições técnicas específicas, observada a Constituição.

Então, isso já existe, isso tudo é feito dentro do Grupo Técnico de Suporte à Segurança Pública, que é o GT-Seg, coordenado pela Anatel, onde há debates interinstitucionais com os órgãos competentes para tanto. E há também o Sistema Integrado de Investigação Telefônico e Telemático - Sittel, que é por meio do qual ocorrem hoje todas as suspensões legítimas do sigilo das comunicações.

Então vamos tratar agora das ferramentas.

Elas são fornecidas por empresas privadas, nacionais e estrangeiras, ao arrepio da legislação que disciplina a suspensão legítima do sigilo das comunicações; não são um apoio às prestadoras de serviços de

telecomunicações, como já vimos na lei; e elas exploram vulnerabilidades da rede pública de telecomunicações e dos sinais dos aparelhos celulares. A título exemplificativo, FirstMile e Pegasus, dos quais vou tratar agora.

A vulnerabilidade da rede de telecomunicações explorada pelo FirstMile é o Sistema de Sinalização nº 7, o SS7, que são protocolos de telecomunicações que fazem a interconexão, que fazem a comunicação entre a estação rádio-base e os nossos celulares, que estão sempre em comunicação com as redes móveis. Por exemplo, temos aqui um raio de cobertura de uma ERB e um celular. Então o celular comunica-se com a ERB, dizendo que ele está lá naquela área de cobertura. A ERB o reconhece, registra que esse celular está lá. Se a pessoa que detém o celular se locomove e vai para uma outra área de cobertura, ela deixa de estar registrada na ERB anterior, vai para a ERB seguinte, onde o mesmo processo acontece. Dessa forma é que se conhece, portanto, o monitoramento das pessoas. Então, esses *softwares* de monitoramento secreto conseguem puxar essas informações da rede de telecomunicações explorando vulnerabilidades, obtendo, em tempo real, dados de tráfego, como o IMSI, que é o número único gravado no SIM Card, mais a geolocalização da ERB. Esses são dados de origem e destino; e é importante aqui fazer um parêntese dizendo que esses dados não são dados cadastrais. Esses são dados de comunicação e, sendo dados de comunicação, são protegidos pela inviolabilidade do sigilo do art. 5º.

Isso também está dito na Convenção de Budapeste, que foi promulgada pelo direito brasileiro por meio do Decreto nº 11.491. Dados cadastrais, nesse caso, todos sabem, são dados constantes em contratos, por exemplo, nome, endereço, CPF. E os dados de tráfego são dados decorrentes do processo de comunicação - não a comunicação em si -, são dados do processo de comunicação de aparelhos interconectados na cadeia de comunicação, que são origem, destino, caminho, hora, data, extensão, duração e tipo de serviço. Esses são dados de tráfego que são sigilos de comunicação regulados pela Constituição Federal.

No caso do Pegasus, a infecção não ocorre na rede de telecomunicações; ela ocorre no aparelho, mas depende da rede para chegar até o aparelho. Então é um *spyware*, é um *software* malicioso com fins de espionagem. A infecção ocorre no dispositivo, que pode ser infectado com clique ou sem clique. Ao fazer isso, dá acesso a todos os aplicativos nele existentes, inclusive pode ligar a câmera, ligar o microfone, acessar fotos, enfim, fazer tudo o que o administrador do aparelho pode fazer.

E qual é o futuro dessa suspensão legítima do sigilo das comunicações?

A nossa visão é de que há uma suficiência do quadro legal vigente, já exposto no primeiro eslaide: Constituição; Lei de Interceptações; a

resolução da Anatel, que diz que as tecnologias necessárias à suspensão do sigilo devem integrar a plataforma da prestadora.

Ou seja, eventuais melhorias, aprimoramentos nessas ferramentas devem ser tratados e abordados dentro do trabalho interinstitucional, que já ocorre hoje em dia no GT-Seg, que é o Grupo Técnico de Suporte à Segurança Pública, dentro da Anatel. Dele participam, legitimamente, o Ministério da Justiça e Segurança Pública, Polícia Federal, Polícias Civis, Ministérios Públicos de forma geral, Poder Judiciário e CNJ - são os agentes legitimados para tratar do tema. E esse debate, ocorrendo nesse grupo, dá oportunidade a que haja transparência e *accountability*, porque nas agências reguladoras toda a discussão é feita de forma transparente, as regulações passam por consulta pública, o processo é claro, aceita a participação de terceiros, de acordo com a Lei do Processo Administrativo.

Então essas são as nossas contribuições. Ficarei à disposição de todos nas perguntas.

Obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Victor Cravo.

No início da audiência, ou da continuidade, eu anunciei a presença da Doutora Elizeta Paiva Ramos. Indago se Vossa Excelência gostaria de

fazer uso da palavra neste início da audiência ou se prefere aguardar depois para eventuais perguntas. Depois.

Da mesma forma, pergunto ao Doutor Leonardo Magalhães, Defensor Público-Geral Federal, se gostaria de fazer o uso da palavra nesse momento inicial, ou ao final, ou em ambas as oportunidades.

O SENHOR LEONARDO CARDOSO MAGALHÃES (DEFENSOR PÚBLICO-GERAL) - Pode ser agora ou ao final, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Pois não. Vossa Excelência tem a palavra.

O SENHOR LEONARDO CARDOSO MAGALHÃES (DEFENSOR PÚBLICO-GERAL) - Bom dia a todos e a todas.

Excelentíssimo Senhor Ministro Cristiano Zanin, Excelentíssima Senhora Subprocuradora-Geral Elizeta Ramos, todos que nos acompanham na audiência. Trata-se de um tema bastante importante.

A Defensoria Pública, como instituição permanente do Estado, instrumento e expressão do regime democrático, ao longo dos anos, tem-se envolvido em debates sobre direitos constitucionais. De fato, é essencial pensarmos as consequências que o uso desses mecanismos, aplicativos e aparelhos podem promover no direito à privacidade, à intimidade, das pessoas e também no direito ao sigilo das comunicações.

É uma honra estar em um fórum tão qualificado como este Supremo Tribunal Federal para discutir esse tema de extrema relevância para nossa sociedade, que são a privacidade e a intimidade digitais, os perigos apresentados pelos aplicativos de intrusão digital.

Em uma sociedade cada vez mais conectada e interconectada como a nossa, a proteção dos dados pessoais e da privacidade do cidadão se tornou um exemplo de extrema preocupação e pauta de interesse de todos nós, no âmbito jurídico, não apenas para a preservação das individualidades e intimidades de cada cidadão, mas é certo que o mal uso das tecnologias acaba por comprometer os direitos humanos e até mesmo comprometer o regime democrático.

Vejamos algumas ameaças, inclusive já citadas no primeiro dia e hoje, como por exemplo o Pegasus *spyware.* Permitam-me começar por esse aplicativo.

Esse programa espião foi desenvolvido pela empresa israelense NSO Group, e o *software* se tornou símbolo de espionagem estatal, sofisticada e invasiva. Suas capacidades incluem acessar mensagens, chamadas, e-mails, além de ativar câmeras, microfones de dispositivos infectados, sem que o usuário, a pessoa tenha o conhecimento de que seu telefone, aparelho celular, esteja contaminado, infectado pelo programa.

Nós tivemos alguns casos verídicos do uso, como o do jornalista saudita Jamal Khashoggi, através de sua trágica morte, o qual teve seus contatos monitorados pelo Pegasus, permitindo rastreamento minucioso das suas atividades. Tivemos também casos de ativistas de direitos humanos no México, onde diversos ativistas, jornalistas e advogados em direitos humanos foram alvos do Pegasus, incluído pelo governo mexicano para intimidar aqueles que questionavam políticas governamentais.

Aí, é importante dizer que muitas vezes a Defensoria Pública se envolve em temas e em defesas de pessoas e comunidades, e, em alguns momentos, nesse papel contramajoritário, acaba por incidir em algumas questões ou interesses estatais que possam comprometer, de certa forma, a segurança dos próprios defensores de direitos humanos.

O FinFisher, ou FinSpy, é outro programa e perigo também. Um exemplo igualmente pernicioso, conhecido como FinSpy, desenvolvido pela empresa alemã Gama Internacional. Esse *software* permite monitorar quase todas as atividades em dispositivos infectados, desde a gravação das teclas até mesmo o acesso às câmeras e microfones.

Nós temos o caso do uso do FinFisher no Bahrein. Ele foi usado para espionar ativistas pró-democracia durante o levante da Primavera Árabe. Os

alvos incluíram advogados e defensores de direitos humanos, os quais foram monitorados de forma contínua e invasiva.

Na Etiópia, também, o governo utilizou o FinFisher para espionar jornalistas e membros da oposição, esforço para suprimir a dissidência política e a liberdade de imprensa.

No Egito, há denúncias também de que a empresa ofereceu ao governo o programa e que dois ativistas de direitos humanos tiveram acesso a documentos na sede do serviço de investigação e segurança do Estado do governo egípcio, em 2011, em que se comprovou o uso desse aplicativo.

O Hacking Team - Remote Control System é uma empresa italiana que desenvolveu o RCS, um *software* espião capaz de infiltrar dispositivos e coletar dados sigilosamente.

Esse aplicativo foi usado no Marrocos para monitorar jornalistas e ativistas de direitos humanos que criticavam e que tinham posturas contrárias ao governo de turno. Relatórios indicam que esse *software* foi usado para acessar e-mails de comunicações privadas, comprometendo a segurança e a liberdade dos indivíduos.

Nos Emirados Árabes Unidos, nós tivemos o uso do RCS também para espionar dissidentes políticos, com relatórios apontados para o uso sistemático do *software* a fim de controlar e intimidar opositores do regime.

O Dark Caracal é outra operação de espionagem cibernética atribuída a um grupo vinculado ao governo libanês e que utilizou esse *spyware* para atacar alvos em todo o mundo. Em vários países essa operação Dark Caracal comprometeu dispositivos, incluindo Estados Unidos, Canadá, Alemanha, França. Os alvos variavam entre militares, jornalistas e até mesmo ativistas de direitos humanos. Ele foi utilizado também para monitorar comunicações privadas, roubar documentos sensíveis e coletar informações pessoais, demonstrando a extensão global e a sofisticação das operações de espionagem.

Diante dessas ameaças, desses programas, aplicativos que se desenvolvem, que evoluem ao longo do tempo, é importante que a legislação brasileira acompanhe essa evolução.

Nós temos hoje tanto o Marco Civil da Internet, entre outros temas também, dispositivos, normas constitucionais que preconizam a privacidade, a inviolabilidade, o sigilo das comunicações e a intimidade, mas, ainda assim, entendemos que merece uma melhor análise, um melhor cuidado por parte do poder público brasileiro em relação à normativa que preconiza e que garante,

de fato, que as pessoas tenham ciência ou que sejam protegidas de qualquer acesso espião e qualquer violação da sua intimidade.

É imperativo que reconheçamos os direitos digitais como uma extensão natural dos direitos humanos. A privacidade digital deve ser protegida com o mesmo vigor que defendemos a privacidade física. A nossa Constituição e os tratados internacionais dos quais o Brasil é signatário também impõem essa proteção.

Por isso, eu evoluo aqui quatro propostas de regulamentação bastante simples para tema de reflexão, como:

1) O fortalecimento das nossas leis de privacidade. Acho que é importante promover uma constante atualização das nossas leis, para incluir proteções específicas contra *spyware* e outras formas de vigilância e intrusão digitais;

2) Criação de um órgão de supervisão independente. Acho que é importante avançarmos em órgãos independentes para supervisionar o uso dessas tecnologias e garantir transparência e responsabilidade no uso e responsabilizar inclusive aqueles agentes públicos que eventualmente adotem ou utilizem esses mecanismos contra a disposição normativa;

3) Ampliar os investimentos em tecnologia de segurança e privacidade, promover o uso da criptografia avançada e outras tecnologias de segurança, para proteger as comunicações e os dados telemáticos de todos os cidadãos;

4) E reforçar colaboração do poder público brasileiro com a colaboração internacional, para promover acordos internacionais, regulamentar o uso do *spyware* e proteger a privacidade digital no âmbito global. Como eu disse, esses exemplos que foram mencionados não são uma situação que ocorre apenas no Brasil, mas no mundo, tanto na Ásia como na África e na Europa.

Excelentíssimo Ministro, a proteção da dignidade, da intimidade humana, da inviolabilidade do sigilo da comunicação e da privacidade digital é fundamental para a preservação de uma sociedade livre e democrática.

A Defensoria Pública da União reafirma o seu compromisso com a defesa dos direitos humanos e dos direitos constitucionais e se coloca à disposição para colaborar na construção de um marco regulatório robusto, que equilibre segurança e liberdade e que resguarde os direitos humanos, inclusive dos ativistas e dos defensores de direitos humanos que eventualmente adotem posições contrárias a posições de governantes de turno e que têm os seus direitos básicos,

como a inviolabilidade e o sigilo de suas comunicações, violados porque oferecem, de certa maneira, uma ameaça a tais governantes.

Convoco todos para um diálogo contínuo, inclusivo, envolvendo todos os *stakeholders*, os agentes importantes - vi aqui que a mesa está composta por diversos especialistas, diversas áreas -, para construirmos um futuro digital mais seguro, mais justo, mais inclusivo para todos os cidadãos e que, de fato, nós tenhamos a certeza de que esses aplicativos não serão usados para violar direitos fundamentais e comprometer o Estado Democrático de Direito.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Leonardo Magalhães pelo pronunciamento.

E antes de dar a palavra ao próximo expositor, eu registro que todas essas exposições que tivemos na data de ontem - foram três blocos - bem como as exposições na data de hoje ficarão disponíveis no canal do Supremo Tribunal Federal para consulta, bem assim as apresentações que forem feitas hoje e as que foram feitas na data de ontem também ficarão disponíveis no site do Supremo Tribunal Federal para consulta.

Então, agora eu passo a palavra para o Doutor Rodrigo Morais Fernandes, que é diretor de inteligência da Polícia Federal.

Doutor Rodrigo Morais Fernandes é graduado em Direito, com pós-graduação em Direito Público, Inteligência de Estado e Inteligência de Segurança Pública. Foi advogado e atua na Polícia Federal desde 2002 e, atualmente, é diretor de inteligência policial.

Doutor Rodrigo Morais, tem a palavra, por gentileza.

O SENHOR RODRIGO MORAIS FERNANDES (POLÍCIA FEDERAL) - Muito obrigado! Bom dia, Ministro Cristiano Zanin; Doutora Elizeta Ramos, Subprocuradora-Geral da República; Doutor Leonardo Magalhães, Defensor Público-Geral Federal.

Inicialmente, Ministro, eu queria agradecer a oportunidade de estarmos aqui colaborando com o tema, um assunto que é muito caro à Polícia Federal e afeta diretamente as nossas atividades.

A minha fala aqui vai muito ao encontro do que o Doutor Victor Cravo, do Ministério da Justiça, já explanou. Do ponto de vista da Polícia Federal, entendemos que não há necessidade de regulamentação da matéria. Entendemos que a legislação atual disciplina plenamente o assunto.

Nós temos, desde a Constituição Federal, que é clara ao dizer que as interceptações telefônicas e telemáticas, o acesso a dados sigilosos e o acesso a dados que afetam a intimidade e a vida privada das pessoas se dão única e exclusivamente para investigação criminal ou para instrução de processos penais,

mediante ordem judicial prévia. E a legislação já vem nesse sentido, esclarecendo exatamente os requisitos e as condições para que se deem essas autorizações judiciais para a interceptação e as possibilidades em que isso pode ocorrer. E a legislação, inclusive, prevê penalidades para quem o faz de forma ilegal ou clandestina.

Nesse debate, Ministro, eu acho interessante termos em mente a separação do conceito do que é inteligência e do que é investigação criminal. Isso precisa ficar bem claro.

A Polícia Federal tem uma peculiaridade, porque nós atuamos precipuamente com atividade investigação criminal, por meio dos nossos inquéritos policiais. Porém, atuamos também com inteligência. Nós fazemos parte do Sisbim, nós atuamos na inteligência de Estado, nós produzimos conhecimento para assessorar o nosso diretor, ministros de Estado e o próprio Presidente da República, mas não nos é permitido o uso desse tipo de ferramenta intrusiva para essa atividade.

Eu não posso interceptar pessoas, não posso ter acesso a dados telemáticos, não posso sequer fazer infiltrações. Eu não posso fazer escutas ambientais, nem mesmo com ordem judicial prévia, porque não tem permissivo legal para isso. Então, eu não posso, de forma alguma, no exercício da atividade de

inteligência que eu faço permanentemente enquanto diretor de Inteligência da Polícia Federal, fazer uso desses mecanismos.

Portanto, na nossa avaliação, isso tem que ficar bem claro, o que é investigação criminal e o que é atividade de inteligência.

E, reforçando a fala do Doutor Victor, acho que minha colaboração pode ser mais no sentido de explanar um pouco sobre essas ferramentas.

Na leitura da peça inicial da Subprocuradora, eu percebo que todas as ferramentas lá citadas dizem respeito à interceptação de comunicações. Aqui já foi dito sobre o Pegasus, o FirstMile. Existem várias outras. Tanto o FirstMile quanto o Pegasus possibilitam a interceptação remota, ou seja, o acesso ao telefone, o acesso aos dados do aparelho celular do cidadão se dá de forma remota. Como disse o Doutor Vitor, ele se dá acessando vulnerabilidades da nossa rede de telefonia, da infraestrutura de telefonia nacional.

Veja a gravidade disso! Uma empresa estrangeira - no caso, Israelense - acessa a nossa rede, a nossa infraestrutura crítica de telefonia e, com isso, simula uma antena, uma ERB, que vai possibilitar acessar o aparelho do cidadão, inclusive inserindo *malwares* lá, o que chamamos de agentes-espiões, para ter acesso a todos os dados do aparelho do cidadão, inclusive, como o Doutor Vitor já falou, acessando as funcionalidades do aparelho.

A gravidade disso é muito grande, porque hoje é possível dizer, em tese - veja bem, em tese -, que o Brasil, a infraestrutura de telefonia brasileira pode estar servindo para a espionagem internacional, porque se consegue, por meio desses aparelhos, interceptar qualquer telefone no mundo inteiro, qualquer um. Em situações, hoje, de guerra que vivenciamos, um alvo qualquer, um cidadão de guerra pode estar sendo monitorado por meio da rede de telefonia brasileira.

No entanto, Ministro, esses recursos são necessários para a atividade de investigação. A Polícia Federal há muito estuda essas ferramentas. Nós nunca adquirimos, justamente por não saber como funcionava. Agora, sabendo, por meio de uma investigação com base em laudos pericial, entendemos a funcionalidade. Estamos em tratativas com a Anatel para tentar regulamentar, porque a gente precisa, sim, para a atividade de investigação criminal, com ordem judicial prévia, ter acesso a esse tipo de solução.

Isso acontece no mundo inteiro, todas as polícias do mundo possuem essas funcionalidades, exercem esse tipo de técnica investigativa, porém com a interveniência das operadoras. Ali, sim, a gente garante a auditabilidade e a segurança de que aquilo está sendo feito conforme a lei determina, não da forma clandestina como hoje a gente verifica.

Então, já temos mecanismos. A Polícia Federal mesmo tem tecnologia suficiente para disponibilizar esse tipo de recurso a quem por direito

pode fazê-lo. O que nós não temos é o acesso à rede, porque, para isso, precisamos das companhias telefônicas. E queremos que as companhias telefônicas estejam envolvidas nesse processo, com a parceria da Anatel, que já está discutindo o tema.

Então, Ministro, eram essas as contribuições que eu tinha a colocar aqui sobre o tema. Fico à disposição, se tiver alguma outra dúvida, poderei esclarecê-la.

Muito obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Muito obrigado, Doutor Rodrigo Moraes, pela exposição.

Eu agora passo a palavra à Doutora Lílian Cintra de Mello, que é também do Ministério da Justiça e Segurança Pública, da Secretaria de Direitos Digitais.

Doutora Lílian Cintra de Mello é doutora e bacharel em Direito pela Universidade de São Paulo, com período de mobilidade internacional como pesquisadora visitante da Faculdade de Direito de Harvard, no Institute for Global Law and Policy. Participou do programa de intercâmbio na Science Po, na França. Foi coordenadora do Grupo Direito e Pobreza da Faculdade de Direito da USP, professora doutora substituta em Direito Comercial na Universidade de Brasília. Atuou no gabinete do Ministro Ricardo Lewandowski, aqui no Supremo Tribunal

Federal, e hoje atua no Ministério da Justiça e Segurança Pública, na Secretaria de Direitos Digitais.

Com a palavra a Doutora Lílian Cintra de Mello, por gentileza.

A SENHORA LILIAN CINTRA DE MELO (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA – SECRETARIA DE DIREITO DIGITAL) - Bom dia a todas e todos. Cumprimento o Excelentíssimo Senhor Ministro Cristiano Zanin, relator desta arguição de descumprimento de preceito fundamental; Excelentíssima Senhora Subprocuradora-Geral da República Elizeta Maria de Paiva Ramos, subscritora dessa ação; Excelentíssimo Senhor Defensor Público-Geral Federal, Leonardo Magalhães; senhores juízes instrutores Doutora Carolina Santos Lima e Doutor Lucas Sales; senhores servidores desta egrégia Corte e demais presentes.

Primeiro, agradeço a oportunidade de estar aqui hoje e parabenizo esta inovadora iniciativa de chamada desta audiência pública.

Os novos meios ocultos de investigação criminal em ambiente digital trazem desafios relevantes, tanto ao Direito Constitucional quanto ao Direito Processual Penal.

Conforme já exposto pelos meus colegas do Ministério da Justiça e da Segurança Pública, a distinção entre atividade investigativa e de inteligência e

práticas de vigilantismo e espionagem é extremamente relevante nesse caso. Então, eu reitero os conceitos aqui trazidos.

Na investigação, a coleta de dados e a produção de elementos probatórios visa à instrução do processo judicial e, por eventualmente poder vulnerar direitos e garantias, carece, no caso de medidas cautelares, de decisão judicial para que qualquer medida posta em prática seja objeto de um contraditório no futuro.

O escopo da atuação de inteligência, por sua vez, é a produção de um conhecimento sensível em níveis estratégicos, táticos e operacionais que se faz por meio de coleta, análise e difusão de informações qualificadas. Ou seja, não se fala em inteligência com dados sensíveis e dados confidenciais; inteligência se faz com dados abertos. E ela se presta, na verdade, a um processo decisório, não podendo ser utilizada como prova em face da restrição de acesso apenas a quem tem a necessidade de conhecer.

Então, mecanismos de controle, tanto interno como externos, bem como rastreabilidade e auditabilidade são pressupostos de tecnologias investigativas para garantia de direitos e garantias fundamentais.

A inteligência, portanto, não se confunde de forma alguma com práticas de vigilantismo e espionagem, que, nesse caso, é o uso inadequado e ilegal, como foi falado pelos meus colegas do Ministério da Justiça, de ferramentas

invasivas não em prol de um interesse público, mas de um interesse privado ou comercial.

E aqui acho importante destacar, quando falamos em prática criminosa, que o próprio Código Penal Brasileiro e a Lei nº 9.296 tipificam essa prática criminosa vedada por lei.

Então, o art. 154 fala que invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita tem pena de reclusão de um a quatro anos e multa. O art. 10º, por sua vez, da Lei nº 9.296 dispõe que constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebra de segredo de justiça sem autorização judicial ou com objetivos não autorizados em lei, e tem uma pena de dois a quatro anos e multa.

Então, percebam que é extremamente relevante para a discussão desse caso essa diferenciação - e aqui eu repito com bastante ênfase - entre investigação, inteligência e práticas de vigilantismo.

E é importante também ressaltar que a generalização do desvio de conduta de servidores públicos no caso de um uso indevido de tecnologias representa um risco grande ao Estado Democrático de Direito, principalmente

numa luta, que é desigual, contra o crime organizado, que não dispõe de limite legal nenhum para sua atuação.

Então, é necessário o fortalecimento das estruturas de fiscalização, o acompanhamento e a responsabilização de atividades ilegais, que não se confundem de forma alguma com as atividades de investigação e de inteligência. E aqui, reitero, investigação sempre com uma decisão judicial; e inteligência sempre com uso de dados abertos.

Acho importante também trazer que algumas recentes investigações da Polícia Federal com lastro em laudos periciais demonstraram que o uso de programas de intrusão virtual remota e outras ferramentas invasivas para fins de interceptação e comunicações fomenta o desenvolvimento e a comercialização de ferramentas por empresas privadas, que se valem de vulnerabilidades das redes de telefonia nacional para, clandestinamente, acessarem os dispositivos eletrônicos, como foi trazido pelos meus colegas Doutor Victor Cravo e Doutor Rodrigo Moraes.

Então, cada vez mais nos deparamos com uma situação em que o combate ao crime organizado, complexo, com o uso de novas tecnologias e diversificado, demanda uma legislação de regência, como já existe hoje, que defina critérios claros para interceptação telemática, quando a medida se faz necessária para apurações penais, que é a realidade que já vivemos. Sendo que essa técnica

deve se dar sempre, preferencialmente, com a intervenção das operadoras de telefonia, as quais são autorizadas pelo Estado a prestar serviço de comunicação telefônica e de dados, permitindo uma auditoria e um controle das ações policiais e judiciais.

Por que eu faço essa ênfase nesse ponto? Porque o uso de atores privados estrangeiros com acesso às nossas redes críticas e à nossa infraestrutura traz, na verdade, um risco por quem está tendo acesso esses dados e pela forma como eles estão sendo geridos.

E aqui faço também um breve comentário com relação ao arcabouço jurídico constitucional e nossas importantes garantias, já previstas no Brasil.

Então, o art. 5º define o direito à privacidade e ao devido processo legal e condiciona a quebra de sigilo a uma prévia decisão judicial que demonstre necessidade, adequação e proporcionalidade do afastamento dos direitos fundamentais, sempre para fins de investigação criminal ou instrução processual.

Mais recentemente, é importante destacar também que a Emenda Constitucional nº 115, de 2022, introduziu um importante direito fundamental, que é a proteção dos dados pessoais, incluídos também no rol do art. 5º. Então, hoje, a proteção e a promoção do direito constitucional à proteção de

dados pessoais demandam o atendimento a princípios como finalidade, necessidade, qualidade dos dados, transparência, segurança, prevenção, prestação de contas, conhecida também como auditabilidade.

Sendo assim, protocolos de segurança no tratamento de dados, bem como as diretrizes e princípios gerais no regime nacional de proteção de dados pessoais, devem ser institucionalizados a níveis de procedimentos administrativos em matéria penal e de atividades finalísticas de trabalho de investigação propriamente dito. E aqui, vejam que em momento nenhum estou falando em atividade de espionagem, pois essa é, claramente, ilegal.

Além disso, essas garantias constitucionais também estão replicadas no próprio Marco Civil da Internet, que estabelece também a necessidade de uma ordem judicial para a guarda e o acesso a registros de conexão, aplicação e conteúdo das comunicações. Então, coleta, armazenamento, guarda, tratamento de registros de dados pessoais e de comunicação, todos esses precisam respeitar o estabelecido no Marco Civil da Internet, que tem também uma forte garantia ao direito à privacidade, à proteção de dados e ao próprio sigilo das comunicações privadas.

E, partindo para o final da minha apresentação, eu queria deixar claro também que, diferentemente do Brasil, há países que atribuem competências de monitoramento aos órgãos de inteligência por motivo de defesa nacional. E o

fazem por meio da sua constituição, como é o caso de alguns países europeus, como a Espanha. Por isso que, nesses países, é possível falar em inteligência com esse tipo de ferramenta.

Mas também existem outros países que proíbem o monitoramento intrusivo de seus cidadãos sem que haja suspeita de crime, como é o caso, por exemplo, de Portugal e dos Estados Unidos.

Então, eu passo a minha conclusão.

O arcabouço legal em vigor protege a intimidade, a vida privada dos cidadãos e o sigilo e, ao mesmo tempo, já estabelece critérios que são rigorosos para a única exceção constitucionalmente prevista para a inviolabilidade do sigilo das comunicações pessoais, ou seja, quando for imprescindível para a apuração criminal.

Então, levando em consideração - e aí eu peço até desculpas por ser repetitiva nessa classificação, mas acho que ela importa demais para a solução do caso - a diferenciação entre atividade investigativa, atividade de inteligência e práticas de vigilantismo e espionagem, o uso e a comercialização de equipamentos intrusivos devem ser coibidos e criminalizados, no estrito termo da legislação atual, impondo-se que o atendimento às necessidades e demandas de interceptação telemática para investigações criminais seja servidas por meio de empresas de

telefonia e de provedores de acesso à internet com sede no Brasil nos termos de decisões judiciais e autorizativas.

Portanto, acho importante também essa preocupação com o acesso à nossa infraestrutura crítica de telecomunicação e com a proteção dos dados de cidadãos brasileiros.

Com isso, eu encerro a minha fala e agradeço a oportunidade de estar aqui novamente.

Obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Lilian Cintra de Melo.

Agora passo a palavra ao Doutor Gustavo Borges, que é Superintendente de Controle de Obrigações da Agência Nacional de Telecomunicações, a Anatel.

O Doutor Gustavo Borges é graduado em Administração de Empresas pela Universidade de Brasília, tem especialização em Finanças pelo Instituto Brasileiro de Mercado de Capitais, ocupa atualmente a Superintendência de Controle de Obrigações da Anatel, onde é servidor de carreira desde 2009. Exerce a liderança e a coordenação do Grupo Técnico de Segurança Cibernética, o

GT-Ciber, e representa a agência no Comitê Nacional de Cibersegurança, o CNCiber.

Com a palavra, o Doutor Gustavo Borges.

O SENHOR GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL) - Bom dia a todos!

Eu gostaria de saudar o excelentíssimo Relator, Ministro Cristiano Zanin, a Subprocuradora-Geral da República Doutora Elizeta Ramos, o Doutor Leonardo Magalhães, Defensor Público, a Doutora Caroline, o Doutor Lucas, todos que estão aqui presentes e os que estão acompanhando pela internet.

Como dito, eu sou Gustavo Borges, Superintendente de Controle de Obrigações da Anatel. É bem difícil fazer essa explanação, uma vez que foram colocadas tantas informações importantes na audiência e pode soar um pouco repetitivo, em alguns momentos, para quem está aqui desde ontem.

A Anatel parabeniza a realização desta audiência pública. Acho que o objetivo é fornecer ao Supremo Tribunal Federal subsídios necessários para a formação de convencimento sobre um tema de alta relevância para a sociedade brasileira.

Já foi muito dito sobre as legislações incidentes, mas acho que vale a pena somente referenciar a Constituição, a Lei Geral de Telecomunicações,

que reafirma o sigilo das telecomunicações, a Lei de Interceptação, a Lei das Organizações Criminosas e o Marco Civil da Internet. Todos eles vão na mesma direção, no sentido de que a regra é o sigilo das comunicações e que a exceção é justamente a questão da investigação e persecução penal mediante decisão judicial.

Em um país com mais de 200 milhões de habitantes, não são raras as ordens de quebra de sigilo, por mais que hoje tenha sido comentado, em algumas falas, que há um certo *démodé* em relação à questão de quebrar o sigilo telefônico. Na verdade, no ano passado, nós tivemos mais de 10 milhões de solicitações às operadoras de telefonia móvel, isso envolvendo tanto a solicitação de dados cadastrais quanto quebras de sigilo.

Imaginem os senhores se essas ordens fossem todas pulverizadas, cada um pedindo à sua maneira e as operadoras recebendo em diversos *locus* diferentes. Então, há dez anos, o Ministério Público Federal requereu à Anatel a implantação de um sistema similar ao Simba, que era o sistema de quebra de sigilo no setor bancário, e isso foi feito. Foi padronizado pela Anatel, junto com as operadoras e órgãos de segurança pública o Sittel, que é o sistema de investigação telefônica e telemática.

De 2014 para cá, nós tivemos evoluções. Nós já temos a versão 2.1, aprovada este ano, que é a versão mais recente do Sittel e que permite o envio

e o atendimento de pedidos judiciais de interceptação telefônica e telemática, incluindo escuta telefônica, fluxo de dados e localização. Então, os dados de localização já estão disponíveis nessa sistemática.

Contudo, é importante esclarecer que os dados de localização não são constituídos como dados cadastrais. Na verdade, são fornecidos nesse sistema, mas somente mediante autorização judicial.

Esse é um sistema que está em constante reavaliação e existe um grupo permanente, conforme foi citado nas falas anteriores, criado pela regulamentação da Anatel. Existe a Resolução nº 738, de 2020, que, de fato, inseriu obrigações às operadoras na questão de sigilo, prevenção à fraudes e apoio à segurança pública.

Então, nessa resolução criou-se o grupo GT-Seg, foi citado algumas vezes, e esse grupo é competente para fazer essa discussão sobre evoluções dos procedimentos para quebra de sigilo, claro, mediante todo o atendimento legal incidente. Esse grupo conta com a participação da Polícia Federal, polícias civis e estaduais, Ministério Público federal e estadual, além das operadoras que são meio para a produção dessas informações.

Então, finalizando esse pedaço, nós temos a existência de um arcabouço legal, que já endereça o atendimento de demandas judiciais, incluindo

dados de localização, por exemplo. Existe a padronização por parte do grupo de trabalho ativo, liderado pela Anatel, e esse grupo é à disposição para fazer melhorias, que essas informações sejam acessíveis para os órgãos competentes.

Agora, um outro ponto que já foi bastante salientado também é que nós vivemos uma era da transformação digital. Todos nós estamos inseridos nesse ambiente digital e isso vai piorar. Hoje, nós estamos totalmente conectados e dependentes do celular. E daqui a pouco, não só nós, as pessoas, mas também as coisas, os carros, o trânsito, quer dizer tudo, encaminha para um ambiente muito mais digital, inseridas aí questões de inteligência artificial. Nós temos a computação quântica a vir. Então, assim, nós temos um ambiente digital que nos favorece em muitas utilidades, mas, ao mesmo tempo, precisa ser resguardado do ponto de vista da segurança, senão nós teremos um risco associado ao uso dessa digitalização.

E a Anatel, como órgão regulador, tem um mandato claro para promover a segurança cibernética das redes e serviços de telecomunicações.

Nosso objetivo é garantir que esses riscos sejam gerenciados de forma eficaz, protegendo a integridade dos dados e a privacidade dos usuários, além de evitar a descontinuidade dos serviços.

As redes de telecomunicações são complexas. Se vocês olharem de perto, é difícil acreditar que isso funciona, porque é muito complexo. São diversas tecnologias fornecidas por diversos fabricantes e numerosas empresas

prestadoras de serviços. No Brasil, nós temos mais de 15 mil prestadores de serviços de telecomunicações, apesar de só lembrarmos de algumas nacionais.

E mesmo com a adoção rigorosa de padrões de segurança, por essas empresas, não é possível garantir que não existam vulnerabilidades. São sistemas digitalizados. Então, a gestão adequada das vulnerabilidades é crucial para a gestão eficaz dos riscos cibernéticos. Quando vulnerabilidades são identificadas na infraestrutura de rede de telecomunicações, elas devem ser reportadas, de maneira responsável, aos fabricantes, fornecedores e prestadores de serviços de telecomunicações para que sejam corrigidas, encerradas, que a gente não alimente essa vulnerabilidade.

Então, diante dessa necessidade, a Anatel estabeleceu regulamentação, existe todo um marco de obrigações para as operadoras quanto à segurança cibernética, elas têm que fazer investimentos massivos em segurança e proteção. E a gente vem aumentando progressivamente os esforços nessa seara de segurança.

No entanto, na contramão desses esforços está o desenvolvimento, fomento e utilização de tecnologias que, em linguagem simples, se sustentam a partir de vulnerabilidades. É uma diversidade de técnicas, são vários aplicativos, mas o comum a todas elas é a busca de informações não

autorizadas a partir de exploração de vulnerabilidades, são ataques. Então, isso é bastante importante de ser salientado.

Eu não vou citar a questão dos aplicativos, que já foram bem mencionados. Mas o modelo de negócio é comum: a venda de dados que são obtidos a partir de ataques e exploração de vulnerabilidade. E isso é uma preocupação da Agência, porque, mesmo que com uma prévia determinação judicial eventual, isso estaria se autorizando o uso de softwares que são comerciais, desenvolvidos por terceiros, de nações estrangeiras, e não são do acompanhamento, controle e conhecimento da Agência ou das prestadoras de telecomunicações no país.

Então a gente entende que, ao autorizar a utilização de softwares comerciais de terceiros, especialmente estrangeiros, incentivam-se a exploração de vulnerabilidades e a realização de ataques às redes de telefonia. Mesmo com ordem judicial, não é possível garantir que somente as ferramentas adquiridas explorem essas vulnerabilidades. Se a vulnerabilidade existe, ela pode ser explorada por um aplicativo ou por outro, por vários, sem controle. Então, o importante que a gente tem em mente é que, identificou uma vulnerabilidade, corrija-se. Aponte, corrija-se.

A gente até pensou num cenário aqui de que o Estado precisaria interagir com a operadora de telefonia para pedir que não estanque uma

vulnerabilidade, porque eu precisaria daquela informação para uma investigação, o que seria inaceitável do ponto de vista da segurança cibernética, bem como da proteção constitucional que é dada à privacidade dos usuários.

O uso de tais ferramentas estrangeiras e comerciais, na visão da agência, poderia ser substituído por uma ferramenta que seja compatível, regulamentada, nacional, produzida com igual qualidade no sentido de provimento de dados aos órgãos competentes, mas que não se alimente de vulnerabilidades, que seja produção de dados sem essa exploração de mercado de vulnerabilidades.

Nós entendemos que a Anatel está à disposição para os órgãos sobre essa avaliação e que, uma vez existente uma alternativa para os órgãos competentes, nós canalizemos os esforços na identificação e correção de eventuais vulnerabilidades, pois os softwares, mesmo que sejam proibidos no país, vão estar comerciais em outros países. Assim é importante que seja mantido um cuidado para que eventuais vulnerabilidades sejam estancadas.

Por fim, especificamente quanto às denúncias de utilização do FirstMile, a Anatel tomou conhecimento dessas denúncias pela mídia e imediatamente instaurou processos administrativos para apuração e para compreender o papel das operadoras. Existia uma dúvida se elas tinham conhecimento ou não do caso. Restou evidente que as prestadoras não tinham

conhecimento do monitoramento e de que as redes foram atacadas, ou seja, foram exploradas vulnerabilidades. Na época, apurou-se também que as operadoras já trabalhavam para a mitigação da vulnerabilidade mesmo sem conhecer que estavam sendo atacadas. No processo de gestão de riscos, você identifica uma vulnerabilidade, contrata a solução para fazer a correção. Isso estava em andamento no mesmo período, até que surgiu a notícia de que um dos serviços parou de funcionar.

Então, a agência hoje está trabalhando justamente identificando o parecer que a Polícia Federal nos encaminhou agora recentemente, o laudo, para que nós possamos trabalhar em eventuais vulnerabilidades que ainda existam. Foram aplicadas correções pelas operadoras, e nós estamos justamente nesse momento fazendo a avaliação da suficiência dessas medidas adotadas.

Então, por todo exposto, nós entendemos que existe toda uma regulamentação incidente sobre a questão da quebra de sigilo, já é operacional há mais de 10 anos, com padronizações feitas por um o grupo técnico. Esse grupo está à disposição para continuar melhorando os dados que são fornecidos, trazendo com mais tempestividade os dados, enfim, tudo é possível melhorar nesses procedimentos. E destacamos que a questão do risco cibernético presente e futuro precisa ser bastante considerada. Então, se possível, discutir a adoção de uma

tecnologia que atenda os órgãos públicos competentes de forma a não explorar vulnerabilidades, seria um caminho mais frutuoso para todo o Brasil.

Muito obrigado a todos, fico à disposição.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Gustavo Borges e passo agora a palavra ao Coronel Croce, que é chefe da Seção de Informação da 2ª Subchefia do Estado-Maior do Comando do Exército Brasileiro. O Coronel Croce, é bacharel em Ciências Militares, mestre em Operações Militares, mestre em Ciências Militares, tem MBA de Política, Estratégia e Gestão de Defesa na FGV, é especialista em Geointeligência, Inteligência de Segurança Pública e Direito Internacional de Conflitos Armados.

Em sua carreira, destaque-se que foi Chefe de Estado Maior da Artilharia Divisionária da 1ª Divisão de Exército; instrutor da Universidade Militar do Ministério da Defesa da Federação da Rússia. Atualmente, é Chefe da 2ª Sessão de Formação da 2ª Subchefia do Estado Maior do Exército

Coronel Croce tem a palavra, por gentileza.

O SENHOR JOÃO RICARDO DA CUNHA CROCE LOPES (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - EXÉRCITO) - Obrigado, Senhor Ministro.

Excelentíssimo Senhor Ministro do Supremo Tribunal Federal, Cristiano Zanin; excelentíssima Senhora Subprocuradora-Geral da República,

Doutora Elizeta Maria de Paiva Ramos; excelentíssimo Doutor Leonardo Magalhães, Defensor Público-Geral Federal; Doutora Caroline Lima, do STF; Doutor Lucas Salles, do STF; excelentíssimos Senhores e Senhoras integrantes do Poder Executivo, Legislativo e Judiciário; integrantes das funções essenciais da Justiça e da sociedade civil, bom dia.

O Comando do Exército Brasileiro agradece a oportunidade de estar presente nesta audiência pública. Como mencionado, sou o Coronel Croce, Chefe da Sessão de Formação da 2ª Subchefia do Estado Maior do Exército.

O Estado Maior do Exército é o órgão de direção geral do Exército Brasileiro, responsável pela elaboração de políticas e diretrizes para o emprego da força, mais precisamente as políticas e diretrizes relacionadas ao sistema de informações, comando e controle do Exército.

A inteligência militar, intrinsecamente ligada à defesa nacional, objetiva a obtenção, análise e disseminação de conhecimentos sobre fatos e situações de imediata ou potencial influência sobre o processo decisório, assessorando os comandos do Exército, da Marinha, da Aeronáutica, com o foco na identificação de ameaças na detecção de oportunidades e na redução de incertezas, a fim de contribuir para salvaguarda do Estado brasileiro, a integridade do território e a soberania nacional.

É uma atividade realizada com irrestrito respeito à legislação vigente, a partir do ordenamento jurídico estabelecido pela Lei nº 9.883, que instituiu o Sistema Brasileiro de Inteligência, do Decreto nº 8.793 e o do Decreto de 15 de dezembro de 2017, que orientam e regulamentam a atividade por meios da política e estratégia nacional de inteligência, passando pela política e estratégia de inteligência de defesa até a doutrina de inteligência que norteia as temáticas e direciona a execução da atividade.

A exemplo do que ocorre em outros países, cito Alemanha, Austrália, Canadá, Estados Unidos, França, Nova Zelândia, Reino Unido, dentre outros, a atividade está sujeita ao controle do Estado, exercida pelo Poder Legislativo, por meio da Comissão Mista de Controle da Atividade de Inteligência. Em todo o seu ciclo, desde a reunião de dados, análise de informações e produção do conhecimento. A inteligência militar é, portanto, uma atividade de Estado, normatizada por sólido arcabouço jurídico, que regulamenta e delimita os parâmetros para seu desenvolvimento em perfeito harmonia com a preservação dos direitos e garantias individuais e demais dispositivos da Constituição, da Lei de Acesso à Informação, da Lei Geral de Proteção de Dados, dos tratados, das convenções, dos acordos e ajustes internacionais em que a República Federativa do Brasil seja parte ou signatária.

No campo da defesa, a política e estratégia nacional de defesa buscam orientar os esforços de toda a sociedade brasileira no sentido de reunir capacidades e de definir as estratégias que deverão nortear suas ações, a fim de desenvolver as condições para garantir a soberania do país, sua integridade e a consecução dos objetivos nacionais.

A política nacional de defesa traz como um dos objetivos assegurar a capacidade de defesa para o cumprimento das missões constitucionais das Forças Armadas, que se traduz em dotá-las em capacidades necessárias para realizar a vigilância, o controle e a defesa do território, das águas jurisdicionais, do espaço aéreo brasileiros, levando-se em conta a necessidade de contínuo aperfeiçoamento de técnicas e da doutrina de emprego das forças, empregando-se tecnologias modernas e equipamentos eficientes, em quantidade compatível com a magnitude das atribuições cometidas.

Em complemento, a estratégia nacional de defesa estabelece as capacidades nacionais de defesa, destacando-se a de proteção, dissuasão, de pronta resposta, de coordenação e controle, e de gestão da informação. Ambos os documentos citados, a política e estratégia nacional de defesa, encontram, na inteligência militar, suporte para os planejamentos do nível político, estratégico, operacional e tático, e proporciona a transformação de dados em conhecimentos confiáveis oportunos, condição essencial para o emprego adequado de meios

militares. A inteligência militar é desenvolvida desde os tempos de paz, pois possibilita o acompanhamento da escalada das crises até a deflagração dos conflitos.

As capacidades militares abordadas nos documentos de defesa citados podem ser compreendidas como a aptidão requerida para cumprir um objetivo militar proposto, que só é obtido por meio de fatores interrelacionados e indissociáveis, tais como a doutrina, o adestramento contínuo e a disponibilidade de materiais tecnológicos.

A evolução da doutrina militar está ligada ao uso de equipamentos tecnológicos modernos, a serem empregados por profissionais qualificados. Isso demanda constante investimento na aquisição e desenvolvimento de novas ferramentas, treinamento contínuo e a participação nas operações militares que as Forças Armadas estão envolvidas diuturnamente.

Nesse sentido, a inteligência militar apresenta-se como uma capacidade crítica para a defesa nacional, visando a obtenção da superioridade de informações, refletindo no constante estado de prontidão que as Forças Armadas Brasileiras devem possuir.

Ainda nessa direção, quanto à obtenção dessa capacidade, as diretrizes do sistema de inteligência de defesa buscam obter, de forma integrada,

soluções que atendam às necessidades no campo da tecnologia da informação, das comunicações e expandir a capacidade de inteligência no espaço cibernético.

Além disso, não se pode olvidar que o Brasil possui importantes projetos estratégicos de defesa, que permitirão lançar o país à autonomia tecnológica. O desenvolvimento do setor espacial, o domínio da tecnologia nuclear embarcada em submarinos, a defesa cibernética, a técnica de construção e uso de mísseis e os sistemas de radares são exemplos de ativos altamente sensíveis, que necessitam de proteção permanente da inteligência militar contra quaisquer possibilidades de espionagem ou sabotagem.

Portanto, a utilização de ferramentas e dispositivos tecnológicos, objeto da presente ação, é um claro exemplo de materiais que contribuem para a geração dessa capacidade crítica.

Além da missão precípua das Forças Armadas de defesa externa, prevista na Constituição, a inteligência militar é uma capacidade que contribui com a defesa e segurança da sociedade brasileira em tempo de paz, sendo amplamente utilizada nas ações subsidiárias, na cooperação com o desenvolvimento nacional e a defesa civil e no apoio aos órgãos federais na repressão dos delitos de repercussão nacional e internacional em território brasileiro.

Recentemente, foi amplamente noticiado na mídia o uso de soluções tecnológicas empregadas pela inteligência militar para o resgate de aproximadamente 50 pessoas que estavam desaparecidas nas enchentes que atingiram o Estado do Rio Grande do Sul. A mesma solução também foi essencial na busca e resgate de vítimas da queda de uma aeronave militar no Estado de Roraima, durante as ações de apoio ao povo Yanomami.

Como ferramenta de comando e controle, essas soluções também são empregadas no monitoramento de comboios sensíveis, no transporte de armas, munições e explosivos, no acompanhamento dos militares que realizam fiscalizações e operações logísticas de apoio e ajuda humanitária, fiscalização de produtos controlados e operação de distribuição de águas aos atingidos pela seca na Região Nordeste.

A possibilidade de acompanhamento dos militares empregados isoladamente ou integrando pequenas frações mostra-se como uma ferramenta eficaz para a segurança dos recursos humanos da Força, evitando ou contrapondo-se a situações de sequestro, roubo de cargas, dentre outras situações de risco.

As ferramentas ora tratadas nessa audiência são utilizadas ainda em apoio às atividades de investigação da Polícia Judiciária Militar, com devida atualização judicial e supervisão do Ministério Público Militar, à luz da legislação

penal brasileira, que estabelece todos os ritos procedimentais para a investigação eficiente.

Neste ínterim, cabe ressaltar a evidente distinção entre a atividade de inteligência militar, voltada para a produção dos conhecimentos oportunos para assessorar um decisor na proteção de um ativo; e a atividade de investigação, que, sob o manto da legislação penal, objetiva elucidar fatos já ocorridos, com o intuito de instrumentalizar a persecução penal.

Em toda e qualquer situação, a atividade de inteligência militar segue rigorosos protocolos de controle e segurança, sob supervisão dos mais altos escalões da Força, e no que se refere aos limites da execução e do uso de técnicas e meios sigilosos, é desenvolvida com fiel observância aos direitos e garantias individuais, aos preceitos éticos que regem os interesses e a segurança do Estado, ressaltando-se mais uma vez o caráter estritamente legal da atividade.

Diante dos aspectos ressaltados, a inteligência militar apresenta-se como uma capacidade crítica, que permite à nação estar preparada para evoluir rapidamente da situação de paz ou de crise para uma situação de conflito armado.

O eventual uso de ferramentas tecnológicas para a atividade de inteligência militar é desenvolvido em total consonância com a legislação nacional e alinhado com as melhores práticas realizadas em outros países.

As diversas normas que regulam as atividades de inteligência no Brasil estabelecem os parâmetros para a atuação dos agentes de Estado, promovendo a harmonia entre o interesse público e os direitos e garantias individuais.

Ressalta-se, ainda, que toda a atividade se desenvolve de forma integrada, sistêmica e colaborativa com os demais integrantes do Sistema de Inteligência e de Defesa, com o intuito de ampliar a capacidade de gestão das informações e de interesse do Estado e da sociedade brasileira.

Por fim, cabe destacar que a vertente preventiva do Estado, preventiva de defesa do Estado brasileiro, reside na ação diplomática, como instrumento da solução de controvérsia. Porém, apenas a existência de uma estrutura militar de credibilidade é capaz de gerar dissuasão efetiva e, nesse sentido, cabe à inteligência militar proteger os bens tutelados à segurança e à defesa nacional, garantindo a soberania com a preservação da integridade territorial, do patrimônio e dos interesses nacionais.

Obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Coronel Croce pela exposição e convido agora para fazer uso da palavra o Tenente-Coronel Engenheiro André Luiz Corrêa, que é chefe da Subdivisão de Segurança Orgânica do Centro de Inteligência da Aeronáutica, do

Comando da Aeronáutica. O Tenente-Coronel Engenheiro André Luiz Corrêa é lotado no Centro de Inteligência da Aeronáutica, possui graduação em Engenharia Elétrica pela Universidade Federal de Uberlândia, MBA em Gestão de Projetos e Especialização em Gerenciamento de Projetos pela Fundação Getúlio Vargas e, atualmente, exerce a função de chefe da Subdivisão de Segurança Orgânica do Ciaer, tendo atuado anteriormente como chefe da Seção de Segurança das Comunicações e Subseção de Segurança Computacional desse mesmo órgão.

Tem a palavra o Tenente-Coronel Engenheiro André Luiz Corrêa, por gentileza.

O SENHOR ANDRÉ LUIZ CORRÊA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - AERONÁUTICA) - Excelentíssimo Senhor Ministro do STF Cristiano Zanin, excelentíssima Senhora Subprocuradora-Geral da República Doutora Elizeta Ramos, demais autoridades que integram a mesa e aqui presentes, Senhoras e Senhores, muito bom dia!

O objetivo da minha apresentação é demonstrar a necessidade do uso de ferramentas tecnológicas com vistas à segurança nacional.

Para isso, eu destaco aqui a missão do Comando da Aeronáutica, da Força Aérea Brasileira, que é manter a soberania do espaço aéreo e integrar o território nacional com vistas à defesa da pátria. Como atribuição subsidiária, as Forças Armadas e a Força Aérea possuem atividades definidas por lei relacionadas

ao desenvolvimento nacional, à defesa civil, ao combate a delitos transfronteiriços e ambientais.

Para que a Força Aérea exerça sua missão e essas atividades subsidiárias, ela necessita do apoio e do suporte da atividade de inteligência, com finalidade de produzir e proteger conhecimentos sensíveis à segurança nacional. Essa atividade é amparada por um vasto arcabouço legal e infraconstitucional, sempre dentro da legalidade.

Além disso, toda a atividade de inteligência é submetida ao controle e à fiscalização externa pelo Congresso Nacional, ou seja, pela Casa do Povo, com o objetivo principal de evitar abusos e desvios de finalidade da atividade de inteligência.

Destaco aqui, como já foi falado em outras apresentações, a diferença entre a atividade de inteligência, que busca assessorar na tomada de decisão e mitigar ameaças, ou seja, antecipação da investigação criminal, que busca a materialidade e a culpabilidade.

A investigação criminal, conforme já foi descrito aqui também, ela ocorre após o fato ocorrido, não é? Não é atividade fim da Força Aérea Brasileira. Na Força Aérea, a atividade de inteligência, ela busca a capacitação e a prontidão dos seus integrantes quanto ao uso das ferramentas tecnológicas de busca e proteção do conhecimento. O objetivo é sempre o preparo e proteção,

preparo e emprego do poder aeroespacial. Isso garante a antecipação e a preparação para uma situação de conflito ou beligerância. O objetivo da atividade de inteligência é evitarmos sermos surpreendidos, e o custo da falha da inteligência, a história comprova, sempre a sociedade acaba pagando um custo alto por essa falha.

E aqui destaco que acaba a atividade de inteligência e começa a investigação policial. Enquanto estamos numa situação de paz sem conflitos ou beligerância, fazemos o uso dual dessas ferramentas tecnológicas aqui discutidas, principalmente nas atribuições subsidiárias da Força Aérea Brasileira. Então aí está a ajuda humanitária, o combate ao narcotráfico e principalmente destaco a última aí que é a operação de busca e salvamento.

Na atribuição subsidiária particular da Força Aérea de busca e salvamento, a geolocalização de celulares em caso de vítimas de acidente desempenha papel fundamental. Destaco aqui um caso real que aconteceu em fevereiro deste ano, dia 19 de fevereiro. Uma aeronave se deslocava de Altamira para Marabá, e ela se acidentou, desapareceu. As equipes de busca foram acionadas, e a única informação que essas equipes de busca tinham era essa linha vermelha, que seria o plano de voo que o piloto declarou que faria. As buscas não tiveram sucesso, essa aeronave foi encontrada dois dias depois, eventualmente, por pescadores, os três ocupantes mortos, inclusive um servidor do Dnit estava a bordo.

E aqui a gente tem um caso de não utilização de geolocalização de celulares. Se essa geolocalização fosse utilizada, talvez o desfecho aqui dessa operação de busca e salvamento teria outro final.

As estatísticas mostradas nesses gráficos são do Cenipa e elas demonstram que estamos em meados de 2024 e o número de acidentes aéreos e de fatalidades tendem a repetir os números de 2023. Essa estatística aumenta em ano de eleições municipais, porque o tráfego de aeronaves de pequeno porte também aumenta. Então é importante destacar aqui que, na busca e salvamento, tempo é vida.

Um exemplo de geolocalização utilizada com sucesso de celulares, que foi destacada há pouco pelo Coronel Croce, foi a geolocalização de 49 pessoas na tragédia do Rio Grande do Sul. Ontem, foi comentado aqui qual seria o custo-benefício para a sociedade de ter um equipamento de geolocalização de celulares. E aí eu mudo a pergunta e passo a indagar: qual é o valor da vida de dezenas de pessoas salvas através de uma ferramenta de geolocalização?

Além das aplicações nas ações subsidiárias, a contrainteligência também se beneficia dessas ferramentas tecnológicas, na busca por identificar e neutralizar ações de busca por informações estratégicas pela inteligência diversa. Aqui está exemplificado o Centro de Lançamento de Alcântara, que é um dos principais pontos no mundo para lançamento de satélites, devido a sua localização

próxima à linha do Equador. E com ferramentas de contrainteligência, a gente consegue perceber, por exemplo, que toda vez que tem uma campanha de lançamento, o número de embarcações, ele praticamente triplica no entorno de Alcântara, e a maioria das embarcações de bandeira estrangeira. Pode ser coincidência? A inteligência não acredita muito em coincidências.

Além disso, foi citado aqui também ontem sobre irradiação eletromagnética por dispositivos eletrônicos, um fenômeno conhecido como *tempest*. Então computadores, cabos, telefones, eles emitem sinais de rádio que podem ser interceptados por esses sensores e essas mensagens, eu consigo reconstruir os dados. Pode ser usado para atividade ilícita, mas, na Força Aérea, também pode ser utilizado, e é o nosso foco, por exemplo, proteger um vetor de primeira linha como o Gripen. Todos os dados e informações do Gripen são configurados numa estação de trabalho, um computador, que emite radiação eletromagnética. Então, eu faço uma Gaiola de Faraday e uso esses sensores para verificar se há algum tipo de vazamento que pode comprometer a missão do Gripen, pode comprometer a própria aeronave e a vida do piloto.

Então, senhores, as ferramentas tecnológicas demonstram aqui que elas podem ter uso legítimo. O desvio de finalidade é veementemente... o Comando da Aeronáutica é veementemente contrário à utilização indevida por qualquer tipo de ferramenta que fira aí os direitos constitucionais do cidadão.

Qualquer desvio de finalidade na atividade de inteligência e contrainteligência, temos aí o Cecai para apurar os fatos, encaminhar ao Ministério Público competente e responsabilizar os infratores, conforme a Resolução nº 2, de 2003, do Congresso Nacional.

Concluo dizendo que é fundamental o constante aperfeiçoamento da legislação. Entretanto, a normativa atual é clara, ampla e garante a legalidade e a proteção dos direitos individuais no exercício da atividade de inteligência. É importante reconhecer e fortalecer a atuação da Cecai como órgão de controle externo. Isso vai favorecer a atividade de inteligência do país.

E por último, a fixação de barreiras, mesmo que provisórias, pode comprometer a eficácia da atividade de inteligência das Forças Armadas no sentido de produzir e proteger conhecimentos essenciais à soberania nacional, além de prejudicar missões de busca e salvamento e favorecer significativamente, enquanto estamos de mãos atadas, a atuação da inteligência adversa.

Muito obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Tenente-Coronel Engenheiro André Luiz Corrêa pela exposição e convido, para fazer uso da palavra, a Capitão de Mar e Guerra Patrícia da Silva Vieira, assessora-chefe da Assessoria de Justiça e Disciplina do Gabinete do Comandante da Marinha.

A Capitão de Mar e Guerra Patrícia Silva Vieira é bacharel em Direito e atualmente desempenha a função de assessora-chefe da Assessoria de Justiça e Disciplina do Gabinete do Comando da Marinha.

Vossa Senhoria tem a palavra, por gentileza.

A SENHORA PATRICIA DA SILVA VIEIRA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - MARINHA) - Excelentíssimo Senhor Ministro do Supremo Tribunal Federal, Cristiano Zanin; Excelentíssima Senhora Subprocuradora-Geral da República, Doutora Elizeta Maria de Paiva Ramos; Excelentíssimo Senhor Defensor Público Federal, Doutor Leonardo Magalhães; Excelentíssimos Senhores e Senhoras integrantes dos Poderes Executivo, Legislativo e Judiciário, bom dia.

Eu sou a Capitã de Mar e Guerra do quadro técnico Patrícia Vieira, da Marinha do Brasil e, em nome dessa Força Naval, nesta audiência pública, explanarei acerca de aspectos jurídicos relacionados ao objeto da ADPF 1.143.

Nesse mister, primeiramente, elucido que a Marinha do Brasil integra o Sistema Brasileiro de Inteligência, o Sisbin, criado pela Lei nº 9.883, de 1999, como órgão permanente, qualificado por dispor de atribuições relativas à segurança interna e à defesa externa, com o propósito de executar atividades de inteligência.

Nesse contexto, é fundamental destacar a diferença entre atividades de inteligência e atividades de investigação criminal, que são competências estatais distintas, disciplinadas por diplomas legais diversos.

Como é sabido, a atividade de investigação criminal se presta à busca de autoria e de materialidade de um fato delitivo, com caráter prévio e de natureza preparatória de um futuro processo penal. A atividade de investigação criminal é essencial no combate à criminalidade, ao crime organizado e atua com prévia autorização judicial para obtenção de dados pessoais de investigados.

Por outro lado, a atividade de inteligência se destina principalmente à produção de conhecimentos necessários ao assessoramento do processo decisório governamental e a salvaguarda de conhecimentos indispensáveis à segurança da sociedade e do Estado. A atividade de inteligência se reveste intrinsecamente de caráter sigiloso e de assessoramento do processo decisório estatal, indispensáveis no combate a ameaças e na preservação de segurança da sociedade e do Estado.

A atividade de inteligência sempre é exercida buscando instrumentalizar o decisor para identificação de riscos, oportunidades e ameaças, de forma a antecipar-se aos acontecimentos; enquanto a investigação normalmente se dá após a consumação de um crime e no intuito de determinar a autoria e a materialidade de um fato delituoso.

O caráter sigiloso e de assessoramento são características que distinguem a atividade de inteligência como instrumento do mais alto nível voltado à produção de conhecimento e de inteligência, oportunos e imprescindíveis à tomada de decisão pelo executivo, diante de fatos ou situações que possam resultar em ameaças ou riscos a interesses da sociedade e do Estado, bem como atinentes a oportunidades que ensejam ação governamental imediata, dentro e fora do território nacional, conforme dispõe o Decreto nº 8.793, de 2016, que institui a Política Nacional de Inteligência - PNI.

Em virtude das características intrínsecas da atividade de inteligência em suporte ao processo decisório das operações militares, as ferramentas tecnológicas de inteligência permitem o acompanhamento de militares desenvolvendo operações em áreas de elevada periculosidade e de alto risco a suas integridades físicas, o controle e o monitoramento da movimentação de cargas sensíveis, como mísseis, torpedos, material nuclear e munição, a localização de náufragos, o apoio às ações de resgate, a localização de pessoas desaparecidas em áreas de desastres naturais, selvas ou regiões inóspitas e o apoio às atividades de contrainteligência e segurança orgânica das organizações militares.

Há de se considerar também as possibilidades de emprego das referidas ferramentas em situação de conflito contra um agressor externo, em que atividade de inteligência militar procura se antecipar em relação às intenções do

inimigo e apoiar as operações militares de defesa e soberania nacional. Nesse panorama, tem-se que o uso da ferramenta de monitoramento já se encontra disciplinado na Constituição Federal, na Lei do Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais.

Com efeito, existe também um microssistema legal que normatiza essa matéria, como, por exemplo, a Constituição Federal, em seu art. 5º, X e XII; a Lei nº 9.296, de 1996, que dispõe sobre a interceptação de comunicações telefônicas para a prova em investigação criminal e instrução processual penal; a Lei nº 12.965, de 2014, Lei do Marco Civil da Internet; Lei nº 13.709, de 2018, Lei Geral de Proteção de Dados Pessoais; Lei nº 12.527, de 2011, Lei de Acesso à Informação.

No outro passo, no que diz respeito à atividade inteligência propriamente dita, também há um arcabouço legal que normatiza, a saber: Lei nº 9.883, de 1999, que institui o Sistema Brasileiro de Inteligência; o Decreto nº 11.693, de 2023, que dispõe sobre a Organização e o Funcionamento do Sistema Brasileiro de Inteligência; Decreto nº 8.793, de 2016, que institui a Política Nacional de Inteligência - PNI, com o objetivo de definir os parâmetros e os limites de atuação da atividade inteligência e de seus executores no âmbito do Sistema Brasileiro de Inteligência; o Decreto nº 15, de dezembro de 2017, que institui a Estratégia Nacional de Inteligência; Resolução nº 2, de 2013, do Congresso Nacional, que

institui a Comissão Mista de Controle de Atividades de Inteligência - CCAI, que fiscaliza e exerce o controle externo das atividades de inteligência e contrainteligência; O Código Penal, em especial os seus arts. 154, 154-A e 154-B, que impõem pena de reclusão aos crimes de violação de segredo profissional e invasão de dispositivo informático; Código Civil, em especial seus arts. 186 e 927, que estabelecem a obrigação de reparar os danos decorrentes de ato ilícito, inclusive do agente público, independentemente de culpa.

Dessa maneira, a atividade de inteligência não é exercida de forma aleatória, tampouco de forma arbitrária, uma vez que se encontra submetida a um conjunto de leis e decretos. Atualmente, a atividade de inteligência é uma das atribuições do Estado mais regulamentadas e se encontra sob o escrutínio meticuloso da Comissão Mista de Controle da Atividade de Inteligência do Congresso Nacional, a CCAI, bem como sob a fiscalização da Câmara de Relações Exteriores e Defesa Nacional do Conselho do Governo, a Creden, nos termos do Decreto nº 9.819/2019.

A CCAI foi instituída justamente com o propósito de fiscalizar e exercer o controle externo das atividades de inteligência e contrainteligência, zelando para que tais atividades sejam realizadas em conformidade com a Constituição Federal e com as normas constantes do ordenamento jurídico nacional, em defesa dos direitos e garantias individuais, do Estado e da sociedade.

Dessa forma, entendemos, com todo o respeito, que já existe todo um microssistema legal composto pela própria Constituição Federal e mais doze normas infraconstitucionais que disciplinam a matéria e que têm o condão de fazer frente a um eventual emprego irregular de programas e ferramentas de monitoramento na atividade de inteligência; que a atividade de inteligência não é exercida de forma aleatória nem de forma arbitrária, pois se encontra subordinada a todo um arcabouço legal e à fiscalização e controle externo da Comissão Mista de Controle de Atividades de Inteligência do Congresso Nacional, a CCAI, bem como sob a fiscalização da Câmara de Relações Exteriores e Defesa Nacional do Conselho do Governo, a Creden, nos termos do Decreto nº 9.819/2019; que a Marinha do Brasil exerce atividade de inteligência de acordo com a legislação em vigor e com as diretrizes prescritas na política nacional de inteligência e na estratégia nacional de inteligência.

Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço a Capitã de Mar e Guerra Patrícia da Silva Vieira pela exposição e convido a Doutora Ana Bárbara Gomes, que é Diretora do Instituto de Referência em Internet e Sociedade.

A Doutora Ana Bárbara Gomes é mestre em política científica e tecnológica pela Unicamp e formada em Ciências Sociais pela Universidade Federal de Minas Gerais. Atua com temas de estudos de infraestrutura no campo dos estudos sociais da ciência e tecnologia, com diálogos sobre o desenvolvimento tecnológico, ética, desenho e aspectos políticos de tecnologia.

Doutora Ana Bárbara Gomes tem a palavra, por gentileza.

A SENHORA ANA BÁRBARA GOMES (INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS) - Muito obrigada. Bom dia a todos. Cumprimento a Mesa, na pessoa do Excelentíssimo Ministro Cristiano Zanin. Cumprimento os demais expositores e as demais senhoras e senhores presentes.

Em nome do IRIS, o Instituto de Referência em Internet e Sociedade, eu saúdo a audiência pública por pautar um tema tão sensível e importante e por dar a oportunidade de trazer as preocupações da sociedade civil. Acreditamos que este debate é primordial para a consolidação de uma sociedade digital segura e fortalecida em direitos.

Esse é um tema que tem sido pautado nas pesquisas realizadas pelo IRIS e a minha fala é, em muito, inspirada pelo relatório publicado pelos

autores Luiza Dutra, Paulo Rená, Victor Barbieri e Wilson Pereira. Todos os nossos trabalhos estão disponíveis de forma pública no *site* do instituto.

Apesar de os usos de ferramentas intrusivas serem relatados desde a década de 90, é mais recente a popularização e a problematização do debate. Pautar a legitimidade do uso de *softwares* espiões pelo Estado é uma oportunidade de reafirmar que não admitimos qualquer desenvolvimento tecnológico em detrimento da garantia de direitos humanos fundamentais.

Essas ferramentas devem ser vistas com a complexidade e risco que representam. Trata-se de armas digitais que permitem a sofisticação de formas de violação dos direitos humanos. Sua capacidade está muito além do que a nossa norma conhece - como, outrora, a interceptação telemática -, e são ameaças graves aos direitos da liberdade de expressão, à privacidade, à livre associação e outros.

O Brasil, por suas políticas de segurança pública, seu sistema de Justiça e propostas normativas em curso, parece ter um cenário particularmente grave em relação à gama de direitos humanos em risco por decorrência de uso de *softwares* espiões. Hoje em dia, um montante significativo de dinheiro público, na ordem de dezenas de milhões de reais, está investido em ferramentas espiãs, como demonstraram os estudos realizados pelo instituto de pesquisa do Recife, *o* Mercadores de Insegurança. E dentre os contratantes são vários, desde autoridades

de investigação, como o Ministério Público e Polícia Civil, mas também outras que não têm nenhuma relação com a pauta de segurança pública, como o Conselho Administrativo de Defesa Econômica, o Cade.

Esse cenário demonstra que o uso indiscriminado e sem previsão legal dessa ferramenta fortalece uma cultura investigativa que vai na contramão de maior proteção de direitos fundamentais e tem demonstrado a falta de observância ao devido processo legal.

Hoje em dia, não há hipótese prevista no ordenamento brasileiro que justifique a aplicação desse recurso. Ao contrário, a falta de previsão o torna proibido.

A isso se sobrepõe o fato de que, para além das conhecidas capacidades de intrusão e vigilância, esses serviços podem ter a capacidade de implantar informações e arquivos em dispositivos, o que nos leva a um outro cenário de desafios para apurar e assegurar a integridade das provas digitais e a garantia da sua cadeia de custódia.

Pesquisadores que apuraram os limites da autorregulação deste mercado demonstraram que, apesar da alegada devida diligência e cuidado para que a ferramenta não seja comercializada com violadores de direitos, a realidade é um cenário de abuso e de dano.

O seu uso contra dissidentes políticos, por exemplo, demonstra um caso extremo de desrespeito à liberdade de expressão e de outros valores democráticos. No cenário brasileiro, onde observamos uma sensível polarização, manifestada sobretudo nos ambientes digitais, isso é um risco. Afinal, não faz muito tempo que tivemos uma exposição de lista de pessoas envolvidas em ações denominadas antifascistas.

É preciso reconhecer que as normas do ordenamento jurídico brasileiro, que já apresentam os princípios pertinentes nesse contexto, quais sejam, a Constituição Federal, a Lei Geral de Proteção de Dados, a Lei de Interceptação Telefônica, já dão ao Ministério Público, portanto, subsídios para apontar a irregularidade dessas ferramentas.

Assim, o seu uso pautado na exploração de vulnerabilidade por parte do Estado, se revela ilegal e ainda inconstitucional, com a violação de uma série de direitos, como o direito ao sigilo. E no âmbito dos direitos humanos, há um risco generalizado de não se garantir o julgamento justo, a validade científica das provas digitais e a presunção de inocência.

Propostas de intervenções tecnológicas que impactem a persecução penal devem ser fundamentadas em pesquisa científica atualizada e multidisciplinar.

Programas de monitoramento secreto devem ser, se utilizados, específicos para atividades de inteligência sobre fatos e situações que ameacem a segurança da sociedade ou do Estado. Não se deve confundir, no entanto, operações de inteligência com as investigações de segurança pública; e iniciativas legislativas que vão no sentido de misturá-las devem ser negadas.

O Alto Comissariado das Nações Unidas Para Direitos Humanos já se manifestou pela necessidade de "moratória pela venda, transferência e uso de ferramentas de hackeamento até que um regime de salvaguardas, baseado em direitos humanos, esteja em vigência".

Advogados, sociedade civil, policiais, jornalistas, autoridades judiciais e autoridades do Estado têm sido espionados por entes públicos e privados em detrimento da garantia de seus direitos. Esses eventos, protagonizando grandes escândalos antidemocráticos, são um alerta para a sensibilidade e o risco de popularização desse método.

Esses casos evidenciam, ainda, o risco à nossa soberania nacional, uma vez que envolvem a permissão de acesso a informações externas extremamente sensíveis para programas de espionagens que são comercializados por empresas estrangeiras, sem que tenhamos o menor parâmetro e garantia sobre a segurança da informação praticada.

Para além disso, apura-se que o conhecido citado *software* Pegasus tenha sido usado para hackear 14 líderes mundiais. Em algum contexto isso poderia começar uma guerra cibernética.

Ainda uma preocupação econômica, estabelecer ferramentas de espionagem como mecanismo de investigação implica assumir uma alta onerosidade, visto que sempre será preciso uma atualização. Uma vez que a vulnerabilidade é corrigida, é preciso um novo esforço de descoberta e exploração de uma nova vulnerabilidade. Isso significa colocar o Estado num papel de incentivador econômico de um mercado baseado na fragilidade de sistemas, um mercado baseado na insegurança digital como um bem a ser explorado, um mercado que também não servirá só às autoridades investigativas, mas também a organizações criminosas, como tem sido denunciado pelo jornalismo ao redor do mundo.

O endosso aos métodos de espionagem também representa um significativo retrocesso no campo da segurança da informação e dos desenvolvimentos tecnológicos. Num contexto cada vez mais digitalizado, o zelo com a privacidade deve fazer parte da nossa formação e da de jovens e crianças. É preciso que a privacidade e proteção dos dados sejam populares. É preciso que ferramentas de proteção individual e coletiva sejam um mote, inclusive endossado pelo Estado.

Hoje temos um cenário de violação sistemática dos nossos direitos humanos com o uso dessas ferramentas de forma deliberada, sem previsão legal, sem transparência de sua aplicação e sem prestação de contas. Há de se zelar pelo respeito aos princípios da reserva legal, da finalidade, da proporcionalidade e da necessidade de ordem judicial. O uso de ferramentas pautadas na promoção de insegurança digital deve ser proibido.

Se decidirmos excetuá-lo para as atividades de inteligência, que em muito se difere do seu uso interno para a segurança pública, que seja regulamentado com a granularidade adequada, com condições e parâmetros restritivos e eficientes, ou, se for aceito no âmbito de investigações criminais, que seja restrito exclusivamente a crimes graves, onde condições seriam elementos que permitem o uso e os parâmetros seriam os elementos que avaliam se o uso foi devido.

Que o Supremo Tribunal Federal possa reafirmar os nossos direitos humanos no ambiente digital com uma leitura pautada na Constituição. E do Estado, em especial do Poder Judiciário, espera-se uma postura garantidora de direitos que não permita o uso abusivo de uma arma digital tão poderosa. E que essa possa ser a premissa adotada ao prosseguirmos com esse debate.

Muito obrigada.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Ana Bárbara Gomes e agora passo a palavra ao Doutor Daniel Limoeiro, que é fundador e diretor-executivo da Turivius Legal Intelligence. É PhD pelo MIT e mestre com distinção pela Oxford University. Autor do *Economic growth, inequality and crony capitalism*. Danilo também tem sete anos de experiência em cargos de liderança, assessoramento de órgãos federais como o Ministério da Fazenda e Presidência da República. Com a palavra, Doutor Danilo Limoeiro, por gentileza.

O SENHOR DANILO LIMOEIRO (TURIVIUS PORTAIS DE CONTEÚDO LTDA) - Bom dia, Excelentíssimo Ministro, Senhor Cristiano Zanin. Bom dia, Subprocuradora-Geral da República, Senhora Elizeta Maria de Paiva Ramos. Bom dia, Doutor Leonardo Magalhães, Defensor Público. Bom dia, Juízes de Instrução Doutora Caroline Lima e Doutor Lucas Salles.

Senhor Ministro, eu tive a oportunidade de fazer parte da minha formação em universidades estrangeiras, e meus estudos acadêmicos e atividades privadas abrangem os campos de relações internacionais, economia política e estatística avançada, que é a base da inteligência artificial. Em especial, durante a minha passagem pelo MIT, dediquei-me à pesquisa sobre a aplicação de inteligência artificial em fenômenos sociais. Mas hoje eu atuo na esfera privada, no setor de inteligência artificial, atualmente como diretor-executivo de uma empresa

chamada Turivius Legal Intelligence. Falo, portanto, não em nome de instituição específica, mas sim como acadêmico e agora agente privado atuando no ramo da intersecção entre tecnologia e questões de governo e Estado.

Senhor Ministro, muito já foi discutido aqui e apropriadamente apresentado a respeito do equilíbrio entre garantias individuais, de um lado, e a necessidade de combate ao crime e de segurança nacional, de outro lado. Portanto, eu vou focar o ponto da minha exposição em três questões principais relacionadas a consequências de segunda e terceira ordem do desenvolvimento e uso desse tipo de tecnologia. Primeiro, eu vou trazer para esse debate algumas conclusões vindas de um debate análogo que acontece na esfera da geopolítica e diz respeito ao advento de armas e ações cibernéticas e suas consequências. Em segundo lugar, eu vou falar sobre as interações dessas ferramentas intrusivas com tecnologias poderosas como a inteligência artificial. E, por fim, eu farei um breve ponto sobre como o uso despropositado desse tipo de ferramenta pode deteriorar o estoque do que os cientistas políticos chamam de capital social do país, tendo efeitos deletérios na promoção de ambiente de negócios saudável, algo caro para mim, como agente privado, e para todos os outros agentes privados também.

Inicio o meu primeiro ponto e nele pretendo jogar luz sobre o tema discutido aqui na ADPF, trazendo elementos de um debate correlato, o qual se refere às armas cibernéticas e à nova lógica da segurança internacional.

E, aqui, vale a pena recorremos a reflexões estrategistas do americano Henry Kissinger, em seu recente livro *A Era da Inteligência Artificial.*

Kissinger discute como a estratégia armamentista mudou com o surgimento de armas cibernéticas. Enquanto as armas nucleares dependiam da dissuasão através do anúncio explícito da sua existência, as armas cibernéticas têm como elemento central da sua utilidade a opacidade. A abertura da existência de capacidade cibernéticas pode deteriorar a sua utilidade. A eficácia dessas armas depende de não revelar a sua existência ou suas capacidades completas. Nenhum agente, seja ator cibernético governamental, ou não governamental, revelou todo o escopo das suas capacidades. E mesmo ações cibernéticas de grande porte, como o ataque de um *software* chamado Stuxnet, que visava danificar centrífugas de enriquecimento de urânio no Irã, têm origem incerta, embora acredite-se terem sido arquitetadas por Estados Unidos e Israel.

Ou seja, enquanto, no passado, ostentar grandes arsenais nucleares era necessário, pois tinha como efeito a dissuasão; atualmente, na guerra cibernética, a opacidade é o elemento necessário nesse tipo de ação agressiva.

Soma-se agora à opacidade intrínseca a digitalização crescente da vida moderna, o que aumenta a vulnerabilidade a ataques cibernéticos.

Nesse ponto, já colocado aqui nessa audiência pública, e trago novamente Kissinger, à medida que as economias integram sistemas de comando

e controle digital em usinas de energia, redes elétricas, e transferem seus programas governamentais para grandes servidores em nuvem e dados de registros eletrônicos, sua vulnerabilidade a ataques cibernéticos se multiplica. O aumento da digitalização, portanto, significa um conjunto muito mais rico de alvos, de modo que um ataque bem-sucedido poderia ser substancialmente mais devastador.

O primeiro ponto de reflexão trazido por Kissinger para o nosso debate é como as ações cibernéticas dizem respeito à sua opacidade essencial, e o segundo ao aumento da superfície de ataque dessas armas cibernéticas, devido à crescente digitalização de funções sociais relevantes. Ou seja, Senhoras e Senhores, na esfera internacional, a estratégia e defesa continuam a evoluir nas sombras da incerteza, enquanto a capacidade tecnológica cresce em velocidade exponencial.

E aqui, Senhor Ministro, temos a conexão entre geopolítica cibernética e regulação das mencionadas ferramentas de intrusão e monitoramento. Ambas atuam explorando vulnerabilidades em sistemas digitais e ambas têm a opacidade como seu ponto central. A realidade digital é crescente, tanto na vida social quanto na privada; e, preocupantemente, a capacidade desse tipo de ferramentas só sobrevive se atuar nas sombras, na opacidade. Assim, à medida que seus alvos crescem, a transparência no seu uso decresce.

O ponto central aqui é que há uma provável capacidade de transferência tecnológica entre armas cibernéticas e sistemas intrusivos. E não é à

toa que um determinado país é conhecido não só pelas ferramentas comerciais, mas também pelas ferramentas de agressão cibernética. Quanto mais intensa for a guerra cibernética - e estrategicamente não é revelada -, mais efetivo serão seus arsenais. E essa capacidade possivelmente pode ser transferida para sistemas de intrusão e monitoramento secreto, pois o objetivo de ambos, novamente, é explorar vulnerabilidades digitais.

E agora, Senhor Ministro, avanço para o meu segundo ponto, o qual diz respeito a entender os desdobramentos do encontro entre tecnologia de monitoramento e intrusão e inteligência artificial. Aqui, podemos ter um grande risco e potencial de disrupção.

Resumidamente, a IA funciona da seguinte forma: o seu programador lhe dá um objetivo e uma quantidade gigantesca de dados. A IA entende esse objetivo, consome os dados e, a partir de um algoritmo matemático, tenta alcançar esse objetivo de forma reiterada, tentando alternativas diferentes e minimizando a chamada *loss function,* ou os erros que comete no caminho, de modo a, obstinadamente, alcançar o seu objetivo. A partir desse processo, a IA encontra padrões, estratégias e possibilidades que são imperceptíveis pelo ser humano.

Essa nova tecnologia, que fique claro, é extremamente promissora e benéfica em vários campos da atividade humana.

Entretanto, no conflito cibernético e monitoramento secreto, essas ferramentas podem utilizar vastas quantidades de dados para aprender a penetrar defesas e explorar vulnerabilidades sem depender da descoberta humana de falhas de segurança em *software*. E a conclusão aqui é: ao adotar alguma IA, quanto mais essas ferramentas captarem dados de vulnerabilidade e utilizar esses dados para explorar brechas em sistemas digitais, mais poderosas elas se transformarão. E aqui meu ponto de vista é bem semelhante ao que foi alertado ontem pelo Doutor Renato Opice Blum. Dessa forma, o avanço da inteligência artificial tem potencial de transformar radicalmente as tecnologias de monitoramento. Kissinger nos convida a imaginar uma versão do Stuxnet, que é uma ferramenta de 2010/2012 e é uma arma digital capaz de causar danos físicos, impulsionada por um IA.

Resumindo, os três elementos comuns entre ações cibernéticas e ferramentas intrusivas de monitoramento são: I) seu objetivo comum, explorar a vulnerabilidade de sistemas digitais, o que proporciona transferências de capacidade tecnológica entre um e outro; II) suas crescentes áreas de atuação com a progressiva digitalização da realidade social e individual, bem como a sua característica essencial de opacidade; e III) à medida que essas ferramentas incorporam tecnologias de IA, sua capacidade de explorar vulnerabilidades de forma indetectável se ampliará quase que exponencialmente.

Esses riscos, Senhor Ministro, levam-me ao terceiro e último ponto: o impacto do uso indiscriminado e não regulado dessas tecnologias no que os cientistas políticos chamam de capital social.

Como foi falado pelos expositores no dia de ontem, dentre os quais está a fala da Doutora Bárbara Simão, o tecnovigilantismo estatal deteriora a confiança no Estado democrático de direito. E isso tem consequências para além da esfera de garantias civis.

O chamado capital social, que, segundo o cientista político norte-americano Robert Putnam, são redes sociais baseadas em confiança e reciprocidade, estão associadas ao desenvolvimento econômico e democrático das nações. Ou seja, a confiança interpessoal e a confiança nas instituições são componentes importantes do capital social. E a literatura científica mostra uma relação direta entre capital social, escolhas empreendedoras e atividade econômica, mais uma vez, um tema caro para o setor privado.

Por exemplo, em um estudo de 2022 intitulado *Entrepreneurial Choices Depend on Trust* (escolhas empreendedoras dependem de confiança), mostra que mudanças na confiança interpessoal e confiança nas instituições afetam a atividade empreendedora ao longo do tempo. Quanto mais confiança, maior a atividade empreendedora. O aumento de qualquer tipo de confiança leva a mais

atividade, enquanto a diminuição da confiança resulta em menor atividade e piora sua qualidade.

Portanto, a espionagem estatal pode deteriorar a confiança nas instituições, resultando em um declínio democrático e do desempenho econômico. A confiança é essencial para o ambiente de negócio saudável e para o desenvolvimento de atividades empreendedoras de alto valor agregado.

Portanto, para proteger e promover o capital social é necessário regulamentação das tecnologias de monitoramento. Isso não só protegerá a privacidade dos cidadãos, mas também manterá a confiança nas instituições e promoverá um ambiente econômico saudável e democrático.

E aqui concluo, Senhor Ministro, enfatizando os três pontos que eu quis trazer ao debate.

Primeiro, analogamente a armas cibernéticas, as tecnologias de monitoramento têm o seu campo de atuação crescente, com o aumento da digitalização da realidade social individual, além de serem intrinsecamente opacas.

Segundo, o uso dessas ferramentas combinado a tecnologias poderosas, como a inteligência artificial, pode aumentar de forma imprevisível sua capacidade de explorar vulnerabilidades em sistemas digitais.

E por fim, o uso indiscriminado dessas ferramentas corrói não apenas garantias fundamentais, mas também o estoque de capital social do país ao reduzir a confiança nas instituições, podendo ter efeitos deletérios na promoção de ambiente econômico saudável e pujante.

E aqui eu encerro, agradeço a oportunidade e fico à disposição para perguntas.

Muito obrigado pela atenção.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Doutor Danilo Limoeiro, pela exposição.

E agora vamos para a última exposição deste bloco, que é da Doutora Nádia Zilotti, diretora de inteligência da Polícia Rodoviária Federal, e falará de forma virtual.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Estamos ouvindo, Doutora Nadia. Vossa Senhoria tem a palavra, por gentileza.

A SENHOR NADIA ZILOTTI ALENCAR (POLÍCIA RODOVIÁRIA FEDERAL) - Obrigada! Excelentíssimo Senhor Ministro Cristiano Zanin, em seu nome, cumprimento as demais autoridades, os expositores e os ouvintes deste evento.

Inicialmente, destacamos a irrefutável importância da discussão trazida nesta audiência pública, na qual tratamos intensamente da regulamentação, por órgãos e agentes públicos, de programas de intrusão virtual, de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal, visando a subsidiar a análise da Arguição de Descumprimento de Preceito Fundamental - ADPF 1.143.

Contextualizando, a Polícia Rodoviária Federal é uma instituição cujas atribuições são voltadas para o patrulhamento ostensivo das rodovias federais, visando a garantir a segurança e a fluidez do trânsito, além do enfrentamento qualificado às organizações criminosas.

Apenas no ano de 2023 foram apreendidas mais de 700 toneladas de drogas, 63 milhões de massas de cigarro, e mais de 2 mil veículos furtados ou roubados foram recuperados pela PRF.

Nossa atuação vem-se notabilizando no enfrentamento à criminalidade, sobretudo mediante a implementação de estratégia de Policiamento Orientado pela Inteligência, conhecido como POI.

O POI se caracteriza pela orientação das intervenções policiais a partir da geração de conhecimento advindo da inteligência de segurança pública.

Essa metodologia confere maior eficiência e eficácia às operações de repressão ao crime, como evidenciado por seus resultados ao longo

dos últimos anos. Ademais, possibilita a condução de abordagens de maneira objetiva, embasadas em análises de risco criteriosas.

Cumpre ressaltar que a inteligência da PRF depende de uma variedade de ferramentas e técnicas para coletar, analisar e utilizar informações relevantes na prevenção e na repressão do crime, que inclui a coleta de informações, análises de dados, identificação de vulnerabilidades, ferramentas de inteligência de fontes abertas, inteligência de fontes humanas e inteligência geoespacial, entre outras - neste momento, faço aspas, para informar que a PRF não adquiriu quaisquer das ferramentas tratadas nesta audiência pública.

Atualmente, a inteligência de segurança pública tem sua atuação otimizada pelas ferramentas tecnológicas e cibernéticas. Essas desempenham papel fundamental no desmantelamento e enfraquecimento das organizações criminosas, auxiliando as autoridades a entenderem melhor seus alvos, planejar estratégias eficazes e tomar medidas decisivas para proteger a sociedade contra o crime.

No tocante à inteligência de segurança pública, entendemos ser necessário um olhar particular, buscando maior entendimento sobre a forma de atuação e as suas capacidades.

Entendemos que as ferramentas disponíveis devem ser utilizadas sob a égide do controle externo sobre as atividades de inteligência, nesse caso, especificamente a CCAI, sendo esse controle fundamental para a garantia dos

direitos civis, a prevenção de abusos de poder, a legitimidade democrática, a prevenção de erros e ineficiências, bem como da proteção da democracia.

Assim, entendemos ser crucial a regulamentação pela Anatel do uso de programas de intrusão virtual remota e de ferramentas de monitoramento de aparelhos digitais de comunicação pessoal, para definição de limites e procedimentos, proteção dos direitos individuais, transparência e prestação de contas, além da prevenção de abusos e violações.

Por fim, entendemos que essa regulamentação é imprescindível, porém clamamos por um olhar atento para as atividades de inteligência, especificamente inteligência de segurança pública, resguardando a sua atuação, visto ser uma ferramenta indispensável à segurança do Estado brasileiro.

Muito obrigada! Permanecemos à disposição para questionamentos.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Nadia Zilotti pela exposição.

PERGUNTAS AOS EXPOSIDORES

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agora, passaremos à fase das perguntas. Na verdade, eu começaria com uma pergunta, poderia ser tanto para o Coronel Croce quanto para o Tenente-Coronel

Engenheiro André Luiz Corrêa ou para a Capitã de Mar e Guerra, Patrícia da Silva Vieira.

Aqui, claramente, temos um tensionamento entre preceitos fundamentais, notadamente as garantias descritas na petição inicial, sobretudo a intimidade, e a eventual necessidade do Estado de fazer uso de equipamentos que possam viabilizar atividades de inteligência e contrainteligência, dentre outras coisas. Minha dúvida é se, para essas atividades de inteligência e contrainteligência, é indispensável ou imprescindível o uso de ferramentas de intrusão ou uso de ferramentas ultrainvasivas como o *Pegasus*. Em caso positivo, como são escolhidos os alvos e qual a destinação final do material coletado?

O SENHOR JOÃO RICARDO DA CUNHA CROCE LOPES (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - EXÉRCITO) - Obrigado pela pergunta, Senhor Ministro! Começando aqui pelo Exército.

A utilização de *software* altamente invasivo, no nosso caso, Exército, não é o caso. Quando falamos que "acompanhamos o militar" - acompanhamento de comboios, de pessoal em operações na fronteira etc. -, ele recebe um celular funcional. Já há, então, essa distinção.

Em termos de operações militares, em que a inteligência militar funcionará, existe um protocolo rigoroso, desde a solicitação ao emprego. A auditoria desses dados, autorizada pelo mais alto nível do Exército brasileiro, para

emprego de alguma ferramenta tecnológica mais invasiva, no caso de operação militar, ao término da operação, a partir da auditoria de todos os dados, esses dados são deletados, *erase* - corta-se, apaga-se, até pela segurança do sistema, pela contrainteligência, pela segurança cibernética dos nossos sistemas.

Respondendo objetivamente, não vejo caso de *software* altamente intrusivo na intimidade da pessoa e assim por diante. Acompanhamos, mas temos nossos próprios celulares funcionais, para não haver problema com o celular do militar.

Obrigado!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Coronel Croce.

O SENHOR ANDRÉ LUIZ CORRÊA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - AERONÁUTICA) - Complementando as palavras do Coronel Croce, em relação à Aeronáutica, não temos e nunca utilizamos o sistema *Pegasus*.

Nossa visão como contrainteligência é conhecer essas ferramentas para que nós possamos proteger em relação a elas. Como eu, como órgão de contrainteligência, garantirei a segurança da autoridade, do meu comandante, se não conheço essa ferramenta? Acho válido a título de preparação e capacitação, como coloquei em minha apresentação, mas não temos aplicação e não

tenho conhecimento da aplicação disso, em nenhum momento, na Força Aérea Brasileira.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Tenente-Coronel e Engenheiro André Luiz Corrêa.

A SENHORA PATRÍCIA DA SILVA VIEIRA (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - MARINHA) - Obrigada pela pergunta! Em complementação, gostaria de deixar claro que as atividades da Marinha são realizadas de forma compartimentada, aqui estou representando o aspecto jurídico aplicado na Força. Não tenho conhecimento técnico sobre a aplicação das ferramentas ou não, porém gostaria de destacar que a Marinha, em suas atividades, em qualquer tipo de atividade, observa as normas legais, ou seja, o princípio da legalidade e o princípio do controle, tanto os controles efetuados em âmbito interno quanto em âmbito externo, disciplinados pela Cecae, pela Credem, pelo TCU e pela CGU.

Muito obrigada!

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço, Capitão do Mar e Guerra Patrícia Silva Vieira!

Aproveito para fazer ao Doutor Rodrigo Moraes uma pergunta similar: se, para as atividades de persecução criminal, especialmente aquelas realizadas pela Polícia Federal, é imprescindível, na visão de Vossa Excelência, o

uso de ferramentas ultrainvasivas como o *Pegasus*. Em caso positivo, se esse uso é sempre precedido de autorização judicial e como se dá a destinação final do material coletado.

O SENHOR RODRIGO MORAIS FERNANDES (POLÍCIA FEDERAL) - Obrigado pela pergunta, Ministro.

Na verdade, entendo que a funcionalidade do *Pegasus* é imprescindível sim para fins de segurança pública. Posso citar várias situações casuísticas de emprego de uma ferramenta como essa que seriam fundamentais para a identificação de organizações criminosas, para atuar enquanto polícia judiciária.

Não usamos a ferramenta, não temos a ferramenta. Há alguns anos, tentamos, prospectamos, ferramentas nesse sentido e não conseguimos identificar como o *Pegasus* funcionava.

Hoje, em razão de uma investigação que temos ainda em curso, mas que já veio a público, sabemos exatamente como funciona: da forma como foi explicado aqui, por meio de acesso a vulnerabilidades em nossa rede, em nossa infraestrutura.

Porém, Ministro, para fins de investigação criminal, termos acesso a ferramentas que viabilizam esse tipo de intrusão durante as investigações, obviamente, com autorização judicial prévia, enfim, nos casos em que a lei permitir,

seria um avanço em termos de segurança pública para o país, inclusive em termos de segurança para as nossas ações.

Por exemplo, são corriqueiros os cumprimentos de mandados nas vilas no Rio de Janeiro. O uso de ferramentas nesse sentido nos poderia possibilitar uma entrada mais cirúrgica, evitando ações colaterais que vitimizam, por vezes, pessoas da população, moradores locais, e outras tantas funcionalidades.

Lembro-me que, quando essa operação da Polícia Federal veio à torna, recebi um telefonema de um delegado da polícia civil de um estado grande do país questionando, indagando-me, dizendo, na verdade, que ele cuida de casos sensíveis de sequestro e que faz uso dessa ferramenta de geolocalização. Essa ferramenta é primordial para o trabalho dele; é essencial, na verdade. Ela é imprescindível. Sem o uso dessa ferramenta, ficaria praticamente impossível identificar os autores e alcançar a vítima, enfim, tirá-la do cárcere.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Que é o FirstMile, por exemplo.

O SENHOR RODRIGO MORAIS FERNANDES (POLÍCIA FEDERAL) - No caso, o FirstMile.

Então, sim, a resposta é sim, Ministro, é fundamental, é imprescindível, eu diria.

No entanto, a gente tem tomado cuidado, temos tido tratativas com a Anatel, no sentido de buscar regulamentar isso. O que propomos é que as companhias telefônicas trabalhem no sentido de coibir essas vulnerabilidades, de evitar e conhecê-las. Já compartilhamos o nosso laudo pericial, e elas já estão, acredito eu, adotando medidas no sentido de fechar essas portas, no sentido de evitar que o esse acesso a essas vulnerabilidades aconteça. No entanto, precisamos do apoio deles, e a própria lei prevê isso. A autoridade policial pode requisitar o apoio das companhias telefônicas para a utilização de técnicas de quebra de sigilo telefônico ou telemático. O que temos buscado junto à Anatel e junto às companhias telefônicas é viabilizar meios técnicos para que possamos fazer.

Com a auditoria, a exemplo do que fazemos com as interceptações telefônicas, todas os mandados judiciais são encaminhados para a operadora. Ela faz o desvio para a Polícia e buscamos ali as informações necessárias. Aquilo vai para os autos e o que não interessa à prova é destruído com autorização judicial, com acompanhamento do Ministério Público, enfim, seguindo o rito da lei. Entendemos que o papel das companhias telefônicas nesse processo nos dá garantia e viabiliza essa auditoria.

Só para complementar, Ministro, entendo também que, uma vez tendo as companhias telefônicas como provedora desse tipo de técnica, acredito que desestimulamos muito a comercialização desses produtos em território

brasileiro. Isso já seria um avanço significativo nesse sentido. Hoje, infelizmente, embora os meios técnicos existam, não temos acesso às redes de telefonia. É o que temos buscado com a Anatel e com as próprias companhias.

O SENHOR MINISTRO CRISTIANO ZANIN - Agradeço ao Doutor Rodrigo Moraes.

Pergunto ao Doutor Gustavo Borges, que representa aqui a Anatel. Neste processo, há notícia de que, em 2021, houve a aquisição do equipamento *Pegasus* no plano Federal. Pergunto a Vossa Senhoria, se a Anatel teve conhecimento dessa aquisição e se, em algum momento, foi procurada para viabilizar o uso desse equipamento, o *Pegasus*, que teria sido adquirido em 2021?

O SENHOR GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES - ANATEL) - Obrigado pela pergunta, Excelentíssimo Ministro! Não, não tenho informação de a Anatel ter sido consultada a respeito da contratação citada.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço a Vossa Senhoria!

Indago à Doutora Elizeta se teria alguma questão a formular aos nossos expositores.

A SENHORA ELIZETA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Tenho algumas perguntas, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN(RELATOR) - Pois não, Doutora Elizeta. Tem a palavra.

A SENHORA ELIZETA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Obrigada! A primeira pergunta vai para o Doutor Victor Cravo. Segundo a apresentação, falou-se que a única forma de se fazer interceptações no Brasil seria por meio de plataformas mantidas pelas empresas concessionárias do serviço de telecomunicações.

Todavia o art. 4º da Lei de Interpretações diz que a autoridade de investigação, ao fazer os pedidos, realizará a indicação dos meios a serem empregados. Da mesma forma, o art. 5º da mesma Lei diz que o juiz indicará a forma de execução da diligência. O art. 7º diz que os órgãos de investigação poder-se-ão valer dos serviços das concessionárias sem haver essa obrigatoriedade.

Gostaria de ouvir as considerações de Vossa Senhoria sobre esses pontos.

O SENHOR VICTOR EPITÁCIO CRAVO TEXEIRA (MINISTÉRIO DA JUSTIÇA E DA SEGURANÇA PÚBLICA) - Como já explanado

por mim e pelo colega Gustavo Borges, a lei é de 1996 e houve um longo caminho até a institucionalização do Sittel.

De início, conversando anteriormente sobre esse tema - inclusive, na época, eu estava como Procurador-Geral da Anatel -, havia uma grande confusão sobre como se cumpririam os mandados de interceptações. Antes mesmo de 1996, eles já existiam. Muitas vezes, a autoridade policial tinha que subir em cima do poste para fazer lá uma espécie de grampo.

Isso foi evoluindo de forma a haver uma progressiva centralização até chegar ao que temos hoje, que é o Sittel, plataforma por meio da qual há o encaminhamento desses pedidos da forma como o juiz especifica, com todos os limites etc., inspirado, como já foi feito pelo Gustavo Borges, no sistema do Banco Central. Foi um longo caminho para isso.

A lei fala que poderá pedir o apoio das companhias de telecomunicações, mas, na verdade, esse é hoje o caminho principal. É mais ou menos dessa forma. Se o colega Gustavo Borges quiser complementar.

A SENHORA ELIZETA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Há a sua perguntinha também. Doutor Rodrigo Moraes, gostaria que Vossa Senhoria explicasse melhor como ocorreria essa parceria entre Polícia Federal e concessionárias de telefonia para implementação de *spywares?* A dúvida decorre da possibilidade desses *spywares*

poderem atuar, em tese, sobre serviços que estão fora da atuação das concessionárias, como, por exemplo, sistemas operacionais de aparelhos remotos.

O SENHOR RODRIGO MORAES FERNANDES (POLÍCIA FEDERAL) - Excelência, na verdade, estamos buscando essa parceria. A Polícia Federal, em trabalho de cooperação com outras polícias, entendemos que a tecnologia existe - inclusive, na Europa, já identificaram e disponibilizaram sistemas capazes de realizar esse tipo de intrusão. Nós não temos acesso à rede de telefonia.

Na nossa avaliação, melhor seria que a própria companhia telefônica desenvolvesse esse recurso que, no meu entender, tecnicamente, não é tão difícil de ser de elaborado e construído, desenvolvido. Esse controle, essa auditoria, seria por meio das próprias operadoras, a exemplo do que fazemos hoje com as interceptações telefônicas. Simplesmente encaminharíamos os ofícios, as autorizações judiciais, e todo o controle, a auditoria e a autenticidade dos dados enviados ficariam sob a tutela e a guarda das próprias companhias.

Não sei se respondi à pergunta.

O SENHOR VICTOR EPITÁCIO CRAVO TEIXEIRA (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA) - Posso complementar?

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Pode.

O SENHOR VICTOR EPITÁCIO CRAVO TEIXEIRA (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA) - De fato, os aplicativos de telefonia celular não são caracterizados como telecomunicações, mas é importante notar, conforme demonstrei naquele *slide*, que os aparelhos de celular estão em constante comunicação com as Estações Rádio Base - ERB. Dessa forma, estando em constante comunicação, há uma interação entre o sistema operacional do celular e as redes de telecomunicações.

É evidente que tem que haver uma interação com as companhias que produzem e instalam esses sistemas operacionais nos aparelhos, mas é importante lembrar que, sem as redes de telecomunicações, também não há, digamos assim, a intrusão dos celulares, seja ela ilícita, como a gente já colocou, seja ela lícita, que é a que queremos construir com essa parceria entre a Anatel e os organismos legitimados para atuar nos casos.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) – Doutor Gustavo Borges, o Sittel, desenvolvido pelo MPF e pela Anatel, envolve a transmissão de ordens judiciais de afastamento de sigilo telefônico às concessionárias e o recebimento

padronizado dos seguintes dados: registro de ligação, dados cadastrais dos usuários, localização da RB sensibilizada. Esse sistema não foi concebido para a interceptação de dados telefônicos e telemáticos.

Como a Anatel entende que esse sistema atenderia ao objetivo da utilização das ferramentas de acesso remoto como os tratados na presente audiência pública?

O SENHOR GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL) - Obrigado, Doutora!

Como Vossa Excelência mencionou, existem as leis que determinam que a autoridade judicial pode determinar a forma da quebra de sigilo. Eventualmente, hoje, um juiz poderia determinar que fosse feito algo que não consta do procedimento do Sittel. Provavelmente, isso chegaria diretamente a uma operadora, que deveria avaliar se conseguiria fazer o atendimento ou não.

Quando há um conjunto de demandas relacionadas ao mesmo modelo, levamos ao grupo do Sittel, para que aquela demanda seja apreciada por todos, em uma melhor forma de padronizar e dar encaminhamento. Se chegar à agência o pedido para fazer o desenvolvimento de um outro método hoje não contemplado, desde que mediante decisões judiciais, discutimos com todos os atores, sob o ponto de vista técnico, de segurança, daquela funcionalidade e de

respeito às regras incidentes. Uma vez alcançado o consenso entre todos, é aprovado para aplicação por todas as operadoras.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Da sua fala também é certo afirmar que as operadoras de telefonia possuem capacidade de indicar a localização, com coordenadas geográficas, de dispositivos de celular? Ou a informação que as operadoras possuem é apenas da localização da antena sensibilizada pela utilização?

O SENHOR GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES – ANATEL) - Existe a informação sobre a localização, já provida hoje, mas há uma discussão sobre métodos para melhorar a informação sobre localização.

Existem técnicas de triangulação em relação às antenas, mas também existe um serviço que a gente chama de GTLOC. Quando se está em uma emergência e o aparelho está sem rede de telefonia, é possível fazer a discagem por esse método. Se ligar para a polícia, por exemplo, a coordenada é indicada com mais precisão.

Avaliam-se evoluções na informação sobre a localização, mas, de fato, sim, temos os dados de localização e é sempre possível aperfeiçoar.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) – Obrigada.

Agora, Coronel Croce, os dispositivos - não sei se vou falar certo - IMSI-catchers permitem a interceptação telefônica e de dados sem a necessidade de intervenção das operadoras de telefonia.

Há autorização judicial para o seu uso pelo Exército? O uso desses dispositivos é feito para fins de inteligência? Quem controla o seu uso?

O SENHOR JOÃO RICARDO DA CUNHA CROCE LOPES (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - EXÉRCITO) - Obrigado pela pergunta, Subprocuradora.

Eu realmente não tenho essa informação, porque eu não sou especialista técnico na parte do IMSI. O que eu posso garantir é que não há um sistema desse previsto - desde a política, diretriz etc. -, só que realmente me falta informação para eu confirmar à Senhora se tem possibilidade de fazer isso ou não, porque não tenho a informação técnica sobre o assunto.

A SENHORA ELIZETA MARIA DE PAIVA RAMOS (SUBPROCURADORA-GERAL DA REPÚBLICA) - Obrigada. É só, Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à doutora Elizeta Maria de Paiva Ramos. E pergunto ao doutor Leonardo

Magalhães, Defensor Público-Geral Federal, se tem alguma pergunta aos expositores.

O SENHOR LEONARDO CARDOSO DE MAGALHÃES (DEFENSOR PÚBLICO FEDERAL) - Sem perguntas, Senhor Ministro.

O SENHOR MINISTRO CRISTIANO ZANIN - Pergunto à doutora Carolina, ao doutor Lucas, juízes-instrutores, se têm alguma pergunta aos expositores.

A SENHORA CAROLINA SANTOS LIMA (JUÍZA-INSTRUTORA) - Uma única pergunta, Ministro.

Eu queria saber do doutor Gustavo Borges, que representa a Anatel. Pelo que foi dito, na manhã de hoje, essas ferramentas, que são tratadas no inicial, elas se valem de vulnerabilidade da rede, podemos dizer assim, de falhas na rede, falhas de segurança. Então, de certa forma, a utilização dessas ferramentas se contrapõe até ao objetivo da Anatel, que busca maior segurança das telecomunicações de modo geral. Na sua visão, o desenvolvimento de uma ferramenta própria, como foi mencionado também por alguns expositores, pelo Estado brasileiro, pelos agentes, aqui, localizados no Brasil, seria compatível, haveria uma compatibilidade, seria possível compatibilizar com os objetivos da própria Anatel, trazendo mais segurança nas telecomunicações? Ou sempre haverá

a necessidade de uma vulnerabilidade, ou mesmo que ela seja mantida durante um tempo? Você poderia só esclarecer esse ponto, por favor?

O SENHOR GUSTAVO SANTANA BORGES (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES - ANATEL) - Obrigado, doutora.

De fato, nós entendemos que a técnica existe, hoje, na forma de ataques às redes de telefonia; e isso sempre buscando e alimentando o mercado de vulnerabilidades totalmente incompatível com a busca de aumentar a segurança cibernética associada aos serviços de telefonia e incompatível com o que determina a Constituição em termos de preservação do sigilo das comunicações.

Então, na medida que essa ferramenta, hoje, existe, é comercial, não temos garantias, pelo menos a Agência não tem o controle de que ela está sendo vendida somente para órgãos competentes e não está sendo vendida, inclusive, para empresas privadas.

Então, entendemos que o ideal seria o desenvolvimento de uma ferramenta que entregue as informações que são importantes para a persecução penal, enfim, que seja feito uma entrega de informação de uma forma que não se baseie na busca de dados por meio de ataque às redes de telefonia. Acho que em um grupo de trabalho com as operadoras, eventualmente com empresas de tecnologia, possa ser discutido o desenvolvimento de uma ferramenta que faça essa entrega desses dados necessários sem o ataque a vulnerabilidades.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Uma pergunta feita pelo doutor Matheus Parma ao Coronel Croce.

Vossa senhoria afirmou que a inteligência militar busca o dado negado em suas ações. Vossa senhoria concorda com a colocação da doutora Lílian Cintra de Melo, que em sua apresentação afirmou que a inteligência se faz apenas com dados de fontes abertas? Vossa senhoria identifica algum risco para o país nessa visão restritiva das operações de inteligência? Quais são as ferramentas de intrusão legalmente disponíveis aos serviços de inteligência de países comparáveis com o Brasil? São várias perguntas.

O SENHOR JOÃO RICARDO DA CUNHA CROCE LOPES (MINISTÉRIO DA DEFESA - FORÇAS ARMADAS DO BRASIL - EXÉRCITO) - Sim, Senhor Ministro. Obrigado pela pergunta. Vamos por partes.

Bem, a inteligência militar, assim no Brasil como em outros países, busca o dado aberto, sim; 95% das informações, digamos assim, estão em fontes abertas. Mas existem também os dados negados. Conforme o nosso companheiro, aqui, o Danilo, mencionou o Stuxnet; então só poderia ser feita aquela operação tendo conhecimento onde as centrífugas estariam e o modo de se chegar lá. Então a inteligência vai buscar o dado negado, ela vai buscar o dado de fonte aberta, mas o *core* da inteligência é, sim, a parte de análise, e defender os nossos dados negados, e defender os nossos dados pessoais e assim por diante.

Como eu mencionei na explanação, nós temos projetos estratégicos aqui de radares, de mísseis, submarinos, desenvolvimento de tecnologia nuclear, que são valorosos a outros países. Então nós temos que proteger, sim. E às vezes eu não preciso ter a ferramenta, mas se eu souber como ela é empregada, eu posso desenvolver protocolos e dispositivos nossos, brasileiros, para fazer essa defesa.

Como também mencionou o Danilo, no futuro, a utilização da IA é preocupante. Então existe um trabalho muito forte desenvolvido nesse sentido para aprofundar o conhecimento na parte da inteligência artificial, que vai ser um agente que vai atrás de dados abertos, e principalmente na capacitação do nosso pessoal. Porque, a partir do momento que eu teclar ou se eu me expuser, a minha vida, o meu trabalho, o meu processo, o meu *modus operandi* de como é que eu trabalho, eu também estou deixando vulnerável a minha instituição, a minha empresa e assim por diante.

Então, respondendo objetivamente, a inteligência militar, não só no País, mas mundialmente, ocorre, sim, atrás do dado negado, ela se utiliza de fontes abertas. Então, é o ponto de vista dela, não tem problema nenhum. Mas, em termos de comando de Exército, nós trabalharemos, sim, na segurança dos nossos dados negados; trabalhamos, sim, na pesquisa de fontes abertas; nós trabalhamos, sim, em parceria com as outras instituições, para que a segurança nacional, a parte

de projetos estratégicos, esteja sempre em segurança dos dados, inclusive dos dados pessoais. Obrigado.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Coronel Croce. Chegaram diversas perguntas, mas infelizmente o tempo não vai permitir que eu possa apresentá-las, mas eu encaminharei a Vossas Senhorias as perguntas.

Nesse momento, faremos um intervalo de 10 minutos para podermos ouvir o último bloco de expositores. Eu agradeço imensamente as exposições que foram feitas neste bloco, as perguntas que foram respondidas, enfim, as contribuições que foram dadas para a instrução desta ação de descumprimento de preceito fundamental. E declaro, então, suspensa a sessão por 10 minutos para um pequeno intervalo com a retomada com o último bloco de expositores.

INTERVALO

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Boa tarde a todos, dando continuidade a esta audiência pública que trata da ADPF 1.143, que tem por objetivo análise da regulamentação do uso por órgãos e agentes públicos de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal.

Nós começamos esta audiência na data de ontem, já tivemos até o momento três blocos de expositores, e agora vamos para o último bloco para ouvir também novos expositores sobre o mesmo tema.

Então, em primeiro lugar, fará uso da palavra o Doutor Juliano Madalena, que é membro do Conselho Jurídico da Associação Fiquem Sabendo. O Doutor Juliano Madalena é doutor e mestre em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul, onde também adquiriu o título de especialista em Direito Internacional. É graduado em Direito pela Fundação Escola Superior do Ministério Público, professor do curso de graduação da FMB e coordenador do curso de pós-graduação em Direito Digital. É presidente da Comissão Especial de Proteção de Dados e Privacidade da OAB do Rio Grande do Sul.

Então, passo a palavra ao Doutor Juliano Madalena, que fará a sua exposição de forma virtual.

O SENHOR JULIANO SOUTO MOREIRA MADALENA (ASSOCIAÇÃO FIQUEM SABENDO) - Muito obrigado, excelentíssimo Ministro Cristiano Zanin. Também cumprimento a excelentíssima Subprocuradora-Geral da República, a Doutora Elizeta Maria da Paiva Ramos; o também excelentíssimo Doutor Leonardo Magalhães, Defensor Público da União, e também gostaria de cumprimentar os magistrados auxiliares, o Doutor Lucas Sales e a Doutora

Carolina Lima, que estão aqui presentes; e os demais que, em razão do sistema virtual, naturalmente, a gente não tem condições de ver todos.

Ministro, antes de iniciar o mérito aqui, o conteúdo, eu só gostaria de contextualizar a agência. Fiquem sabendo, é uma agência de dados independente, que eu apresento hoje enquanto conselheiro. Ela é especializada na Lei de Acesso à Informação, é uma associação sem fins lucrativos, apartidária e comprometida com a transparência pública no país.

E o tema que nós estamos tratando hoje, gostaria de parabenizar a Doutora Elizeta pelo desenvolvimento dessa ação, porque certamente nós podemos observar, por todas as falas que antecederam e os profícuos debates aqui travados mostram justamente a importância de nós darmos luz a essa matéria e a essa questão.

Particularmente em razão do escopo da agência que é justamente a Lei de Acesso à Informação, eu notei, inclusive, Ministro Cristiano Zanin, por algumas vezes, foi falado, foi questionado sobre alguma prática específica, alguma ferramenta específica, alguma conduta específica, e nós tivemos, como resposta, a seguinte afirmação: não tenho essa informação.

É claro que nós devemos também apontar e respeitar que, neste momento nem todos os envolvidos em operações, seja da Polícia Federal, seja do Exército, da Marinha ou da própria Aeronáutica, nós não temos aqui todos os

responsáveis efetivos por realizar operações e que naturalmente podem posteriormente prestar informações mais detalhadas.

Mas a agência, fiquem sabendo, no seu escopo de atuação, ela atua justamente buscando transparência. E esse é um ponto, Ministro e Senhoras e Senhores aqui presentes, que pouco foi falado. No final do dia, a grande questão que nós temos é que esses instrumentos, independentemente do seu mérito, da sua estrutura regulatória, eles são endereçados para o indivíduo, para a população. E o questionamento que eu gostaria de trazer é quais são os instrumentos que nós indivíduos temos para exercermos justamente o nosso direito de saber em especial, Ministro Cristiano Zanin, um ponto muito relevante: quais são os instrumentos tecnológicos de investigação de que o Estado brasileiro e as suas instituições dispõem? Esse é um ponto relevantíssimo!

A agência, fiquem sabendo, diariamente, através da Lei de Acesso à Informação e todos os outros expedientes, trabalha liberando dados que se entende que devem ser dados de acesso público. E nós podemos afirmar que dados relacionados à aquisição desses tipos de ferramentas são dados extremamente difíceis de serem conseguidos e de serem acessados pela população, porque, vejam, a depender da ferramenta adquirida pelo Estado brasileiro, nós teremos um escopo e um alcance material em relação àquilo que se está investigando. E nós não estamos nem falando aqui no sistema posto que nós temos

de ordem judicial específica, que o Ministro muito bem conhece, todos que estão aqui conhecem, e sabemos que nós estamos submetidos num procedimento de investigação.

Nós não estamos falando aqui na estrutura já utilizada para esse tipo de atividade regular, e não só regular, como necessária. Não existe Estado sem processamento de dados, não existe Estado sem instrumento de investigação. Todos nós estamos cientes e estamos em concordância em relação a isso. Agora, quais instrumentos? Com quais condições?

Então, quando nós observamos, na petição inicial muito bem redigida, aqui parabenizo a Subprocuradora, nós observamos que o grande objetivo é, por meio de regulamentação do uso, ou seja, lá no pedido final nós temos uma busca de regulamentação do uso, mas faz parte da regulamentação do uso a regulamentação da aquisição.

E aqui eu falo, inclusive, observando e destacando as falas das Forças Armadas. Nós temos aqui um grande problema de soberania nacional, ou seja, quando nós estamos falando em aquisição de instrumentos de tecnologia desenvolvidos por empresas privadas, muitas delas estrangeiras, particulares, que estão submetidas a regulações de outros Estados, diretamente oferecendo produtos serviços dessa natureza e com esse escopo para o Estado brasileiro. Portanto, como que se dá essa aquisição? É o questionamento que a agência se põe a público.

E uma outra questão: como pode o cidadão brasileiro, através da Lei de Acesso à Informação, através da transparência, poder identificar exatamente quais são as ferramentas que estão disponíveis? Porque nós não estamos falando aqui num questionamento se, eventualmente, determinada pessoa está sendo investigada. Nós não estamos falando aqui num questionamento se determinada pessoa está sendo objeto de um processo de inteligência. Não é isso! Nós estamos sabendo no exercício amplo e democrático.

O Brasil possui determinadas ferramentas que estão sendo apontadas, seja na petição inicial, ou seja nas falas que nos antecederam. Onde nós encontramos essa informação? Então, vejam que esse trabalho, quando eu falo aqui da Agência Fiquem Sabendo, que é um trabalho de transparência, de busca por efetiva transparência, principalmente em matéria de instrumentos de aquisição desses utensílios, deve existir uma conduta ativa por parte do Estado em listar exatamente quais são as ferramentas disponíveis.

E isso, em razão do sistema que nós temos de organização, inclusive do Estado brasileiro, tem se mostrado extremamente complexo, ao passo em que determinadas entidades possuem procedimentos próprios para adquirir, outras com diversos convênios também o fazem de outras maneiras, de modo que o cidadão fica com uma dificuldade tremenda de realizar, de promover o exercício do que nós chamamos de autodeterminação informativa, quer é saber como os

dados dele estão sendo tratados? Por quem estão sendo tratados? Por quanto tempo? Por qual razão? E por qual base legal?

Então, eu acho que, entre tantos temas que estão sendo tratados aqui, nós precisamos dar luz para o indivíduo. Sabemos que, por formas transversais, o impacto final será esse, mas como isso está sendo utilizado, eu não tenho dúvida, como todas as autoridades que aqui falaram, essa utilização se dá dentro do escopo legal que o direito brasileiro propõe. No entanto, nós não sabemos quais são efetivamente essas ferramentas e por quais condições estão sendo adquiridas.

Então, me preocupa e nos preocupa muito, Ministro Cristiano Zanin, exatamente isso, essa reação a essa resposta, que seja por uma questão de gestão organizacional, que é completamente compreensível, ou por efetiva dificuldade do próprio ente em identificar aquilo que se tem, acerca da manifestação no sentido de que não se tem a informação.

Então, eu gostaria de agradecer a oportunidade entre tantos especialistas, tantas entidades que foram aqui ouvidas e autoridades também. Nós observamos que foi prestigiada essa entidade relacionada à transparência em medidas, inclusive, ao combate ao *lawfare*, Ministro Cristiano.

Nós não podemos permitir que o indivíduo fique sem ter instrumentos de viabilizar o seu efetivo direito, a autodeterminação informativa e,

principalmente, em realizar os controles. Que o Estado possui um sistema de controles efetivo, que as autoridades entre elas cooperam, seja para as questões de investigação, tudo isso está muito posto, está muito claro, mas lá fora? Fora desse quórum especializado, como um indivíduo realiza o exercício do amplo direito que lhe é garantido constitucionalmente para que se evite aquilo que nós não queremos que é a perseguição individual, que é obscurantismo e que é o uso da máquina estatal para perseguição?

Mais uma vez eu agradeço em nome da Agência Fiquem Sabendo e também gostaria de registrar aqui a presença do Poasec, que é um grupo de segurança da informação de Porto Alegre, através do qual muitos dos nossos colegas estão nos acompanhando aqui do sul, gaúchos.

Mais uma vez, Ministro Cristiano Zanin, agradeço a Vossa Excelência e parabenizo a todos pela participação.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Juliano Madalena pela exposição e agora passo a palavra ao Doutor Thiago Pavin, pesquisador de tecnologias de inteligência artificial aplicadas.

O Doutor Thiago Pavin é da Fipe, Fundação Instituto de Pesquisas Econômicas, além de ser, atualmente, pesquisador da Fipe/USP na área de tecnologias aplicadas à inteligência artificial, também é diretor de produtos de

inteligência artificial, empreendedor e mentor na área de dados e inteligência artificial.

Então, concedo à palavra ao Doutor Thiago, que falará também de forma virtual.

O SENHOR THIAGO PAVIN RODRIGUES (FUNDAÇÃO INSTITUTO DE PESQUISAS ECONÔMICAS - FIPE) - Boa tarde, Excelentíssimo Ministro Cristiano Zanin. Boa tarde, Subprocuradora-Geral da República Doutora Elizeta Maria de Paiva Ramos!

Cumprimento todas as autoridades e os participantes presentes.

Parabenizo todos os idealizadores desta audiência pública e considero uma honra dela participar na condição de pesquisador de tecnologias e inteligência artificial pela Fipe.

A Fipe é uma fundação de pesquisa ligada à Faculdade de Economia, Administração e Contabilidade da USP, na qual atuo desenvolvendo tecnologias que visam monitorar e estimular o desenvolvimento econômico em nosso país. Falo, portanto, da perspectiva de um desenvolvedor de produtos.

Uma das minhas linhas de pesquisa é como desenvolver inteligência analítica de alto nível e, ao mesmo tempo, proteger a privacidade dos indivíduos. Eu participo e me inspiro em parcerias com outras universidades de

países democráticos, como o MIT, Harvard e Stanford, nos Estados Unidos, e também em outros pesquisadores em universidades europeias.

Do ponto de vista tecnológico, nós separamos os conceitos de segurança da informação e privacidade. O primeiro diz respeito a prevenir a intrusão e a invasão que levam a roubo de dados. O segundo, a privacidade, por sua vez, envolve prevenir o mau uso dos dados, mesmo quando há acesso consentido por parte do usuário.

Posso afirmar tranquilamente que a prática diária de desenvolvedores de tecnologia envolve ações como coletar e analisar dados sensíveis, compartilhar dados entre instituições e parceiros, desenvolver algoritmos de inteligência artificial e desenvolver funcionalidades, geralmente, em cima de peças técnicas que os fabricantes ou outras empresas já disponibilizam como base, às vezes, de código aberto (*open source*), às vezes, não. Essas práticas são repletas de vulnerabilidades potenciais que exigem muito domínio técnico e muita experimentação para serem contornadas.

Nas últimas duas décadas, a comunidade científica se deparou com várias violações que desafiam continuamente a confiança das pessoas na tecnologia e nas empresas que as fornecem, como casos de anonimização insuficiente, engenharia reversa usando dados para descobrir informações

pessoais, e uso de base de dados para fins contrários aos interesses de seus usuários. Poderiam ser citados vários exemplos.

Eu deixei uma apresentação à disposição também desta audiência, que pode servir como base. Lá há vários exemplos, mas eu posso trazer, no caso, a Netflix, nos Estados Unidos. Fizeram um *rackathon* e o pessoal da Universidade de Austin, no Texas, conseguiu fazer uma engenharia reversa e descobrir quem eram as pessoas, a orientação sexual e coisas do tipo. Há o caso da Uber também, em que houve vazamento de dados, e o caso, famoso, da Cambridge Analytica, que usou os dados da Meta, no Facebook, na época, para influenciar as eleições. Então, todos esses casos, em conjunto, deixaram, de fato, a comunidade científica preocupada em como trabalhar para resolver esse problema.

Atualmente, a tecnologia tem amplificado o dilema entre direito individual e coletivo quando se trata de uso das informações tecnológicas. Por um lado, o indivíduo quer proteger a sua privacidade e seu bem-estar social. Por outro lado, esse bem-estar está intrinsicamente ligado ao interesse coletivo.

Há vários exemplos recentes, alguns inclusive citados aqui, em que o rastreio de celulares, quando bem empregado, protege a sociedade. Um deles é quando se usa a geolocalização para identificar focos transmissores de doenças infecciosas e avisar às autoridades de saúde local, um caso que se justifica pela

tutela à saúde, por exemplo. Outro caso é o acesso a sinal de celulares específicos para encontrar pessoas perdidas em situações de desastre natural. Há, portanto, finalidades legítimas em situações de proteção social. Porém, há, nesse dilema, uma grande região de penumbra e tensão natural entre os interesses individuais e coletivos.

Vários estudiosos têm trabalhado em novas tecnologias para descentralizar o controle da informação, empoderando indivíduos e sociedade civil nesse controle. Esse é um tema atual e premente em vários centros avançados de pesquisa. Eu mesmo tenho participado desse tipo de agenda junto ao MIT. Posso dizer que é uma linha de pesquisa recente.

Trago à luz, portanto, quatro novas tecnologias que visam contribuir para um maior respeito à privacidade, sobretudo no que diz respeito ao avanço da inteligência artificial e o uso de dados. Elas serão amplamente usadas no futuro, tanto para a inteligência quanto para a contrainteligência.

A primeira é a Web 3.0. Diria que, grosso modo, é uma proposta de criar uma nova internet, uma nova arquitetura para sites e aplicativos. Na arquitetura atual, os sites e aplicativos retêm a informação dos indivíduos gerada e cadastrada nos seus bancos de dados, especialmente dados sensíveis. Na nova proposta, essas informações sensíveis ficam sob a posse e o controle do indivíduo e o que circula na internet é apenas uma pseudoidentidade, cabendo a ele conceder

e retirar o acesso de terceiros quando bem entender. Inclusive, essa arquitetura é passível de controle do Estado.

A segunda tecnologia - pode passar o *slide*, por favor - é chamada *differential privacy*. Ela visa assegurar que, após a criação de um algoritmo, a predição resultante não possa gerar danos ao indivíduo que consta no banco de dados. Trata-se, portanto, de incluir uma camada de ruído matemático no banco de dados, no momento da construção do algoritmo, que impossibilita, portanto, uma engenharia reversa.

A terceira é *federated learning*. Sua finalidade é favorecer a construção de inteligência artificial sem que as instituições tenham que abrir ou compartilhar seus dados. Em vez de o banco de dados ser cedido aos cientistas de dados, este é que vai circular o algoritmo para ser treinado no banco de várias instituições participantes de um consórcio. Desse modo, o algoritmo captura apenas os pesos matemáticos. O algoritmo, a técnica permite, então, capturar os pesos matemáticos e, por fim, pondera e consolida num algoritmo federado, o qual é mais acurado e com menos vieses que os anteriores.

Assim, as instituições compartilham inteligência, sem, contudo, ter que compartilhar seus dados. Isso já é um grande avanço.

A quarta tecnologia é a criação de dados sintéticos. Quando se precisa compartilhar bancos em que constam dados sensíveis, geralmente a

anonimização não é suficiente. Ela pode ser insuficiente e permitir engenharia reversa ou ser excessiva e impedir as análises apropriadas dos dados. Nesse caso, aplicam-se técnicas matemáticas para sintetizar. Nesse caso, aqui, já é aplicação da técnica de dados sintético, o resultado é uma base na qual a identidade de cada indivíduo é maquiada e impossibilita a engenharia reversa, porém os principais atributos estatísticos dessa base de dados ficam preservados, como por exemplo as características sociodemográficas da população estudada.

Diante desses dilemas e avanços iminentes, trago algumas conclusões e provocações positivas a fim de contribuir para a presente temática.

De um modo geral, minha primeira conclusão é que existem interesses coletivos legítimos que demandam coleta passiva de informações. Mas, obviamente, isso precisa ser regulamentado e transmitido às comunidades e desenvolvedores. A gente precisa levar essas normas para dentro das universidades.

É certo, em segundo lugar, que toda tecnologia nasce com vulnerabilidades, as quais são corrigidas quando há contribuição entre os técnicos e os usuários - e isso acontece ao longo do tempo.

Muitas vezes elas surgem e se acumulam, ao longo de toda uma cadeia de desenvolvimento de códigos-fonte, porque é feita aplicação sobre aplicação.

O que eu penso é que a exploração maliciosa dessas vulnerabilidades não ajuda a proteção da sociedade e atrapalha a agenda dos desenvolvedores. Mas é uma luta sem fim.

Um terceiro ponto é que há grupos competentes e democráticos desenvolvendo novas técnicas de combate às violações de privacidade. Penso que como política pública é preciso investir nesses grupos de pesquisa e incentivar a inovação sobre essa temática em nosso país.

Quarto, é urgente evoluirmos a normativa para regulamentar a qualidade de softwares e correção de vulnerabilidades da indústria nacional. Temos excelentes técnicos, só precisamos organizar melhor essa agenda.

Quinto, como desenvolvedor de softwares e inteligências artificiais, preocupo-me com a soberania nacional no campo da tecnologia. Penso que o Brasil tem condições de criar um aparato *govware* para institucionalizar a intrusão regulamentada, a qual deve ser devidamente pautada em leis e incluir o controle social em seu monitoramento, como no exemplo da Alemanha.

Sexto, por fim, como entusiasta de tecnologia, penso ser produtivo regulamentar a venda e o acesso de softwares intrusivos internacionais, incluindo fiscalização e punição em caso de abuso tanto do Estado quanto da sociedade civil.

Encerro minha fala agradecendo novamente pela oportunidade de participar desta audiência e permaneço à disposição.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço ao Doutor Thiago Pavin pela exposição e agora concedo a palavra à última expositora, Doutora Tereza Mellin Gimenes, que é coordenadora da Comissão Jurídica de Tecnologias da Informação e da Comunicação da Associação Brasileira de Indústria Elétrica e Eletrônica. A Doutora Tereza Gimenes fala virtualmente e tem a palavra.

A SENHORA TEREZA MELLIN GIMENES (ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA ELÉTRICA E ELETRÔNICA - ABINEE) - Olá, boa tarde, excelentíssimo Ministro Cristiano Zanin, na pessoa de quem cumprimento os demais presentes. Prometo ser breve.

Estou aqui no papel de representante da Abinee, que é a Associação Brasileira da Indústria Elétrica e Eletrônica. É uma associação com mais de 60 anos, e está aqui representada a maior parte do setor de telefonia, informática, também o setor de produção de *chips*, componentes para a montagem e fabricação desses produtos.

Atualmente, a indústria investe pesadamente em ferramentas de controle para manter os produtos cada vez mais seguros. Temos métodos atuais de duplicidade de senhas, redundância de formas de desbloqueio, os famosos *shields*,

os escudos que é possível configurar no aparelho, configuração para *download* de fontes seguras.

E quando se fala no uso de ferramentas que trabalham na fragilidade do sistema, estamos falando de prejuízo severo, algo em que a indústria já trabalha pesadamente para a configuração. No mesmo sentido, a indústria hoje colabora com as ordens judiciais e de autoridades policiais no sentido de fornecer os dados, mesmo que limitados, a que ela tem acesso para as investigações que forem necessárias. Então, nesse sentido, quando se fala de softwares *malwares* que estão trabalhando na fragilidade, é difícil identificar aqueles que estão sendo usados com propósito positivo daqueles que estão sendo usados com propósito negativo. E hoje temos, cada vez mais frequentemente, golpes aplicados a pessoas que não possuem conhecimento suficiente ou até mesmo àquelas que possuem e acabam clicando e que instalam produtos de *phishing*, que buscam dados e que acabam prejudicando o consumidor. É nesse sentido que a indústria sempre trabalha para deixar o produto cada vez mais seguro.

Então, como bem pontuado pelo representante da Anatel, estamos construindo um caminho para ter ferramentas que possam ser utilizadas pelas autoridades responsáveis na obtenção de dados de fato necessários. E quando falamos em trabalhar na brecha, ou na fragilidade, prejudicamos aquilo que está sendo construído à luz e ao uso de muita tecnologia de hoje.

Nesse mesmo sentido, eu gostaria de pontuar, por exemplo, que o mercado de produtos irregulares e ilegais, vindos por meio de contrabando para o Brasil, praticamente duplicou as vendas no último ano. Ou seja, ainda temos o ingresso de produtos no mercado não homologados pela Anatel, não passaram pela indústria brasileira e entraram de forma irregular no país. Então, quando falamos no fomento de tecnologias executadas na brecha, no desconhecimento, mencionamos também o incentivo a esse tipo de venda de produtos e o mercado que está fora do controle tanto da indústria, quanto da agência regulatória.

Eu venho aqui mais no intuito de responder eventuais dúvidas que o público desta audiência venha a ter em relação à parte tecnológica e dizer que, como sempre, a indústria colabora intimamente com todos os órgãos de governo na construção de um sistema mais robusto e que cumpra as legislações já vigentes.

Com isso, encerro a minha exposição, ficando disponível para perguntas.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço à Doutora Tereza Gimenes pela exposição.

Eu teria uma pergunta para fazer a Vossa Senhoria: se a associação e seus integrantes, especialmente os fabricantes de produtos de telefonia, identificaram tentativas de vulnerabilidades por parte de equipamentos

ou ferramentas de intrusão, as chamadas ferramentas de monitoramento ou espionagem e se existe algum trabalho algum trabalho, alguma atuação da associação e dos seus membros em relação especificamente a essas ferramentas de intrusão.

A SENHORA TEREZA MELLIN GIMENES (ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA ELÉTRICA E ELETRÔNICA - ABINEE) - Atualmente, as ferramentas de que temos conhecimento trabalham numa intrusão na rede e não no aparelho em si. Com relação às ferramentas que atuam no aparelho, nós trabalhamos pesadamente em parceria com a Anatel, com as autoridades policiais, com o Procon, para justamente educar a população de hoje em como utilizar o próprio produto na identificação desse tipo de intrusão. Então, quando falamos do escopo desse processo, eu não tenho como dizer, porque, de fato, é algo que está na rede de telefonia e não no aparelho em si. Porém, quando nos referimos a *fishing*, instalação de software desconhecido, a indústria utiliza diversos meios para fortalecer o aparelho e na educação do consumidor no sentido de como usar esse fortalecimento, seja até com avisos visuais. Por exemplo, meu áudio avisou, através de uma plataforma, que está sendo ligado; se a câmera está ligada, haverá uma sinalização verde dizendo que está ligada. É uma ferramenta construída tanto para a adaptação visual de pessoas com alguma deficiência, tal como auditiva, como também no uso de segurança. Logo, tanto na educação, como

em parceria com os órgãos públicos, a indústria está sempre ativa, trabalhando nesse sentido.

O SENHOR MINISTRO CRISTIANO ZANIN (RELATOR) - Agradeço a Vossa Senhoria pela exposição e resposta.

Aqui, encerramos todas as exposições previstas para essa audiência pública. Registro que, desde a manhã de ontem até agora, nós tivemos oportunidade de ouvir a Procuradoria-Geral da República, a Ordem dos Advogados do Brasil, a Defensoria Pública da União, membros do Ministério Público, representantes da Presidência da República, do Ministério da Justiça, da Polícia Federal, da Polícia Rodoviária Federal, das Forças Armadas, por meio do Exército, da Marinha e da Aeronáutica. Também ouvimos a Anatel, ouvimos representantes da sociedade civil, pesquisadores e especialistas neste relevante tema tratado na Ação de Arguição de Descumprimento de Preceito Fundamental 1.143.

Todo esse material ficará disponível nas plataformas do Supremo Tribunal Federal e ajudará a instruir esta ADPF, que será julgada oportunamente pelo Supremo Tribunal Federal.

Então, com essas considerações, eu declaro encerrada esta audiência pública, desejando uma boa tarde a todos vocês.

****