Manohar vs. Índia

País: Índia

Região: Ásia e Pacífico Asiático

Número do caso: Requerimento de ordem judicial (Penal) nº 314 de 2021

Data da decisão: 27 de outubro de 2021

Desfecho: Deferimento do pedido

Órgão judicial: Supremo Tribunal

Área do direito: Direito Constitucional

Temas: Segurança Nacional / Liberdade de Imprensa / Privacidade / Proteção e Retenção de Dados

Palavras-chave: Segurança Nacional, Direito à Privacidade, Liberdade de Imprensa, Monitoramento

ANÁLISE DO CASO

Resumo do caso e desfecho

O Supremo Tribunal da Índia considerou que havia necessidade de se criar um Comitê de Especialistas para analisar as alegações de vigilância não autorizada e violações de privacidade por parte do governo indiano e estrangeiros em relação a cidadãos

indianos. Diferentes requerentes, incluindo jornalistas, advogados e outros ativistas de direitos humanos, alegaram que seus dispositivos digitais foram comprometidos pelo spyware Pegasus, desenvolvido por uma empresa israelense de tecnologia, com base em uma investigação realizada por 17 organizações dos meios de comunicação de todo o mundo. O Tribunal decidiu que a vigilância não autorizada dos dados armazenados a partir dos dispositivos digitais dos cidadãos por meio de spyware por quaisquer motivos além da segurança da nação seria ilegal, censurável e poderia ter graves consequências não apenas para os direitos de privacidade, mas também para os direitos à liberdade de expressão. Considerando a recusa do governo em fornecer informações sob a defesa abrangente da "segurança nacional", o Tribunal considerou que o governo não tinha fornecido informações suficientes para justificar a sua posição e, assim, ordenou a criação de um comitê independente para investigar as alegações dos requerentes.

Fatos

Os requerentes, no caso em tela, constituíam um grupo de cidadãos indianos - incluindo jornalistas, advogados e ativistas de direitos humanos - que alegaram ser diretamente afetados pelo spyware Pegasus, aliados a diversos outros litigantes de interesse público preocupados com a vigilância não autorizada e a interceptação de comunicações na Índia.

Em setembro de 2018, um laboratório de pesquisa canadense (Citizen Lab) revelou que certas agências de inteligência governamental e de aplicação da lei não identificadas estavam utilizando o Pegasus, "um conjunto de spyware" desenvolvido por uma empresa de tecnologia de Israel (o Grupo NSO). O software compromete o dispositivo digital de uma pessoa ao dar a um usuário do Pegasus acesso em tempo real a todos os dados armazenados, e-mails, mensagens de texto, chamadas telefônicas, câmera e gravações de áudio da pessoa monitorada.

O usuário do Pegasus recebe todo o controle e, consequentemente, pode controlar remotamente diferentes funcionalidades do dispositivo sem qualquer ação por parte do proprietário do dispositivo (pessoa monitorada). O Citizen Lab estimou que tinha afetado cidadãos de quase 45 países. Em maio de 2019, a gigante de mensagens instantâneas WhatsApp Inc. anunciou que o Pegasus poderia ter infiltrado os dispositivos dos usuários do WhatsApp. Em 20 de novembro de 2019, o então Ministro de Direito e Eletrônica e Tecnologia da Informação da Índia divulgou no parlamento que certos cidadãos indianos tinham sido afetados pelo software.

Em 15 de junho de 2020, o Citizen Lab e a Anistia Internacional anunciaram que tinham descoberto outra ação do spyware, que tinha como alvo nove pessoas na Índia. Em 18 de julho de 2021, 17 organizações dos meios de comunicação de todo o mundo, incluindo uma organização indiana ("The Wire"), divulgaram uma lista de cerca de 50.000 números de celular que foram alegadamente infiltrados pelo software Pegasus (portanto, sob vigilância de clientes do Grupo NSO).

Assim, os governos estrangeiros começaram a se envolver com o governo de Israel ou iniciaram investigações internas sobre as alegações. Segundo denunciaram, cerca de 300 números de celular eventualmente monitorados pertenciam a jornalistas, médicos, figuras políticas e funcionários do tribunal indiano. No momento da propositura dos requerimentos, havia sido confirmado que o software Pegasus tinha se infiltrado em dez celulares de cidadãos indianos.

Em 18 de julho de 2021, o Ministro do Transporte Ferroviário, Comunicações e Eletrônica e Tecnologia da Informação (representando o governo indiano, que foi o Réu neste caso) questionou a base factual das denúncias e negou a ocorrência de qualquer vigilância ilegal. O ministro também repetiu a natureza "extremamente rigorosa" das leis indianas relativas à vigilância e intercepções de comunicação e afirmou que nenhum monitoramento ilegal seria capaz de ocorrer sob o referido governo [§ 8].

Em 10 de agosto de 2021, a petição foi apresentada ao Procurador Geral da Índia. Os requerentes propuseram seus pedidos perante o Tribunal Superior da Índia em face do governo indiano, em que solicitavam uma investigação independente sobre as alegações de vigilância ilegal, ataque cibernético e violação da privacidade desses cidadãos indianos. Mencionando a inércia do governo indiano em analisar devidamente as diversas denúncias apresentadas sobre a utilização do software Pegasus, os requerentes questionaram se o Réu e as suas agências tinham sido clientes do Grupo NSO, contrariando o regime legal estabelecido sobre vigilância na Índia.

Visão geral da decisão

Em 27 de outubro de 2021, o Presidente do Tribunal da Índia, N. V. Ramana, a Ministra Hima Kohli e o Ministro Surya Kant proferiram sua decisão em colegiado. O ponto central da lide era analisar se os autores da ação tinham devidamente demonstrado, a partir de uma análise sumária, a verossimilhança dos fatos narrados, ou seja, que as suas alegações acerca da vigilância não autorizada e violação de sua privacidade possivelmente teria ocorrido, o que lhes permitiria o deferimento do pedido que consistia na constituição de um comitê independente para investigar as denúncias oferecidas.

1) Os argumentos dos autores:

Os autores apresentaram uma série de argumentos contra o réu. Para sustentar suas alegações, eles contaram com várias declarações juramentadas de especialistas em segurança cibernética, reportagens verificadas de diversas organizações jornalísticas conceituadas em todo o mundo e relatórios de organizações, como o Citizen Lab.

Ademais, os requerentes afirmavam que a vigilância ilegal realizada pelo réu, por meio do spyware Pegasus, não apenas violou o seu direito à privacidade, como também constituiu uma "intimidação" da sua liberdade de expressão [§ 21].

Ainda, sustentaram que o software Pegasus além de poder ser utilizado para monitorar o dispositivo de um indivíduo, também permite implantar evidências e documentos falsos no equipamento, o que poderia trazer prejuízo à vítima. Assim, retomaram que o governo tem por obrigação "tomar as medidas necessárias para proteger os interesses e direitos fundamentais dos cidadãos, especialmente quando havia o risco de referido ataque ser orquestrado por uma entidade estrangeira" [§ 19]. Também, os autores afirmaram que, apesar do reconhecimento do Parlamento em 2019 de que alguma forma de hacking tinha ocorrido, nenhuma ação subsequente tinha sido tomada, o que caracterizaram como uma "questão preocupante" [§ 18]. Pelo contrário, no momento, o Estado se recusou a fornecer qualquer informação, o que entenderam como uma violação aos seus direitos fundamentais como cidadãos indianos.

Além disso, foi indicado que o réu não tinha feito nenhuma declaração específica negando as alegações acerca da utilização do software ou do monitoramento ilegal dos autores. Desta forma, podia-se concluir que o réu tinha admitido a veracidade das alegações. Ademais, considerando a ausência de contestação dos referidos fatos narrados, os requerentes entenderam que não se podia confiar no réu para deliberar a formação de seu próprio Comitê para investigar o caso. Em vez disso, segundo os autores, o Tribunal deveria criar um Comitê independente orientado por um juiz reformado para evitar quaisquer "questões de credibilidade" [§ 20].

2) Argumentos do réu:

O réu juntou uma "declaração juramentada limitada", argumentando que o tipo de informação de vigilância solicitada pelos requerentes não poderia ser tornada pública, pois haveria o risco de se comprometer a segurança nacional do Estado e poderia ser utilizada por grupos terroristas. Reiterando a declaração feita pelo Ministro da Tecnologia da Informação, o réu enfatizou que não havia qualquer envolvimento estatal em monitoramento ilegal.

Além do mais, o réu estava disposto a criar um Comitê de Especialistas para investigar "todos os aspectos" da denúncia elaborada a fim de "amenizar as preocupações do público e dissipar quaisquer falsas narrativas" [§ 17]. Assim, apesar das preocupações dos requerentes, o governo argumentou que não havia razão para o público duvidar da credibilidade de tal Comitê que viria a ser formado pelo réu.

3) Lei Aplicável

A privacidade é assegurada pela Constituição da Índia sob a proteção do "direito à vida", expresso no artigo 21 da Magna Carta. O direito à vida na Índia possui uma interpretação extensiva e, assim, "não se refere à mera existência do indivíduo, mas também contempla a garantia de certa qualidade [de vida]". Ainda, ressalta-se que, conforme decidido pelo Tribunal no processo histórico de K. S. Puttaswamy vs. Índia (2017) 10 SCC 1 ("Puttaswamy"), o direito à privacidade na Índia foi considerado "tão sagrado quanto a existência humana e inalienável à dignidade e autonomia humanas" [§ 32]. "Ainda assim, o Tribunal, naquele processo, reconheceu que o direito à privacidade não é absoluto e registrou hipóteses em que há conflitos de direitos e,

dessa maneira, possibilitariam a aplicação de medidas legais, como: a) disposição que justifique a violação da privacidade; b) a existência de um "objetivo legítimo do Estado" e razoabilidade da medida que garanta "natureza e o conteúdo da lei que impõe a restrição se enquadra na zona de razoabilidade"; e a proporcionalidade da legislação em relação ao "objeto e necessidades que a lei pretende cumprir" [parág. 34].

4) O direito à privacidade na era da informação

Inicialmente, a Corte classificou o direito à privacidade como "sagrado" e ressaltou a sua proteção garantida na Constituição, conforme sua decisão anterior em Puttaswamy [§ 32]. Ainda, os magistrados, tendo em vista que na era da "revolução da informação, onde a integralidade da vida dos indivíduos armazenadas em nuvem ou em um dossiê digital", entenderam que deve ser reconhecida a possibilidade da tecnologia romper com a privacidade individual enquanto aprimora a vida das pessoas [§ 31]. Ademais Corte notou que as informações dos cidadãos indianos atualmente não são coletadas apenas por agências do estado e de inteligência, mas também por companhias de serviços financeiros, telefones, e-mails, etc. - o que pode ser usado para objetivos legítimos como prevenir violência e terrorismo, devendo ser utilizadoa partir de evidência e da "absoluta necessidade para a segurança/interesse nacional e [...] proporcional" [§§ 35-36].

Ainda, com base no art. 21 da Constituição, a Corte entendeu que todo cidadão indiano como "membros de uma sociedade democrática civilizada têm uma expectativa razoável de privacidade [...] o que permite exercer suas escolhas, liberdades e liberdade" [§ 32]. Contudo, como visto anteriormente, o direito à privacidade pode sofrer razoáveis limitações - assim como todos os demais direitos fundamentais - cabendo à Corte ponderar os direitos e interesses conflitantes.

Ao aplicar os princípios legais ao presente caso, a Corte reconheceu que em um Estado Democrático de Direito, a espionagem indiscriminada sobre indivíduos não pode ser permitida, devendo seguir parâmetros legais estabelecidos na Constituição [§ 36]. Ainda, o Tribunal apontou que o direito à privacidade é violado diretamente sempre que o Estado ou qualquer agência externa monitora ou espiona um indivíduo, sendo assim imprescindível a razoabilidade na imposição de medidas que limitem esse direito.

5) Vigilância e liberdade de imprensa

O Tribunal observou ainda que a ameaça da vigilância, ou até mesmo o conhecimento da possibilidade de estar sendo espionado, pode ter um forte impacto na forma como um cidadão "exerce os seus direitos", podendo por consequência resultar em autocensura, o que traz preocupação sobre a garantia à liberdade de imprensa [§ 39]. Assim, a Corte entendeu que "tal efeito intimidatório sobre a liberdade de expressão é um ataque ao papel vital da imprensa, que pode prejudicar a capacidade da imprensa de oferecer informações exatas e confiáveis" [§ 39]. Referindo-se ao caso Anuradha Bhasin vs. Índia, (2020) 3 SCC 637, o Tribunal aplicou um teste de dano comparativo, em que julgou se as medidas do Estado tiveram um efeito restritivo proporcional entre

os autores da ação e demais indivíduos. Considerou-se que sem essa evidência seria impossível "diferenciar a reivindicação legítima de um efeito intimidatório (*chilling effect*) de um mero argumento emocional para atender a um objetivo pessoal" [§ 39].

Ainda, o Tribunal salientou a importância de proteger as fontes de informação, como uma das condições mais básicas de qualquer liberdade de imprensa na Índia. Sem essa proteção, as fontes poderiam ser dissuadidas de ajudar os meios de comunicação a informar a população sobre assuntos de vital interesse público [§ 40]. Desta forma, o Tribunal argumentou que este caso assumiu "grande relevância", considerando a "importância da proteção das fontes jornalísticas para a liberdade de imprensa em uma sociedade democrática e o possível efeito intimidatório (*chilling effect*) que as técnicas de espionagem podem ter" [§ 41].

6) O argumento da "segurança nacional"

O réu se recusou a fornecer informações suficientes ao Tribunal sobre este assunto sob o argumento [de preservação] da "segurança nacional" e não esclareceu a sua posição sobre os fatos narrados pelos denunciantes [§. 45]. Tomando como base o precedente estabelecido por Ram Jethmalani vs. União da Índia, (2011) 8 SCC 1, o Tribunal condenou a retenção de informações pelo réu, que atuou "cegando os autores" [§ 46]. O Tribunal também observou que o fornecimento de informações pelo réu foi um "importante passo para a transparência e abertura governamental, que são valores celebrados na Constituição" [§ 47].

Além disso, a Corte considerou que embora possa haver circunstâncias específicas em que o réu possa defender de maneira justa a sua posição de negar ao Tribunal e/ou aos requerentes o acesso a certas informações (com o objetivo de proteger a soberania nacional, a ordem pública e afins), o réu não poderia obter um "passe livre" sempre que mencionasse a segurança nacional, relegando ao Tribunal o papel de um "espectador mudo". Segundo o colegiado, a segurança nacional não pode "ser um obstáculo do qual o Judiciário se afasta em virtude da sua mera menção" [§§ 49-50].

Então, o Tribunal determinou que o réu deveria arguir, provar e justificar a aplicação de suas medidas, nos termos da declaração juramentada. Ainda que se trate de fatos relevantes que demandem sigilo pelo interesse da segurança nacional.

No caso em tela, o réu não havia demonstrado como a divulgação das informações poderia afetar a segurança nacional e, dessa maneira, a simples menção da segurança nacional pelo réu não obstaculiza o Tribunal de exercer o seu poder. Desta forma, o Tribunal entendeu que deveria aceitar o caso *prima facie* apresentado pelos autores para investigar as suas alegações.

O Tribunal considerou haver um "amplo consenso de que a vigilância/acesso não autorizado aos dados armazenados em telefones e outros dispositivos dos cidadãos por motivos além da segurança nacional seria ilegal, questionável e motivo de preocupação" [§ 52]. Com base nisso, a questão que se colocava era qual tutela jurídica deveria ser instituída.

7) O Comitê de Especialistas independente

Considerando o fato do réu ter reiteradamente falhado em protocolar anteriormente uma declaração juramentada com quaisquer fatos sobre o caso ou que sustentasse o seu argumento de segurança nacional, o Tribunal mostrou-se relutante em ordenar em juízo ao réu que apresentasse uma declaração juramentada com os fatos relevantes. Por outro lado, o Tribunal emitiu uma decisão para constituir um Comitê de Especialistas independente sob a supervisão de um juiz aposentado do Tribunal Superior, R. V. Raveendran, que investigaria a natureza das alegações, a "importância pública e o suposto alcance e natureza da violação em grande escala dos direitos fundamentais dos cidadãos do país" [§ 55]. O Comitê também contará com um grupo imparcial, sem opiniões prévias e independente, incluindo o Sr. Alok Joshi, ex-oficial da IPS; Dr. Sundeep Oberoi, presidente da ISO/IEC; Dr. Naveen Kumar Chaudhary, professor de segurança cibernética e forense digital; Dr. Prabaharan P., professor da Escola de Engenharia; e Dr. Ashwin Anil Gumaste, professor associado e presidente do Instituto.

O Tribunal argumentou que isto era necessário, tendo em vista o possível impacto no direito à privacidade e à liberdade de expressão, além do eventual "efeito intimidatório" sobre os direitos de toda a população indiana, a inércia do réu, o governo alegadamente privando conscientemente os direitos dos seus cidadãos, e a gravidade de qualquer possível envolvimento de partes/países, agências ou outras entidades privadas estrangeiras [§ 56]. O Tribunal não admitiu que o réu nomeasse um Comitê de Especialistas para investigar as denúncias, pois entendeu que se assim o fizesse violaria o princípio judicial estabelecido contra a parcialidade, ou seja, que "a justiça não deve apenas ser feita, mas também vista como sendo feita" [§ 57].

O Tribunal solicitou que o Comitê de Especialistas analisasse diversos fatos, incluindo se o spyware Pegasus fora utilizado para acessar ou interceptar as informações dos cidadãos indianos, quais cidadãos foram vítimas de um eventual ataque, se esse spyware foi adquirido pelo réu e, se utilizado, nos termos de qual lei foi implantado. O Comitê de Especialistas também foi solicitado a fazer recomendações sobre diversas questões, incluindo a necessidade da implementação ou alteração de quaisquer leis que envolvam vigilância, melhoria da segurança cibernética, prevenção da invasão do direito dos cidadãos à privacidade por meio de spyware, estabelecimento de um mecanismo de reclamação e criação de uma agência independente de primeira linha para investigar vulnerabilidades cibernéticas [§ 61].

8) Conclusão

O Tribunal considerou que a vigilância não autorizada ou de acesso aos dados armazenados nos dispositivos dos cidadãos, por qualquer motivo que não fosse o de preservar a segurança nacional, seriam "ilegais, censuráveis e motivo de preocupação" [§ 52]. Considerando os possíveis impactos do caso sobre a liberdade de imprensa e o direito à privacidade, além da retenção de informação por parte do réu com uma defesa abrangente de "segurança nacional", o Tribunal ordenou a criação de um Comitê de

Especialistas independente. O réu e suas agências/autoridades associadas foram orientados a dar total apoio a este Comitê, conforme necessário. O Tribunal solicitou que o inquérito do Comitê e o relatório subsequente fossem preparados com a maior celeridade possível.

ORIENTAÇÃO DA DECISÃO

Ampliação da Liberdade de Expressão

O Tribunal Superior da Índia ampliou o direito à liberdade de expressão nos termos da Constituição, vinculando a este o direito à privacidade de todos os seus cidadãos, incluindo jornalistas. Ao decidir que a vigilância não autorizada e a ameaça de espionagem poderiam não apenas causar a autocensura, mas também colocar em risco a segurança das fontes jornalísticas e o funcionamento adequado dos meios de comunicação social em uma democracia, o Tribunal salvaguardou de forma essencial o direito à liberdade de expressão e o vinculou à dignidade e à civilidade mais ampla da vida dos seus cidadãos.

PERSPECTIVA GLOBAL

Leis internacionais e regionais correlatas

- **Índia, Keshavanand Bharti vs. Estado de Kerala (1973) 4 SCC 225**
- **Índia, Juiz Puttaswamy (aposentado) e Anr vs. União da Índia & Ors (2017), 10 SCC 1**
- **Índia, Bhasin vs. União da Índia (2020), Requerimento de ordem judicial (Civil) nº 1031/2019.**
- **Índia, Indian Express Newspapers (Bombay) Private Ltd. vs. União da Índia, (1985) 2 S.C.R. 287**
- **Índia, Ram Jethmalani e Ors. vs. União da Índia, (2011) 8 SCC 1**

SIGNIFICÂNCIA DO CASO

A decisão estabelece um precedente vinculante ou persuasivo dentro de sua jurisdição

DOCUMENTOS OFICIAIS DO CASO

Documentos oficiais do caso:

- **Decisão (Inglês)**