***Manohar vs. União da Índia***

**Análise do processo**

# Metadados

* **Número do processo**: Requerimento de ordem judicial (Penal) nº 314 de 2021
* **Data do acórdão**: 27 de outubro de 2021
* **Região**: Ásia e Pacífico Asiático
* **País**: Índia
* **Tipo de expressão**: Comunicação eletrônica/Baseada na Internet, Imprensa/Jornais
* **Órgão judicial**: Supremo (tribunal de última instância)
* **Tipo de Direito**: Direito Constitucional
* **Temas principais**: Liberdade de imprensa, Segurança nacional, Privacidade, Proteção e Retenção de Dados
* **Resultado**: Acórdão - Resultado processual, Pedido concedido
* **Status**: Fechado
* **Identificadores**: Segurança nacional, Direito à privacidade, Liberdade de imprensa, Vigilância

# Análise

### Resumo e Resultado

O Tribunal Superior da Índia considerou que havia um caso *prima facie* para criar um Comitê de Especialistas para analisar as alegações de vigilância não autorizada e violações de privacidade por parte do governo indiano e partes estrangeiras em relação a cidadãos indianos. Diversos suscitantes, incluindo jornalistas, advogados e outros ativistas de direitos humanos, alegaram que seus dispositivos digitais foram comprometidos pelo spyware Pegasus, desenvolvido por uma empresa de tecnologia de Israel, 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 outros 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 suscitantes.

### Fatos

Os suscitantes neste caso eram um grupo de cidadãos indianos, incluindo jornalistas, advogados e ativistas de direitos humanos, que reivindicaram ser diretamente afetados pelo spyware Pegasus, juntamente com inúmeros 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. O usuário do Pegasus recebe todo o controle e pode então controlar remotamente diferentes funcionalidades do dispositivo sem qualquer ação por parte do proprietário do dispositivo. 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 haviam sido afetados pelo software.

Em 15 de junho de 2020, o Citizen Lab e a Anistia Internacional anunciaram que tinham descoberto outra campanha de spyware que tinha como alvo nove pessoas na Índia. Em 18 de julho de 2021, 17 organizações de 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). Desta forma, os governos estrangeiros ou começaram a se envolver com o governo de Israel ou a iniciar investigações internas sobre as alegações. Alegadamente, cerca de 300 desses números de celular pertenciam a jornalistas, médicos, figuras políticas e funcionários do tribunal indiano. No momento da interposição dos requerimentos de ordem judicial, havia sido confirmado que o software Pegasus tinha se infiltrado em dez celulares de cidadãos indianos.

Em 18 de julho de 2021, o Ministro dos Caminhos de Ferro, Comunicações e Eletrônica e Tecnologia da Informação (representando o governo indiano, que foi o Réu neste caso) questionou a base fatual 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 que nenhuma vigilância ilegal seria capaz de ocorrer em tal regime [parág. 8].

Em 10 de agosto de 2021, os pedidos foram apresentados ao Procurador Geral da Índia. Os suscitantes interpuseram seus pedidos perante o Tribunal Superior da Índia contra o Réu (o governo indiano), solicitando uma investigação independente sobre as alegações de vigilância ilegal, ataque cibernético e violação da privacidade desses cidadãos indianos. Mencionando a inação do Réu em relação a considerar adequadamente as alegações apresentadas pelas diversas denúncias em relação à utilização do software Pegasus, os suscitantes questionaram se o Réu e as suas agências tinham sido clientes do Grupo NSO sem seguir o regime legal estabelecido relativamente à vigilância na Índia.

### Visão geral da decisão

Em 27 de outubro de 2021, o Presidente do Tribunal da Índia, N V Ramana, a juíza Hima Kohli e o juiz Surya Kant proferiram a sentença do Tribunal Superior da Índia como um plenário de três juízes. A principal questão a considerar era se um caso *prima facie* tinha sido suficientemente apresentado pelos suscitantes contra o Réu relativamente à alegada vigilância não autorizada e violação da privacidade, o que justificaria a criação de um comitê independente para investigar as alegações.

Os argumentos dos Suscitantes:

Os Suscitantes apresentaram diversos argumentos contra o Réu. Para reforçar suas reivindicações, 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.

Mais importante ainda, os suscitantes alegaram que a vigilância não autorizada do Réu por meio do spyware Pegasus não apenas violou o seu direito à privacidade, como também constituiu uma “intimidação” da sua liberdade de expressão [parág. 21].

Eles argumentaram que o software Pegasus poderia ser usado não apenas para monitorar o dispositivo de um indivíduo, mas também para implantar documentos falsos e evidências nele, o que poderia implicar essa pessoa. Como tal, era responsabilidade do Réu “tomar as medidas necessárias para proteger os interesses e direitos fundamentais dos cidadãos, particularmente quando existia o risco de um tal ataque ser feito por uma entidade estrangeira” [parág. 19]. Da mesma forma, os suscitantes alegaram que, apesar do reconhecimento do Parlamento em 2019 de que alguma forma de *hacking* tinha ocorrido, nenhuma ação subsequente tinha sido tomada, o que era uma “grave preocupação” [parág. 18]. Em vez disso, o Réu tinha-se recusado a fornecer qualquer informação sobre a questão, e essa retenção de informações violava os seus direitos fundamentais como cidadãos indianos.

Também foi indicado que o Réu não tinha feito nenhuma declaração específica negando as alegações de que tinha usado o software ou de que tinha monitorado ilegalmente os suscitantes. Desta forma, podia-se inferir que o Réu tinha admitido as alegações. Além disso, considerando esta falta de negação, não se podia confiar no Réu para formar o seu próprio Comitê para investigar a questão. Em vez disso, o Tribunal deve criar um Comitê independente orientado por um juiz reformado para evitar quaisquer “questões de credibilidade” em que nem o público nem os suscitantes confiariam nos resultados da investigação [parág. 20].

Argumentos do Réu:

O Réu interpôs uma “declaração juramentada limitada”, argumentando que o tipo de informação de vigilância solicitado pelos suscitantes não poderia ser tornada pública, pois poderia comprometer a segurança nacional da Índia e poderia ser utilizada por grupos terroristas. Reiterando a declaração feita pelo Ministro da Tecnologia da Informação, o Réu enfatizou que não havia se envolvido em nenhuma vigilância ilegal.

O Réu estava disposto a criar um Comitê de Especialistas para investigar “todos os aspectos” dessas alegações, e para “amenizar as preocupações do público e dissipar quaisquer narrativas erradas” [parág. 17]. Apesar das preocupações dos suscitantes, argumentou que não havia razão para o público duvidar da credibilidade de tal Comitê constituído pelo Réu.

Lei Aplicável

O direito à privacidade é constitucionalmente protegido nos termos do “direito à vida”, consagrado no artigo 21 da Constituição da Índia. Este direito à vida na Índia tem um “significado ampliado”, que “não se refere a uma mera existência animal, mas encerra uma qualidade específica garantida” [parág. 30], incluindo o “espaço privado sagrado de um indivíduo” [parág. 31]. Conforme decidido pelo Tribunal no processo histórico de K S Puttaswamy vs União da 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” [parág. 32]. O Tribunal, nesse processo, reconheceu que o direito à privacidade não é absoluto e registrou os direitos conflitantes de outras restrições constitucionalmente válidas: nomeadamente, uma lei que justifique tal violação da privacidade; a exigência de um “objetivo legítimo do Estado” 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].

O direito à privacidade na era da informação

O Tribunal começou por defender imediatamente o direito à privacidade como “sagrado” e constitucionalmente protegido, conforme sua decisão anterior em Puttaswamy [parág. 32]. Particularmente nesta era de “revolução da informação, onde toda a vida dos indivíduos é armazenada na nuvem ou em um dossiê digital”, o Tribunal estipulou que deve reconhecer a capacidade da tecnologia de violar a privacidade de um indivíduo da mesma forma que pode melhorar suas vidas [parág. 31]. Além disso, observou que as informações dos cidadãos indianos são agora coletadas não apenas por agências clássicas do Estado e de inteligência, mas também por empresas de serviços financeiros, telefones, e-mails e afins, que podem ser utilizadas para fins legítimos, como a prevenção da violência e do terrorismo, mas qualquer uso desse tipo deve ser “baseado em evidências”, bem como “absolutamente necessário para a segurança/interesse nacional e... proporcional” [parag. 35-6]. Com base no artigo 21 da Constituição, o Tribunal argumentou que cada cidadão da Índia como “[m]embros de uma sociedade democrática civilizada tem uma expectativa razoável de privacidade... [e] é essa expectativa que nos permite exercer nossas escolhas, liberdades e autonomia” [parág. 32]. Entretanto, como referido acima, este direito tem restrições razoáveis, como todos os outros direitos fundamentais, e o Tribunal terá de equilibrar os interesses conflitantes em conformidade.

Ao aplicar estes princípios legais ao presente caso, o Tribunal reconheceu que “[em] um país democrático regido pelo estado de direito, a espionagem indiscriminada de indivíduos não pode ser permitida, a não ser com suficientes salvaguardas legais, seguindo o procedimento estabelecido por lei nos termos da Constituição” [parág. 36]. O Tribunal indicou que o direito à privacidade é violado diretamente sempre que o Estado ou qualquer agência externa vigia ou espiona um indivíduo, e esta troca deve ser devidamente equilibrada.

Vigilância e liberdade de imprensa

O Tribunal observou ainda que a ameaça da vigilância, ou mesmo o conhecimento de que se pode estar a ser espiado, pode ter um impacto enorme na forma como um cidadão “decide exercer os seus direitos” e pode resultar em autocensura, o que é particularmente significativo quando se trata da liberdade de imprensa [parág. 39]. Afirmou que “tal efeito de intimidação em relação à liberdade de expressão é um ataque ao papel vital da imprensa, que pode prejudicar a capacidade da imprensa de oferecer informações exatas e confiáveis” [parág. 39]. Referindo-se ao caso Anuradha Bhasin vs. União da Índica, (2020) 3 SCC 637, o Tribunal aplicou um teste de prejuízo comparativo pelo qual julgou se as restrições do Estado tinham tido um efeito restritivo em relação a outros indivíduos semelhantes durante aquele tempo, bem como em relação a qualquer um desses Autores e que, sem essa evidência, é impossível “diferenciar a reivindicação legítima de um efeito de intimidação de um mero argumento emocional para atender a um objetivo pessoal” [parág. 39].

Da mesma forma, 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 o público sobre assuntos de interesse vital para o público [parág. 40]. Desta forma, o Tribunal argumentou que este caso assumiu “importante significado”, considerando a “importância da proteção das fontes jornalísticas para a liberdade de imprensa em uma sociedade democrática e o possível efeito de intimidação que as técnicas de espionagem podem ter” [parág. 41].

A desculpa da “segurança nacional”

O Réu se recusou a fornecer informações suficientes ao Tribunal sobre este assunto, por motivos de “segurança nacional”, e não esclareceu a sua posição sobre estas alegações ou sobre quaisquer outros fatos da questão [parág. 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 e de outra forma “cegando o suscitante”, particularmente em um caso como este em que os direitos constitucionalmente protegidos e fundamentais de seus cidadãos estão envolvidos [parág. 46]. O Tribunal observou, de maneira aflitiva, que o fornecimento de informações pelo Réu foi um “importante passo para a transparência e abertura governamental, que são valores celebrados n[a] Constituição” [parág. 47]. Embora possa haver circunstâncias específicas em que o Réu possa defender de maneira justa a sua posição de negar ao Tribunal e/ou aos suscitantes o acesso a certas informações (como para proteger a soberania da Índia, a ordem pública, o desprezo ao tribunal e afins), o Réu não poderia obter um “passe livre” sempre que mencionasse a segurança nacional, permitindo que o Tribunal se tornasse um “espectador mudo”, e nem a segurança nacional poderia “ser o barrete do qual o Judiciário se afasta, em virtude da sua mera menção” [paras. 49-50]. O Tribunal estipulou que o Réu deve poder invocar, provar e justificar especificamente uma preocupação constitucional específica ou outra imunidade legal nos termos da declaração juramentada, a par dos fatos relevantes que indicam a informação que solicita que permaneça em segredo no interesse da segurança nacional.

Neste caso, o Réu não tinha conseguido mostrar como a divulgação da informação podia afetar a segurança nacional e que a simples menção da segurança nacional não impedia o Tribunal de exercer o seu poder. Desta forma, o Tribunal sentiu que deveria aceitar o caso *prima facie* apresentado pelos suscitantes para investigar as 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” [parág. 52]. Com base nisso, a questão que se colocava era qual tutela jurídica deveria ser utilizada.

O Comitê de Especialistas independente

Considerando o fato de o Réu ter repetidamente falhado em protocolar uma declaração juramentada com quaisquer fatos sobre o caso ou sobre a sua defesa de segurança nacional, o Tribunal mostrou-se relutante em ordenar 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” [parág. 55]. O Comitê também contam com um grupo imparcial, sem opiniões prévias e independente, incluindo o sr. Alok Joshi, ex-oficial da IPS; dr. Sundeep Oberoi, presidente, ISO/IEC; dr. Naveen Kumar Chaudhary, professor (Segurança Cibernética e Forense Digital); dr. Prabaharan P., Professor (Escola de Engenharia); e dr. Ashwin Anil Gumaste, professor associado presidente do Instituto.

O Tribunal argumentou que isto era necessário, por motivos incluindo o possível impacto no direito à privacidade e à liberdade de expressão, o possível “efeito de intimidação” deste caso em relação aos direitos de toda a população indiana, a falta de ação do Réu, o governo alegadamente privando conscientemente os direitos dos seus cidadãos, e a gravidade de qualquer possível envolvimento de partidos/países, agências ou outras entidades privadas estrangeiras [parág. 56]. Recusou-se a permitir que o Réu nomeasse um Comitê de Especialistas para efeitos de investigação das alegações, uma vez que tal linha de ação violaria o princípio judicial estabelecido contra a parcialidade, ou seja, que “a justiça não deve ser feita, mas também confirmada” [parág. 57].

O Tribunal solicitou que o Comitê de Especialistas determinasse diversos fatos, incluindo se o spyware Pegasus foi utilizado para acessar ou interceptar, de outra forma, as informações dos cidadãos indianos existentes em seus dispositivos, quais cidadãos foram afetados, 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 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, o estabelecimento de um mecanismo de reclamação e a criação de uma agência independente de primeira linha para investigar vulnerabilidades cibernéticas [parág. 61].

Conclusão

O Tribunal considerou que as alegações de vigilância não autorizada ou de acesso, de outro modo, aos dados armazenados nos dispositivos dos cidadãos, por qualquer motivo para além da segurança nacional, seriam “ilegais, censuráveis e motivo de preocupação” [parág. 52]. Considerando as possíveis ramificações em relação à liberdade de imprensa e o direito à privacidade, juntamente com a 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 brevidade possível.

# Direção

**Resultado**: Ampliação da expressão

O Tribunal Superior da Índia ampliou o direito à liberdade de expressão nos termos da Constituição, vinculando seu importante significado ao 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

### Tabela de fontes de direito

Jurisprudência, normas ou leis nacionais

* 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

# Significado

A decisão estabelece um precedente vinculante ou persuasivo na respectiva jurisdição.

# DOCUMENTOS OFICIAIS DO PROCESSO

* [Sentença](https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/pegasus-order-supreme-court-403008.pdf) (inglês)

**Relatórios, análises e artigos de notícias:**

* **[Pegasus] “Não queremos um governo que possa ter utilizado o Pegasus para criar um comitê próprio”: Kapil Sibal comparece perante o Tribunal Superior**[**https://www.livelaw.in/top-stories/pegasus-supreme-court-government-committee-kapil-sibal-it-act-infiltration-179670**](https://www.livelaw.in/top-stories/pegasus-supreme-court-government-committee-kapil-sibal-it-act-infiltration-179670)
* **Pegasus – Audiência do Tribunal Superior de Justiça – Sustentação oral**[**https://www.livelaw.in/top-stories/pegasus-snoop-gate-supreme-court-sit-probe-181466?infinitescroll=1**](https://www.livelaw.in/top-stories/pegasus-snoop-gate-supreme-court-sit-probe-181466?infinitescroll=1)
* **Como compreendemos a decisão do Tribunal Superior sobre o Pegasus**[**https://indianexpress.com/article/opinion/columns/pushback-on-pegasus-supreme-court-7594173/**](https://indianexpress.com/article/opinion/columns/pushback-on-pegasus-supreme-court-7594173/)
* **A decisão do Tribunal sobre o Pegasus ainda é insuficiente**[**https://www.thehindu.com/opinion/lead/the-courts-order-on-pegasus-still-falls-short/article37274506.ece**](https://www.thehindu.com/opinion/lead/the-courts-order-on-pegasus-still-falls-short/article37274506.ece)
* **Tribunal Superior indiano ordena inquérito sobre a utilização do spyware Pegasus pelo Estado**[**https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware**](https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware)
* **Uma investigação credível: Sobre o veredito do Tribunal Superior sobre o Pegasus**[**https://www.thehindu.com/opinion/editorial/a-credible-probe-the-hindu-editorial-on-supreme-court-verdict-on-pegasus-row/article37200571.ece**](https://www.thehindu.com/opinion/editorial/a-credible-probe-the-hindu-editorial-on-supreme-court-verdict-on-pegasus-row/article37200571.ece)
* **O spyware é vendido aos governos para combater o terrorismo. Na Índia, era utilizado para *hackear* jornalistas e terceiros.**[**https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/**](https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/)