Global Freedom of Expression
COLUMBIA UNIVERSITY

Manohar c. Union of India

Inde, Asie et Asie-Pacifique

Affaire Résolue
Renforce la liberté d'expression

MODE D'EXPRESSION
Communication électronique / Internet, Presse / Journaux

DATE DE LA DECISION
27 octobre 2021

NUMERO DE L'AFFAIRE
Recours légal (criminel) n° 314 de 2021

ORGANE JUDICIAIRE
Cour suprême (Tribunal de dernière instance)

TYPE DE DROIT
Droit constitutionnel

PRINCIPAUX THEMES:
Liberté de la presse, Sécurité nationale, Vie privée, Protection et conservation des données

ISSUE :
Décision - Résultat de la procédure, Requête accordée

MOTS CLES :
Sécurité nationale, Droit à la vie privée, Liberté de la presse, Surveillance

L'examen comprend :

- L'analyse de l'affaire
- Le sens de la décision
- La perspective globale
- L'importance de l'affaire

ANALYSE DE L'AFFAIRE

Résumé et issue

La Cour suprême de l'Inde a estimé qu'il existait un motif suffisant pour créer un comité d'experts chargé d'examiner les allégations de surveillance non autorisée et de violation de la vie privée de citoyens indiens par le gouvernement indien et des entités étrangères. De nombreux pétitionnaires, dont des journalistes, des avocats et d'autres militants des droits de l'homme, ont allégué que leurs appareils numériques avaient été compromis par le logiciel espion Pegasus, développé par une entreprise technologique israélienne, sur la base d'une enquête menée par dix-sept organisations médiatiques du monde entier. La Cour a statué que la surveillance non autorisée des données stockées sur les appareils numériques des citoyens par le biais d'un logiciel espion pour des raisons autres que la sécurité nationale serait illégale, répréhensible et susceptible d'avoir de lourdes conséquences non seulement sur le droit à la vie privée, mais aussi sur le droit à la liberté d'expression. Compte tenu du refus du gouvernement de fournir des informations sous la couverture de la "sécurité nationale", la Cour a estimé que celui-ci n'avait pas fourni suffisamment d'informations pour justifier sa position et a donc ordonné la création d'un comité indépendant pour enquêter sur les allégations des requérants.

Les faits

Les requérants dans cette affaire étaient un groupe de citoyens indiens, dont des journalistes, des avocats et des militants des droits de l'homme, qui affirmaient être directement affectés par le logiciel espion Pegasus, aux côtés de nombreux autres plaignants d'intérêt public préoccupés par la surveillance non autorisée et l'interception des communications en Inde.

En septembre 2018, un laboratoire de recherche canadien nommé Citizen Lab a révélé sans les nommer que certaines agences gouvernementales de renseignement et forces de l'ordre avaient utilisé Pegasus, « un ensemble de logiciels espions » développée par une entreprise technologique israélienne (le groupe NSO). Le logiciel compromet l'appareil numérique d'une personne en donnant à l'utilisateur de Pegasus un accès en temps réel à l'ensemble des données stockées, des courriels, des messages SMS, des appels téléphoniques, de la caméra et des enregistrements audio de cette personne. Le contrôle total est donné à l'utilisateur de Pegasus, qui peut alors contrôler à distance différentes fonctionnalités de l'appareil sans aucune action du propriétaire de l'appareil. Citizen Lab a estimé que ce logiciel avait touché des citoyens de près de quarante-cinq pays. En mai 2019, le géant de la messagerie instantanée WhatsApp Inc a annoncé que Pegasus pourrait avoir infiltré les appareils des utilisateurs de WhatsApp. Le 20 novembre 2019, le ministre indien d l'électronique et des technologies de

l'information de l'époque a révélé au parlement que certains citoyens indiens avaient été affectés par le logiciel.

Le 15 juin 2020, Citizen Lab et Amnesty International ont annoncé avoir découvert une autre campagne de logiciels espions qui visait neuf personnes en Inde. Le 18 juillet 2021, dix-sept organisations médiatiques du monde entier, dont une organisation indienne (« The Wire »), ont révélé une liste de quelque cinquante mille numéros de téléphone mobile qui auraient été infiltrés par le logiciel Pegasus (et donc surveillés par des clients du groupe NSO). Par conséquent, les gouvernements étrangers ont entamé des discussions avec le gouvernement israélien ou ouvert des enquêtes internes sur ces allégations. Environ trois cent de ces numéros de téléphone appartiendraient à des journalistes, des médecins, des personnalités politiques et des membres du système judiciaire indiens. Au moment du dépôt des requêtes, il a été confirmé que le logiciel Pegasus se trouvait sur dix téléphones de citoyens indiens.

Le 18 juillet 2021, le ministre des chemins de fer, des communications, de l'électronique et des technologies de l'information (représentant le gouvernement indien, qui était le défendeur dans cette affaire) a mis en doute la base factuelle des rapports et a nié l'existence de toute surveillance illégale. Le ministre a également réitéré la nature « extrêmement rigoureuse » des lois indiennes relatives à la surveillance et aux interceptions de communications, et a affirmé qu'aucune surveillance illégale ne pourrait avoir lieu sous ce régime [paragraphe 8].

Le 10 août 2021, les recours ont été adressés au Solicitor General de l'Inde. Les requérants ont déposé leurs recours devant la Cour suprême de l'Inde contre le défendeur (le gouvernement indien), demandant une enquête indépendante sur les allégations de surveillance illégale, de cyberattaque et de violation de la vie privée de ces citoyens indiens. Compte tenu de l'inaction du défendeur à examiner de manière appropriée les allégations soulevées par les nombreux rapports sur l'utilisation du logiciel Pegasus, les requérants ont estimé possible que le défendeur et ses agences aient été client du groupe NSO sans suivre le régime légal établi concernant la surveillance en Inde.

Aperçu de la décision

Le juge en chef de l'Inde, N V Ramana, le juge Hima Kohli et le juge Surya Kant ont rendu l'arrêt de la Cour suprême de l'Inde en tant que collège de trois juges le 27 octobre 2021. La principale question à examiner était de savoir si les requérants avaient suffisamment établi le bien-fondé de leurs allégations de surveillance non autorisée et de violation de la vie privée contre le défendeur, ce qui justifierait la création d'un comité indépendant chargé d'enquêter sur ces allégations.

Arguments des requérants :
Les requérants ont soulevé divers arguments contre le défendeur. Pour étayer leurs affirmations, ils se sont appuyés sur diverses déclarations sous serment d'experts en cybersécurité, sur des rapports recoupés de diverses organisations de presse réputées à travers le monde, et sur des rapports d'organisations comme Citizen Lab.

De manière plus significative, les requérants ont affirmé que la surveillance non autorisée par le défendeur au moyen du logiciel espion Pegasus a non seulement violé leur droit à la vie privée, mais a également constitué une « dissuasion » dans l'exercice de leur liberté d'expression [paragraphe 21].

Ils ont fait valoir que le logiciel Pegasus pouvait être utilisé non seulement pour surveiller l'appareil d'une personne, mais aussi pour y implanter de faux documents et de fausses preuves - qui pourraient impliquer cette personne. En tant que tel, il était de la responsabilité du défendeur « de prendre les mesures nécessaires pour protéger les intérêts et les droits fondamentaux des citoyens, en particulier lorsqu'il existe un risque qu'une telle attaque soit menée par une entité étrangère » [paragraphe 19]. De même, les Requérants ont affirmé que, malgré la reconnaissance par le Parlement en 2019 qu'une certaine forme de piratage avait eu lieu, aucune action subséquente n'avait été prise - ce qui était une « grave préoccupation » [paragraphe 18]. Au lieu de cela, le Défendeur avait refusé de leur fournir toute information sur l'affaire en cours - et cette rétention d'information violait leurs droits fondamentaux en tant que citoyens indiens.

Il a également été avancé que le défendeur n'avait pas fait de déclaration précise niant les allégations qu'il avait utilisé le logiciel ou autrement surveillé illégalement les pétitionnaires. En tant que tel, il pourrait être déduit que le défendeur a admis les allégations. De plus, étant donné cette absence de démenti, on ne pouvait pas confier au défendeur le soin de former son propre comité pour enquêter sur l'affaire - la Cour doit plutôt créer un comité indépendant dirigé par un juge à la retraite pour éviter tout « problème de crédibilité » qui ferait que ni le public ni les requérants n'auraient confiance dans les résultats de l'enquête [paragraphe 20].

Les arguments du défendeur :

Le défendeur a déposé une déclaration sous serment restreinte, soutenant que le type d'informations de surveillance demandé par les requérants ne pouvait pas être rendu public car il pourrait compromettre la sécurité nationale de l'Inde et pourrait être utilisé par des groupes terroristes. Réitérant la déclaration du ministre des technologies de l'information, le défendeur a souligné qu'il ne s'était livré à aucune surveillance illégale.

Le défendeur était prêt à créer un comité d'experts pour enquêter sur « tous les aspects » de ces allégations, et pour « apaiser les inquiétudes du public et dissiper tout récit erroné » [paragraphe 17]. Malgré les préoccupations des requérants, le défendeur a fait valoir qu'il n'y avait aucune raison pour que le public doute de la crédibilité d'un tel comité constitué par le défendeur.

Droit applicable

Le droit à la vie privée est constitutionnellement protégé par le « droit à la vie », inscrit à l'article 21 de la Constitution indienne. Ce droit à la vie en Inde a un « sens élargi » - qui "ne se réfère pas à une simple existence animale mais englobe une certaine qualité assurée" [paragraphe 30], y compris « l'espace privé sacré d'un individu » [paragraphe 31]. Comme l'a jugé la Cour dans l'affaire historique K S Puttaswamy c. Union of India (2017) 10 SCC 1 (« Puttaswamy »), le droit à la vie privée en Inde a été jugé « aussi sacro-saint que l'existence humaine et inaliénable à la dignité et à l'autonomie de l'homme » [paragraphe 32]. Dans cette affaire, la Cour a reconnu que le droit à la vie privée n'est pas absolu et a noté les droits concurrents d'autres restrictions constitutionnellement valides : à savoir, une loi justifiant tout empiètement sur la vie privée ; l'exigence d'un « but légitime de l'État » garantissant que « la nature et le contenu de la loi qui impose la restriction se situent dans la zone du raisonnable » ; et la proportionnalité de la législation à « l'objet et aux besoins que la loi cherche à satisfaire » [paragraphe 34].

Le droit à la vie privée à l'ère de l'information

La Cour a commencé par confirmer immédiatement que le droit à la vie privée est " sacro-saint " et protégé par la Constitution, comme elle l'avait déjà fait dans l'arrêt Puttaswamy [paragraphe 32]. Particulièrement en cette ère de « révolution de l'information, où la vie entière des personnes est stockée dans le cloud ou dans un dossier numérique », la Cour a stipulé qu'elle devait reconnaître la capacité de la technologie à porter atteinte à la vie privée d'un individu de la même manière qu'elle peut améliorer sa vie [paragraphe 31]. En outre, elle a noté que les informations des citoyens indiens sont désormais collectées non seulement par l'État et les agences de renseignement, mais aussi par les sociétés de services financiers, les téléphones, les courriels et autres - qui peuvent être utilisés à des fins légitimes telles que la prévention de la violence et du terrorisme, mais toute utilisation de ce type doit être « fondée sur des preuves », ainsi qu'« absolument nécessaire pour la sécurité/les intérêts nationaux et... proportionnelle » [paragraphes 35-6]. S'appuyant sur l'article 21 de la Constitution, la Cour a estimé que chaque citoyen indien, en tant que « membre d'une société démocratique civilisée, peut raisonnablement s'attendre à ce que sa vie privée soit respectée... C'est cette attente qui nous permet d'exercer nos choix, nos libertés et notre liberté » [paragraphe 32]. Toutefois, comme indiqué

ci-dessus, ce droit est assorti de restrictions raisonnables - comme tous les autres droits fondamentaux - et la Cour devra mettre en balance les intérêts concurrents en conséquence.

Tout en appliquant ces principes juridiques à la présente affaire, la Cour a reconnu que « dans un pays démocratique régi par la primauté du droit, l'espionnage aveugle des individus ne peut être autorisé qu'avec des garanties légales suffisantes, en suivant la procédure établie par la loi en vertu de la Constitution » [paragraphe 36]. La Cour a estimé que le droit à la vie privée est directement violé lorsque l'État ou un organisme extérieur surveille ou espionne un individu, et que ce compromis doit être mis en balance de manière appropriée.

Surveillance et liberté de la presse

La Cour a également noté que la menace de surveillance, ou même le fait de savoir qu'une personne peut être espionnée, peut avoir un impact considérable sur la façon dont un citoyen « décide d'exercer ses droits » et peut entraîner une autocensure, ce qui est particulièrement important en ce qui concerne la liberté de la presse [paragraphe 39]. Selon sa déclaration, « un tel effet dissuasif sur la liberté d'expression est une atteinte au rôle essential de contre-pouvoir de la presse, qui peut compromettre la capacité de la presse à fournir des informations exactes et fiables » [paragraphe 39]. Se référant à l'affaire Anuradha Bhasin c. Union of India, (2020) 3 SCC 637, la Cour a appliqué un test de préjudice comparatif selon lequel elle a évalué dans quelle mesure les restrictions de l'État avaient eu un effet restrictif sur d'autres individus similaires pendant cette période, ainsi que sur tout plaignant de ce type et que, sans cette preuve, il est impossible de « distinguer une allégation légitime d'effet dissuasif d'un simple argument émotif dans un but intéressé » [paragraphe 39].

De même, la Cour a souligné l'importance de la protection des sources d'information, comme l'une des conditions les plus fondamentales de toute liberté de la presse en Inde. Sans cette protection, les sources pourraient être dissuadées d'aider les médias à informer le public sur des questions d'intérêt essentiel pour celui-ci [paragraphe 40]. La Cour a donc estimé que cette affaire revêtait une « grande importance » étant donné « l'importance de la protection des sources journalistiques pour la liberté de la presse dans une société démocratique et l'effet potentiellement inhibiteur que peuvent avoir les techniques d'espionnage » [paragraphe 41].

Le prétexte de la « sécurité nationale »

Le défendeur avait refusé de fournir des informations suffisantes à la Cour sur cette question, au motif de la « sécurité nationale », et n'avait pas clarifié sa position sur ces allégations ou sur tout autre fait de l'affaire [paragraphe 45]. S'appuyant sur le précédent établi par Ram Jethmalani c. Union of India,

(2011) 8 SCC 1, la Cour a condamné le fait que le défendeur ait retenu des informations et ait autrement « privé le requérant de ses droits », en particulier dans une affaire comme celle-ci où les droits fondamentaux de ses citoyens, protégés par la Constitution, sont concernés [paragraphe 46]. La Cour a mis en exergue le fait que la communication d'informations par le défendeur constituait un « pas important vers la transparence et l'ouverture du gouvernement, qui sont des valeurs consacrées par la Constitution » [paragraphe 47]. Bien qu'il puisse y avoir des circonstances spécifiques dans lesquelles le défendeur peut à juste titre défendre sa position de refuser à la Cour et/ou aux requérants l'accès à certaines informations (comme pour protéger la souveraineté de l'Inde, l'ordre public, l'outrage à la Cour et autres), le défendeur ne pouvait néanmoins obtenir un « laissez-passer » chaque fois qu'il invoquait la sécurité nationale, faisant ainsi de la Cour un « spectateur muet », et la sécurité nationale ne pouvait pas non plus « être la bête noire dont le pouvoir judiciaire se détourne, du fait de sa simple mention » [paragraphes 49-50]. La Cour a statué que le défendeur doit être en mesure d'invoquer, de prouver et de justifier spécifiquement une préoccupation constitutionnelle ou une autre immunité statutaire par une déclaration sous serment, ainsi que les faits pertinents qui indiquent les informations qu'il demande de garder secrètes dans l'intérêt de la sécurité nationale.

Ici, le défendeur n'est pas parvenu à démontrer comment la révélation d'informations pourrait affecter la sécurité nationale et la simple mention de la sécurité nationale n'empêchait pas la Cour d'exercer son pouvoir. À ce titre, la Cour a estimé qu'elle devait accepter les arguments *prima facie* apportés par les requérants pour enquêter sur les allégations.

La Cour a estimé qu'il y avait un « large consensus sur le fait que la surveillance/accès non autorisé à des données stockées sur les téléphones et autres appareils des citoyens pour des raisons autres que la sécurité nationale serait illégale, répréhensible et préoccupante » [paragraphe 52]. Sur cette base, il restait à déterminer la mesure corrective qu'elle devait prendre.

Le comité d'experts indépendants

Compte tenu du fait que le défendeur avait à plusieurs reprises omis de déposer une déclaration sous serment sur le dossier avec des faits sur l'affaire ou sur leur défense de sécurité nationale, la Cour était réticente à ordonner au défendeur de déposer une déclaration sous serment avec les faits pertinents. En revanche, la Cour a ordonné la constitution d'un comité d'experts indépendants sous la supervision d'un juge de la Cour suprême à la retraite, R V Raveendran, qui enquêterait sur la nature des allégations, « l'importance publique et la portée et la nature présumées de la violation à grande échelle des droits fondamentaux des citoyens du pays » [paragraphe 55]. Le comité était en outre composé d'un groupe impartial, non préjudiciable et autrement indépendant, comprenant M. Alok Joshi, ancien officier de l'IPS ; le Dr Sundeep Oberoi, président de l'ISO/IEC ; le Dr Naveen Kumar Chaudhary,

professeur (cybersécurité et criminalistique numérique) ; le Dr Prabaharan P., professeur (école d'ingénierie) ; et le Dr Ashwin Anil Gumaste, professeur associé à la présidence de l'Institut.

La Cour a estimé que cela était nécessaire pour des raisons telles que l'impact potentiel sur le droit à la vie privée et à la liberté d'expression, le potentiel « effet dissuasif » de cette affaire sur les droits de l'ensemble de la population indienne, l'inaction du défendeur, le gouvernement qui aurait sciemment privé ses citoyens de leurs droits, et la gravité de toute implication potentielle de parties/pays étrangers, d'agences ou d'autres entités privées [paragraphe 56]. Elle a refusé d'autoriser le défendeur à nommer un comité d'experts pour enquêter sur les allégations, car une telle démarche violerait le principe judiciaire établi contre la partialité, à savoir que « la justice doit non seulement être rendue mais aussi être perçue comme telle » [par. 57].

La Cour a demandé au Comité d'experts de déterminer divers faits, notamment si le logiciel espion Pegasus a été utilisé pour accéder ou intercepter de quelque manière que ce soit les informations détenues par les citoyens indiens sur leurs appareils, quels citoyens ont été affectés, si ce logiciel espion a été acquis par le défendeur et, s'il a été utilisé, en vertu de quelle loi il a été déployé. Le comité d'experts a également été invité à formuler des recommandations sur plusieurs questions, notamment la nécessité ou la modification de toute loi relative à la surveillance, l'amélioration de la cybersécurité, la prévention de l'atteinte au droit à la vie privée des citoyens par le biais de logiciels espions, la mise en place d'un mécanisme de réclamation et la création d'une première agence indépendante chargée d'enquêter sur les cyber-vulnérabilités [paragraphe 61].

Conclusion

La Cour a estimé que les allégations de surveillance non autorisée ou d'accès aux données stockées dans les appareils des citoyens pour toute raison autre que la sécurité nationale seraient « illégales, répréhensibles et préoccupantes » [paragraphe 52]. Compte tenu des ramifications potentielles pour la liberté de la presse et le droit à la vie privée, ainsi que de la rétention d'informations par le défendeur avec une défense générale de « sécurité nationale », la Cour a ordonné la création d'un comité d'experts indépendants. Le défendeur et ses agences/autorités associées ont reçu l'ordre de fournir un soutien total à ce comité, si nécessaire. La Cour a demandé que l'enquête du Comité et le rapport ultérieur soient préparés dès que possible.

SENS DE LA DECISION

Issue : Renforce la liberté d'expression

La Cour suprême de l'Inde a élargi le droit à la liberté d'expression prévu par la Constitution, en liant sa grande signification au droit à la vie privée de tous ses citoyens, y compris les journalistes. En statuant que la surveillance non autorisée et la menace d'être espionné peuvent non seulement conduire à l'autocensure, mais aussi mettre en danger la sécurité des sources journalistiques et le bon fonctionnement des médias dans une démocratie, la Cour a sauvegardé de manière cruciale le droit à la liberté d'expression et l'a lié à la dignité et à la civilité dont jouissent les citoyens.

PERSPECTIVE GLOBALE

Sommaire des références

Normes, lois ou jurisprudence nationales

- Inde, Keshavanand Bharti c. Etat de Kerala (1973) 4 SCC 225
- Inde, Justice Puttaswamy (Retd) & Anr c. Union of India & Ors (2017), 10 SCC 1
- Inde, Bhasin c. Union of India (2020), Writ Petition (Civil) No. 1031/2019.
- Inde, Indian Express Newspapers (Bombay) Private Ltd. c. Union of India, (1985) 2 S.C.R. 287
- Inde, Ram Jethmalani & Ors. c. Union of India, (2011) 8 SCC 1

IMPORTANCE DE L'AFFAIRE

La décision établit un précédent contraignant ou persuasif dans sa juridiction.

DOCUMENTS OFFICIELS DE L'AFFAIRE

- Jugement (Anglais)

Rapports, analyses et articles de presse :

- **[Pegasus] "Nous ne voulons pas qu'un gouvernement qui aurait utilisé Pegasus mette en place son propre comité" : Kapil Sibal s'adresse à la Cour suprême https://www.livelaw.in/top-stories/pegasus-supreme-court-government-committee-kapil-sibal-it-act-infiltration-179670**
- **Pegasus - Audience de la Cour suprême - Arguments oraux https://www.livelaw.in/top-stories/pegasus-snoop-gate-supreme-court-sit-probe-181466?infinitescroll=1**

- **Comment lire l'ordonnance Pegasus de la Cour suprême ?**
  https://indianexpress.com/article/opinion/columns/pushback-on-pegasus-supreme-court-7594173/
- **L'ordonnance de la Cour sur Pegasus reste insuffisante**
  https://www.thehindu.com/opinion/lead/the-courts-order-on-pegasus-still-falls-short/article37274506.ece
- **La Cour suprême indienne ordonne une enquête sur l'utilisation par l'État du logiciel espion Pegasus**
  https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware
- **Une enquête crédible : Le verdict de la Cour suprême dans l'affaire Pegasus.**
  https://www.thehindu.com/opinion/editorial/a-credible-probe-the-hindu-editorial-on-supreme-court-verdict-on-pegasus-row/article37200571.ece
- **Le logiciel espion est vendu aux gouvernements pour lutter contre le terrorisme. En Inde, il a été utilisé pour pirater des journalistes et d'autres personnes.**
  https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/