

Enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents

2022/2077(INI) - 23/05/2023 - Rapport déposé de la commission, lecture unique

La commission d'enquête chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents a adopté le rapport de Sophia IN 'T VELD (Renew, NL) relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents.

En juillet 2021, le projet Pegasus, un collectif de journalistes d'investigation, d'ONG et de chercheurs, a publié un rapport fondé sur une liste en sa possession d'environ 50.000 numéros de téléphone qui pouvaient avoir été ciblés au moyen de logiciels espions Pegasus. Ces logiciels espions ont été largement utilisés par des gouvernements autoritaires comme démocratiques dans le monde entier, avec ou sans contrôle judiciaire, pour cibler des journalistes, des avocats, des juges, des militants, des hommes et femmes politiques et des fonctionnaires. Cela soulève des préoccupations touchant à différents niveaux de l'ordre juridique de l'Union en ce qui concerne la protection des données et de la vie privée, la liberté d'expression, la liberté de la presse, la liberté d'association, les mécanismes et les voies de recours, le droit à un procès équitable et les processus et institutions démocratiques.

En réaction à ce scandale d'une ampleur croissante, le Parlement européen a décidé, le 10 mars 2022, de constituer une commission d'enquête.

Aux fins de l'enquête, la commission PEGA a adopté une définition large de ce que sont les logiciels espions, à savoir, qu'il s'agit de logiciels espions de surveillance installés sur des appareils mobiles grâce à l'exploitation de vulnérabilités informatiques.

Certains États membres ont déployé des logiciels espions et refusé de formuler des observations à ce sujet en invoquant la sécurité nationale, qui, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne (traité UE), «reste de la compétence exclusive de chaque État membre». Néanmoins, **les jurisprudences de la Cour de justice de l'Union européenne (CJUE) et de la Cour européenne des droits de l'homme (CEDH)** précisent que les considérations de sécurité nationale doivent être conciliées avec les droits fondamentaux et les normes démocratiques profondément ancrées dans le droit de l'Union. **L'absence d'une définition claire de la sécurité nationale** et l'interprétation excessivement large de son périmètre par les autorités nationales compliquent la compréhension des justifications apportées à l'utilisation des logiciels espions.

Depuis les révélations du projet Pegasus, les États-Unis ont pris un certain nombre de mesures pour enquêter sur ces pratiques et les réglementer. Au sein de l'Union, très peu de mesures ont été prises à ce jour. Les députés estiment que **des règles claires doivent être adoptées** pour réglementer l'utilisation et la commercialisation des logiciels espions, de préférence en partenariat avec d'autres pays tels que les États-Unis.

Une question européenne

Bien que cela ne soit pas officiellement confirmé, il est permis de supposer avec une certaine certitude que tous les États membres de l'Union ont acheté un ou plusieurs logiciels espions commerciaux. L'entreprise israélienne NSO Group a commercialisé ses produits auprès de 22 utilisateurs finaux dans pas moins de 14 États membres, parmi lesquels la Pologne, la Hongrie, l'Espagne, les Pays-Bas et la Belgique. Dans au moins quatre États membres, à savoir **la Pologne, la Hongrie, la Grèce et l'Espagne**, il y a eu une utilisation illégitime de logiciels espions, et des soupçons quant à une telle utilisation existent pour Chypre. Deux États membres, Chypre et la Bulgarie, servent de plaques tournantes pour l'exportation de logiciels espions. Un État membre, l'Irlande, offre un régime fiscal favorable à un grand fournisseur de logiciels espions, tandis qu'un autre État membre, le Luxembourg, est un centre bancaire pour de nombreux acteurs du secteur des logiciels espions.

Les députés ont condamné des violations majeures de la législation européenne en Pologne et en Hongrie où les gouvernements respectifs ont démantelé les mécanismes de contrôle indépendants. Ils ont également fait part de leurs préoccupations concernant l'utilisation de logiciels espions en Grèce et en Espagne.

Capacité de réaction de l'Union européenne

Le rapport note que certains gouvernements ont employé de puissants logiciels espions hautement invasifs et intrusifs contre des citoyens de l'Union, abusant ainsi de leur droit de recourir à la surveillance en cas de risque pour la sécurité nationale. Cela met en péril la démocratie, l'état de droit et les droits fondamentaux des citoyens.

L'Union dispose de **peu de moyens pour contrer ces menaces**, et elle s'avère mal équipée pour lutter contre les activités criminelles potentielles des autorités nationales, même si elles nuisent à l'Union elle-même.

Les députés indiquent que la Commission estime que la lutte contre les transgressions du droit de l'Union relève de la seule responsabilité des autorités nationales. Face à des violations flagrantes de l'état de droit et des droits fondamentaux, cette position - qui n'a aucun fondement dans les traités de l'Union - devient très problématique. Bien que la subsidiarité et la répartition des compétences constituent un pilier du droit de l'Union, **elles ne devraient pas conduire à l'impunité des gouvernements** qui utilisent des logiciels espions contre des citoyens de l'Union à des fins politiques.

En réaction au scandale des logiciels espions, la Commission a dans un premier temps écrit des lettres afin de demander des éclaircissements aux gouvernements de la Pologne, de la Hongrie, de l'Espagne, de la Grèce, de Chypre et de la France. Il semblerait toutefois que cet avertissement de la Commission n'ait pas été suivi d'autres mesures. S'il est vrai que la Commission ne dispose d'aucune compétence pour agir dans le domaine de la sécurité nationale, **la «sécurité nationale» ne doit pas être interprétée comme donnant droit à une dérogation illimitée aux lois et traités européens** et devenir un domaine de non-droit. Il appartient aux États membres de «démontrer que la sécurité nationale serait compromise en l'espèce».

Le 21 décembre 2022, la Commission a envoyé une lettre générale à tous les États membres aux fins d'une «cartographie» de la situation dans les États membres. La Commission a posé des questions spécifiques concernant, entre autres, la finalité de l'utilisation de logiciels espions, les autorités autorisées à les déployer, la définition nationale de la sécurité nationale, la législation régissant le traitement des données à des fins de sécurité nationale, les garde-fous, l'autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, la surveillance et les notifications.

Le 28 mars 2023, le commissaire Reynders a déclaré à la commission PEGA qu'une grande majorité des États membres avaient répondu, mais que la Commission était toujours en train de recueillir les réponses

des États membres à cet exercice de cartographie et qu'elle «évaluerait soigneusement» les réponses. Sur la base de cet exercice de cartographie, **la Commission réfléchira aux options dont elle dispose pour réglementer l'utilisation des logiciels espions dans les États membres.** Toutefois, aucune échéance spécifique n'est prévue pour l'évaluation de la Commission, «compte tenu du caractère évolutif et sensible de l'évaluation». La Commission a également indiqué qu'elle suivrait de très près les conclusions de la commission PEGA.

Les députés estiment que le Parlement, la Commission et le Conseil ont **le pouvoir et le devoir de légiférer, de réglementer et de faire respecter la législation**, et ils doivent le faire avec vigueur et ambition, en plaçant la défense de notre démocratie au-dessus des considérations politiques courtermistes.

L'utilisation de logiciels espions devrait toujours être proportionnée et autorisée par un pouvoir judiciaire indépendant, ce qui n'est malheureusement pas le cas dans certaines régions d'Europe. Un contrôle plus strict au niveau de l'UE est nécessaire pour s'assurer que l'utilisation de logiciels espions soit l'exception, pour enquêter sur les crimes graves, et non la norme.