**Suite donnée à la résolution non législative du Parlement européen sur l’absence de suites législatives données par la Commission à la résolution sur l'utilisation de Pegasus**

1. **Résolution présentée conformément à l’article 123, paragraphe 2, du règlement intérieur du Parlement européen**
2. **Numéros de référence:** [2023/2988 (RSP)](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2023/2988(RSP)) / B9-0464/2023 / P9\_TA(2023)0440
3. **Date d'adoption de la résolution:** 23 novembre 2023
4. **Commission parlementaire compétente:** sans objet
5. **Analyse/évaluation succincte de la résolution et des demandes qu’elle contient:**

Le Parlement européen déplore vivement que la Commission n’ait pas pris de mesures d’exécution ni assuré le suivi législatif de la recommandation du Parlement du 15 juin 2023 à la suite de 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. Le Parlement adresse une mise en garde à cet égard, appelant à ne pas négliger les menaces que l’utilisation abusive de logiciels espions fait peser sur les citoyens et la démocratie dans l’Union et prie la Commission de présenter sans retard un plan de mesures visant à prévenir l’utilisation abusive de logiciels espions dans l’Union, en tirant pleinement parti de tous les moyens législatifs et non législatifs disponibles prévus par les traités européens. Le Parlement demande aussi une nouvelle fois à la Commission d’évaluer, d’ici au 30 novembre 2023, le respect des conditions spécifiques pour Chypre, la Grèce, la Hongrie, la Pologne et l’Espagne, énoncées dans la recommandation.

1. **Réponse à ces demandes et aperçu des mesures que la Commission a prises ou envisage de prendre:**

La Commission condamne fermement tout accès illégal aux communications interpersonnelles et autres données stockées sur les appareils des utilisateurs, quels qu'en soient les auteurs. Toute tentative d’accès illégal aux données des citoyens, y compris des journalistes et des opposants politiques, si avérée, est inacceptable. Les logiciels espions sont des technologies particulièrement intrusives qui, si elles sont employées dans des conditions injustifiées ou disproportionnées, ou à mauvais escient, vont à l’encontre de nos valeurs fondamentales. C’est pourquoi il est absolument capital que les règles du marché intérieur et les droits fondamentaux au respect de la vie privée, à la protection des données et à la liberté d’expression, tels que consacrés par le droit de l’Union, soient pleinement respectés partout dans l’Union.

La Commission prend acte de la demande du Parlement de présenter un plan de mesures visant à prévenir l’utilisation illicite de logiciels espions dans l’UE.

La Commission rappelle entre autres que la liberté de fournir et de recevoir des services, garantie par l’article 56 du traité sur le fonctionnement de l'Union européenne (TFUE), est applicable. En effet, la liberté des prestataires de services, tels que les journalistes, les avocats, les hommes d’affaires et, en réalité, de tout opérateur économique détenant des informations sensibles ou confidentielles, peut être entravée si ces personnes sont la cible d’un logiciel espion. Étant donné le caractère invasif des logiciels espions tels que Pegasus, dans la mesure où il existe de façon avérée ou probable une dimension transfrontalière, il peut être considéré que la simple possibilité de pirater l’appareil d’une personne à l’aide d'un logiciel espion est susceptible de gêner son activité et donc, constitue pour elle une restriction à la libre prestation de services. Les restrictions à une liberté fondamentale sont acceptables seulement si elles sont non discriminatoires, justifiées par une raison impérieuse d’intérêt général et proportionnées et si elles respectent la sécurité juridique et les droits fondamentaux garantis par la charte des droits fondamentaux de l’Union européenne.

La Commission a cherché à intégrer la nécessité d’aborder cette question dans plusieurs propositions législatives récentes. Celles-ci visent à la fois à prévenir les risques que des logiciels espions tombent entre de mauvaises mains et à renforcer la protection des victimes potentielles de ces logiciels.

La **législation européenne sur la liberté des médias**, sur laquelle les colégislateurs sont parvenus à un accord politique provisoire adopté par le Parlement le 13 mars 2024, introduit notamment de solides garde-fous pour les fournisseurs de services de médias, y compris les journalistes, contre les logiciels de surveillance intrusifs. Elle comprend également, en son article 4, une interdiction générale d’utiliser ces logiciels, à laquelle il ne peut être dérogé que dans des cas bien déterminés, pour des enquêtes sur des formes graves de criminalité, dans des conditions strictes, notamment en dernier recours. Cette étape législative importante témoigne de l’engagement de la Commission à protéger la liberté des médias, mais aussi à défendre les droits fondamentaux contre l’utilisation abusive de logiciels espions au sein de l’UE.

La **directive vie privée et communications électroniques** interdit l’interception de communications, le stockage d’informations dans un équipement terminal et l’accès à celles-ci sans le consentement préalable de l’utilisateur concerné. Cette directive ne s’applique pas aux activités des autorités étatiques dans les domaines de la défense et de la sécurité nationale n’incluant pas d’activités de traitement de données d’entités privées. Lorsque la directive vie privée et communications électroniques ne s’applique pas, les États membres sont, en tout état de cause, tenus par les garanties prévues par les autres instruments juridiques de l’Union et, selon le cas, par la Convention européenne des droits de l’homme et par leur droit national.

De plus, le **règlement sur la cyberrésilience**, sur lequel les colégislateurs sont parvenus à un accord politique provisoire adopté par le Parlement le 12 mars 2024, a pour but d’établir des exigences en matière de cybersécurité pour l’accès au marché européen de matériels et logiciels, et fixe des obligations correspondantes pour les fabricants de ces produits. Ces exigences permettront ainsi de réduire la surface d’attaque du matériel et des logiciels que tentent d’exploiter les logiciels espions.

La Commission poursuit également ses efforts pour renforcer le contrôle des exportations de biens de cybersurveillance de l’UE vers des pays tiers au moyen d'une mise en œuvre effective du **règlement** modernisé **sur les biens à double usage** de 2021. Aucun de ces biens de cybersurveillance ne peut quitter le territoire de l’UE sans une autorisation (ou licence) d’exportation émise par une autorité compétente d’un État membre.

La Commission travaille également sur une **initiative non législative clarifiant l’interaction entre le droit de l’Union, en particulier en ce qui concerne la protection des données, et les objectifs de sécurité nationale lors de l’utilisation de logiciels espions**.

En ce qui concerne la demande du Parlement d’évaluer le respect des conditions spécifiques pour plusieurs États membres, la Commission aimerait rappeler qu’elle ne dispose d’aucun pouvoir d’enquête et qu’elle ne peut, par conséquent, pas évaluer si la sécurité nationale était en jeu dans des cas particuliers. La Commission ne dispose d’aucun accès aux dossiers pertinents, n’a pas compétence dans ce domaine et peut uniquement examiner les garanties qui sont en place au niveau national. La Commission attend des autorités et juridictions nationales compétentes qu’elles fassent pleinement usage de leurs pouvoirs pour enquêter de manière approfondie sur les allégations relatives à des activités de surveillance illégales.