Recommandation à l'intention du Conseil européen et de la Commission 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

2023/2500(RSP) - 15/06/2023 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 411 voix pour, 97 voix contre et 37 abstentions, une recommandation au Conseil et à la Commission suite à l'enquête sur les allégations d'infractions et de mauvaise administration dans l'application du droit de l'Union en ce qui concerne l'utilisation de Pegasus et de logiciels espions de surveillance équivalents.

Le Parlement a souligné l'importance indéniable de la protection de la vie privée, du droit à la dignité, de la vie privée et familiale, de la liberté d'expression et d'information, de la liberté de réunion et d'association, et du droit à un procès équitable. Elle a souligné que les violations de ces droits et libertés fondamentaux sont déterminantes pour le respect des principes juridiques communs énoncés dans les traités et que la démocratie elle-même est en jeu, car l'utilisation de logiciels espions contre des hommes politiques, des acteurs de la société civile et les journalistes a un effet dissuasif et porte gravement atteinte au droit de réunion pacifique, à la liberté d'expression et à la participation à la vie publique.

La recommandation a **condamné fermement l’utilisation de logiciels espions** par les pouvoirs publics d’ États membres ou par des agents d’autorités ou d’institutions publiques en vue de surveiller, de faire chanter, d’intimider, de manipuler et de discréditer l’opposition, les voix discordantes et la société civile, de neutraliser le contrôle démocratique et la presse libre, de manipuler les élections et de compromettre l’ état de droit en ciblant des juges, des procureurs et des avocats à des fins politiques.

Absence de réponse aux attaques

Le Parlement a noté **l'inadéquation fondamentale de la structure de gouvernance actuelle de l'Union** pour répondre aux attaques contre la démocratie, les droits fondamentaux et l'État de droit à l'intérieur de l'Union, ainsi que l'absence de mesures prises par de nombreux États membres. Il est également préoccupé par l’apparente **réticence à enquêter** sur l’utilisation abusive de logiciels espions, que le suspect soit une institution publique de l’Union ou d’un pays tiers.

Le cadre juridique de certains États membres ne fournit pas de garanties précises, efficaces et complètes pour ce qui est d’ordonner et de mettre en œuvre des mesures de surveillance ainsi que d’éventuels mécanismes de recours contre ces mesures.

Le Parlement a regretté que les gouvernements des États membres, le Conseil et la Commission **n'aient pas coopéré pleinement** avec la commission d'enquête et n'aient pas partagé toutes les informations pertinentes et significatives, afin d'aider la commission d'enquête à remplir ses tâches, comme indiqué dans son mandat. Il en conclut que ni les États membres, ni le Conseil, ni la Commission ne semblaient

vouloir tout mettre en œuvre pour faire toute la lumière sur le recours abusif à des logiciels espions, et qu' ils protègent ainsi sciemment des gouvernements de l'Union qui portent atteinte aux droits de l'homme à l' intérieur et à l'extérieur de l'Union.

Infractions graves et mauvaise administration dans l'application du droit de l'Union en Pologne, Hongrie, Grèce, Espagne et Chypre

Le Parlement a demandé à la **Hongrie et à la Pologne** de se conformer aux arrêts de la Cour européenne des droits de l'homme et de rétablir l'indépendance judiciaire et les organes de contrôle. Les deux pays devraient également garantir une autorisation judiciaire indépendante et spécifique avant de déployer des logiciels espions, lancer des enquêtes crédibles sur les cas d'abus et garantir que les citoyens ont accès à des recours juridiques significatifs.

Le gouvernement **grec** est invité à rétablir et à renforcer d'urgence les garanties institutionnelles et juridiques, à abroger les licences d'exportation qui ne sont pas conformes à la législation de l'UE en matière de contrôle des exportations et à respecter l'indépendance de l'Autorité hellénique pour la sécurité des communications et la protection de la vie privée.

Notant que **Chypre** a servi de plaque tournante pour l'exportation de logiciels espions, le Parlement a déclaré qu'il devrait abroger toutes les licences d'exportation qui ne sont pas alignées sur la législation de l'UE.

Les **autorités espagnoles** devraient garantir des enquêtes complètes, équitables et efficaces, en particulier dans les 47 affaires où il n'est pas clair si les personnes concernées ont été ou non visées par l'agence nationale de renseignement espagnole. Les autorités espagnoles devraient également veiller à ce que les personnes ciblées disposent de véritables recours juridiques, selon la recommandation.

Des règles pour prévenir les abus

Si la lutte contre la grande criminalité et le terrorisme est d'une importance cruciale pour les États membres, la protection des droits fondamentaux et de la démocratie est essentielle. Le Parlement a souligné que l'utilisation de logiciels espions par les États membres doit **être proportionnée, ne doit pas être arbitraire et que la surveillance ne doit être autorisée que dans des circonstances étroitement déterminées à l'avance**.

En raison de la dimension transnationale et européenne de l'utilisation des logiciels espions, un contrôle coordonné et transparent au niveau de l'UE est nécessaire pour garantir non seulement la protection des citoyens de l'UE, mais aussi la validité des preuves recueillies au moyen de logiciels espions dans les affaires transfrontalières. Il existe un besoin évident de **normes européennes communes** réglementant l'utilisation des logiciels espions par les organismes des États membres.

La recommandation souligne que les logiciels espions ne peuvent être mis sur le marché que pour être vendus et utilisés par les autorités publiques, sur la base d'une liste fermée, dont les mandats comprennent des enquêtes sur des infractions ou la protection de la sécurité nationale, ce pour quoi l'utilisation de logiciels espions peut être autorisée, et utilisés par celles-ci. Les agences de sécurité ne devraient utiliser les logiciels espions que lorsque toutes les recommandations formulées par l'Agence des droits fondamentaux ont été mises en œuvre.

Le Parlement a conclu que lorsqu'un État membre a acheté un logiciel espion, l'acquisition doit pouvoir être **contrôlée par un organisme d'audit indépendant et impartial** doté de l'habilitation adéquate. La Commission est invitée à mener une enquête approfondie sur toutes les allégations et suspicions d'utilisation de logiciels espions à l'encontre de ses fonctionnaires, et à faire rapport au Parlement et aux autorités compétentes chargées de l'application de la loi, le cas échéant.

Coopération internationale pour protéger les citoyens

Le Parlement a demandé l'adoption d'une **stratégie commune UE-États-Unis** en matière de logiciels espions, comprenant une liste blanche et/ou une liste noire commune(s) de fournisseurs de logiciels espions à risques dont les outils ont été utilisés de manière abusive ou risquent d'être utilisés de manière abusive par des gouvernements étrangers faisant état de piètres résultats en matière de droits de l'homme pour cibler dans une intention malveillante des agents d'État, des journalistes ou la société civile, et qui agissent contre la sécurité nationale et la politique étrangère de l'Union, autorisés ou non à vendre aux autorités publiques, des critères communs permettant d'inclure les fournisseurs dans l'une ou l'autre liste, des accords en vue de la création d'un rapport commun sur le secteur, un examen commun, des obligations communes en matière de devoir de vigilance des fournisseurs et la criminalisation de la vente de logiciels espions à des acteurs non étatiques.

Protection de la vie privée

La recommandation appelle à la protection de toutes les communications électroniques, du contenu et des métadonnées contre l'utilisation abusive des données personnelles et des communications privées par les entreprises privées et les autorités gouvernementales. Le Parlement a souligné que les outils de sécurité numérique dès la conception, tels que le **cryptage de bout en bout**, ne devraient pas être affaiblis.

La Commission devrait évaluer la mise en œuvre par les États membres de la directive «vie privée et communications électroniques» dans l'ensemble de l'UE et entamer des procédures d'infraction en cas de violation.

Laboratoire technologique de l'UE

La Commission est invitée à entreprendre sans plus attendre la création d'un **institut interdisciplinaire de recherche indépendant pour l'Union**, axé sur la recherche et le développement relatifs aux enjeux liés aux technologies de l'information et de la communication, aux droits fondamentaux et à la sécurité. Le laboratoire devrait être mis en place en étroite collaboration avec l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-EU) et l'ENISA. Un financement adéquat devrait être assuré et il est recommandé à la Commission de proposer un système de certification pour l'analyse et l'authentification de matériel scientifique.

Action législative

La Commission devrait rapidement présenter des propositions législatives sur la base de cette recommandation.