DÉCISIONS

DÉCISION (UE) 2022/480 DU PARLEMENT EUROPÉEN

du 10 mars 2022

sur la constitution, l'objet de l'enquête, les compétences, la composition numérique et la durée du mandat de la commission d'enquête chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents

LE PARLEMENT EUROPÉEN,

— vu la demande présentée par 290 députés visant à la constitution d'une commission d'enquête chargée d'examiner et d'enquêter sur les allégations d'infraction au droit de l'Union ou de mauvaise administration dans l'application de celui-ci, en ce qui concerne l'utilisation de Pegasus et de logiciels espions de surveillance équivalents installés sur des appareils mobiles en exploitant les vulnérabilités informatiques (ci-après dénommés «logiciels espions de surveillance équivalents»),

— vu la proposition de la Conférence des présidents,

— vu l'article 226 du traité sur le fonctionnement de l'Union européenne,

— vu la décision 95/167/CE, Euratom, CECA du Parlement européen, du Conseil et de la Commission du 19 avril 1995 portant modalités d'exercice du droit d'enquête du Parlement européen ([1]),

— vu l'attachement de l'Union européenne aux valeurs et aux principes de la liberté, de la démocratie et du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'état de droit, tels qu'ils sont énoncés dans le préambule du traité sur l'Union européenne, et notamment aux articles 2, 6 et 21 dudit traité,

— vu l'article 4, paragraphe 2, du traité sur l'Union européenne, qui réaffirme la compétence exclusive des États membres en matière de maintien de l'ordre public et de sauvegarde de la sécurité nationale,

— vu les articles 16 et 223 du traité sur le fonctionnement de l'Union européenne,

— vu la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), et notamment ses articles 7, 8, 11, 21 et 47, qui reconnaissent les droits, libertés et principes spécifiques qui y sont énoncés, tels que le respect de la vie privée et familiale et la protection des données à caractère personnel, la liberté d'expression et d'information, le droit à la non-discrimination, ainsi que le droit à un recours effectif et à accéder à un tribunal impartial, et qui s'appliquent pleinement aux États membres lorsqu'ils mettent en œuvre le droit de l'Union, et son article 52, paragraphe 1, qui autorise une certaine limitation de l'exercice des libertés et droits fondamentaux,

— vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») ([2]),

— vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([3]),

— vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ([4]),

([1]) JO L 113 du 19.5.1995, p. 1.
([2]) JO L 201 du 31.7.2002, p. 37.
([3]) JO L 119 du 4.5.2016, p. 1.
([4]) JO L 119 du 4.5.2016, p. 89.

— vu la décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres ([5]), telle que modifiée par la décision (PESC) 2021/796 du Conseil du 17 mai 2021 ([6]),

— vu le règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage ([7]),

— vu l'acte portant élection des membres du Parlement européen au suffrage universel direct ([8]),

— vu la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et notamment ses articles 8, 9, 13 et 17, ainsi que ses protocoles,

— vu les principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme ([9]),

— vu sa résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures ([10]), ainsi que ses recommandations concernant le renforcement de la sécurité informatique au sein des institutions, organes et agences de l'Union,

— vu l'article 208 de son règlement intérieur,

A. considérant qu'il a récemment été révélé que plusieurs pays, y compris des États membres, ont utilisé le logiciel espion de surveillance Pegasus à l'encontre de journalistes, de responsables politiques, d'agents des services répressifs, de diplomates, d'avocats, d'hommes et femmes d'affaires, d'acteurs de la société civile et d'autres acteurs, et que ces pratiques sont extrêmement alarmantes et semblent confirmer les dangers de l'usage abusif des technologies de surveillance au détriment des droits de l'homme et de la démocratie;

1. décide de constituer une commission d'enquête pour examiner les allégations d'infraction au droit de l'Union ou de mauvaise administration dans l'application de celui-ci, en ce qui concerne l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, sans préjudice des compétences des juridictions nationales ou de l'Union;

2. décide que la commission d'enquête sera chargée:

— d'enquêter sur la portée des allégations d'infraction au droit de l'Union ou de mauvaise administration dans l'application de celui-ci découlant de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, de recueillir des informations sur la mesure dans laquelle les États membres, notamment la Hongrie et la Pologne, ou des pays tiers, recourent à une surveillance intrusive au point de violer les droits et libertés consacrés par la Charte, et d'évaluer le niveau de risque que cela représente pour les valeurs consacrées à l'article 2 du traité sur l'Union européenne, telles que la démocratie, l'état de droit et le respect des droits de l'homme;

— en vue de l'accomplissement de son mandat, de recueillir et d'analyser les informations permettant de déterminer:

— l'utilisation et le fonctionnement de Pegasus et de logiciels espions de surveillance équivalents et leur incidence négative présumée sur les droits fondamentaux garantis par la Charte, lors de la mise en œuvre du droit de l'Union par les États membres,

— le cadre juridique existant dans lequel les États membres ont acquis et utilisé Pegasus et des logiciels espions de surveillance équivalents,

— si les autorités des États membres ont utilisé Pegasus et des logiciels espions de surveillance équivalents à des fins politiques, économiques ou à d'autres fins injustifiées pour espionner des journalistes, des responsables politiques, des agents des services répressifs, des diplomates, des avocats, des hommes et femmes d'affaires, des acteurs de la société civile ou d'autres acteurs, en violation du droit de l'Union et des valeurs consacrées à l'article 2 du traité sur l'Union européenne ou des droits consacrés par la Charte,

([5]) JO L 129 I du 17.5.2019, p. 13.
([6]) JO L 174 I du 18.5.2021, p. 1.
([7]) JO L 206 du 11.6.2021, p. 1.
([8]) JO L 278 du 8.10.1976, p. 5.
([9]) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_FR.pdf
([10]) JO C 378 du 9.11.2017, p. 104.

— si l'utilisation, en violation du droit de l'Union, de Pegasus et de logiciels espions de surveillance équivalents a eu une incidence négative sur les processus démocratiques dans les États membres en ce qui concerne les élections aux niveaux local, national et européen,

— les allégations d'infraction à la directive 2002/58/CE ou de mauvaise administration par les États membres, découlant de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, en particulier en ce qui concerne le principe de confidentialité des communications et l'interdiction d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes de personnes, ou de les soumettre à tout autre moyen d'interception ou de surveillance,

— si l'utilisation de Pegasus et de logiciels espions de surveillance équivalents par les États membres a constitué, entraîné ou révélé des violations de la directive (UE) 2016/680 et du règlement (UE) 2016/679,

— si la Commission disposait de preuves de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents à l'encontre de personnes,

— si les États membres ont donné des garanties institutionnelles et juridiques suffisantes pour éviter l'utilisation illégale de logiciels espions et si les personnes qui soupçonnent que leurs droits ont été violés par l'utilisation de logiciels espions ont accès à un recours effectif,

— la prétendue absence d'action des États membres en ce qui concerne la participation d'entités dans l'Union au développement, à la diffusion ou au financement de Pegasus et de logiciels espions de surveillance équivalents, y compris la chaîne d'approvisionnement sur le plan des technologies et de leur exploitation, dans la mesure où cela enfreint le droit de l'Union, y compris le règlement (UE) 2021/821, et notamment lorsque des logiciels de surveillance commercialisés à certaines fins (par exemple, la lutte contre le terrorisme) sont utilisés dans un autre contexte,

— le rôle du gouvernement d'Israël et d'autres pays tiers dans la fourniture aux États membres de Pegasus et de logiciels espions de surveillance équivalents,

— si l'utilisation de Pegasus ou de logiciels espions de surveillance équivalents par les autorités des États membres a entraîné le transfert de données à caractère personnel vers des pays tiers, en particulier, mais pas uniquement, vers le groupe NSO, ainsi que les gouvernements de pays tiers,

— si l'utilisation de Pegasus ou de logiciels espions de surveillance équivalents, impliquant directement ou indirectement des entités liées à l'Union, a contribué à l'espionnage illégal de journalistes, de responsables politiques, d'agents des services répressifs, de diplomates, d'avocats, d'hommes et femmes d'affaires, d'acteurs de la société civile ou d'autres acteurs dans des pays tiers, et si cela a donné lieu à des violations des droits de l'homme ou à d'autres atteintes aux droits de l'homme qui suscitent de graves préoccupations en ce qui concerne les objectifs de la politique étrangère et de sécurité commune de l'Union, et si cette utilisation était contraire aux valeurs consacrées par l'article 21 du traité sur l'Union européenne et par la Charte, également compte dûment tenu des principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme et d'autres droits consacrés par le droit international relatif aux droits de l'homme,

— s'il existait des motifs suffisants pour que le Conseil adopte des mesures restrictives ou des sanctions dans le cadre de la politique étrangère et de sécurité commune de l'Union à l'encontre d'un ou de plusieurs pays tiers lorsqu'une décision, adoptée conformément au titre V, chapitre 2, du traité sur l'Union européenne, prévoyait l'interruption ou la réduction des relations économiques ou financières, conformément à l'article 215, paragraphe 1, du traité sur le fonctionnement de l'Union européenne,

— si l'utilisation de Pegasus ou de logiciels espions de surveillance équivalents par des pays tiers a eu une incidence sur les droits fondamentaux garantis par le droit de l'Union et s'il existait des motifs suffisants pour que le Conseil réévalue des accords de coopération internationale relevant de l'espace de liberté, de sécurité et de justice conclus avec des pays tiers en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne;

— de formuler toutes les recommandations qu'elle jugera nécessaires en la matière;

— de formuler des recommandations pour protéger les institutions de l'Union, ses membres et son personnel contre ce type de logiciels espions de surveillance;

3. décide que la commission d'enquête déposera son rapport final dans un délai de 12 mois à compter de l'adoption de la présente décision;
4. décide qu'il appartiendra à la commission d'enquête de tenir compte, dans ses travaux, de toute évolution pertinente entrant dans le champ de son mandat pendant la durée de celui-ci;
5. souligne qu'afin d'assurer une bonne coopération et un bon flux d'informations entre la commission d'enquête et les commissions permanentes et sous-commissions concernées, le président et le rapporteur de la commission d'enquête pourraient être associés aux débats pertinents des commissions permanentes et sous-commissions, et inversement, en particulier pour les auditions de la commission d'enquête;
6. décide que toute recommandation formulée par la commission d'enquête sera transmise aux commissions permanentes et sous-commissions concernées dans leurs domaines de compétence respectifs, tels que définis à l'annexe VI du règlement intérieur;
7. décide que la commission d'enquête comptera 38 membres;
8. charge sa présidente d'assurer la publication de la présente décision au *Journal officiel de l'Union européenne*.