ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 13030	De **Mme Sylvie Ferrer** (La France insoumise - Nouvelle Union Populaire écologique et sociale - Hautes-Pyrénées)	**Question écrite**
Ministère interrogé > Europe et affaires étrangères	**Ministère attributaire** > Europe et affaires étrangères	
Rubrique >droits fondamentaux	**Tête d'analyse** >Logiciels espions	**Analyse** > Logiciels espions.
Question publiée au JO le : **21/11/2023** Réponse publiée au JO le : **20/02/2024** page : **1244** Date de changement d'attribution : **12/01/2024**		

Texte de la question

Mme Sylvie Ferrer interroge Mme la ministre de l'Europe et des affaires étrangères sur l'usage des logiciels espions. Depuis plusieurs années, des organisations des défense des droits humains alertent sur la crise liée à la surveillance numérique, qui représente une menace pour les droits humains partout dans le monde. Le scandale Pegasus a révélé comment des États ont ciblé des journalistes, des militants, des avocats et des personnalités politiques en ayant recours au logiciel espion Pegasus. Plusieurs journalistes français ont ainsi été illégalement espionnés - des infections confirmées par les autorités françaises - tandis que le président Emmanuel Macron, le Premier ministre d'alors, Edouard Philippe, et quatorze ministres faisaient partie des cibles potentielles en 2019. Deux ans plus tard, le scandale des *Predator Files* a révélé que des membres de la société civile, des journalistes, des personnalités politiques et des universitaires dans l'Union européenne (UE), aux États-Unis d'Amérique et en Asie ont été les cibles d'attaques révoltantes menées au moyen du logiciel espion Predator. Ce logiciel est développé et commercialisé par l'alliance Intellexa, basée en Europe et dont fait partie le groupe français Nexa. Les instruments actuels tels que l'arrangement de Wassenaar ou le règlement de l'Union européenne sur les exportations des biens à double usage ainsi que les initiatives non contraignantes comme les codes de conduite volontaire, ne permettent pas une réelle protection des droits humains, qui nécessite une réglementation encadrant strictement les pratiques et les transferts de ces technologies. Au regard des dangers que représentent ces outils de surveillance pour les droits humains, elle souhaiterait savoir si la France soutient l'interdiction des logiciels espions hautement intrusifs ainsi que l'appel au moratoire mondial sur l'utilisation, la vente, l'exportation et le transfert de ces technologies concernant les autres logiciels espions.

Texte de la réponse

La France a publiquement fait savoir que l'utilisation de logiciels espions à des fins de surveillance ciblée illégale constituait un acte d'une extrême gravité et que toute tentative d'espionnage à l'encontre de journalistes ou de parlementaires était inacceptable. De telles pratiques peuvent conduire à de sérieuses violations des droits de l'Homme et des libertés fondamentales. Dans ce contexte, la France joue un rôle de premier plan pour proposer un cadre de régulation des usages de ces capacités, avec ses partenaires affinitaires et au-delà. Elle s'est activement mobilisée pour l'élaboration et l'adoption de la Déclaration conjointe relative aux efforts visant à lutter contre la prolifération et l'usage abusif des logiciels espions commerciaux, rendue publique le 30 mars 2023, à l'occasion du deuxième Sommet pour la démocratie. L'Australie, le Canada, le Costa Rica, le Danemark, les États-Unis, la Norvège, la Nouvelle-Zélande, le Royaume-Uni, la Suède et la Suisse ont également apporté leur signature. À ce titre, la France s'est engagée à empêcher l'exportation de logiciels espions à des utilisateurs finaux susceptibles de

les utiliser dans le cadre d'activités cyber malveillantes, en prévenant notamment toute intrusion non autorisée dans un système d'information, conformément à nos cadres juridiques, réglementaires et politiques respectifs ainsi qu'à nos régimes de contrôle des exportations existants en la matière. Toute action dérogeant à ce cadre ne peut être tolérée. Au-delà des seuls logiciels espions, la France considère que la commercialisation croissante de capacités cyber offensives privées renforce et élargit la menace cyber. Dans ce contexte, limiter la prolifération des technologies cyber offensives est un enjeu-clé pour les droits humains, notre sécurité nationale et la stabilité du cyberespace. Face à un phénomène d'ampleur mondiale, la France appelle à une réponse internationale large, au-delà de l'Union européenne. Conformément à la déclaration bilatérale du 36e sommet franco-britannique du 10 mars 2023, la France est engagée, avec le Royaume-Uni, pour promouvoir une initiative internationale visant à édicter des normes de comportement responsable et à lutter contre la prolifération d'outils et de services cyber offensifs. Dans le cadre de cette initiative, la France travaille à sensibiliser ses partenaires à la menace représentée par la croissance du marché des capacités cyber pouvant être utilisées à des fins offensives et à construire un consensus international sur le sujet. Dans la continuité des discussions multi-acteurs tenues à l'occasion de la 6e édition du Forum de Paris sur la paix, la France co-organise, avec le Royaume-Uni, à Londres, en février 2024, une conférence internationale sur la lutte contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché, pour proposer un cadre à la commercialisation de ces capacités. En parallèle, la France mobilise la communauté de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, qui fédère plus de 80 États, 36 organismes publics et administrations territoriales, 390 organisations et membres de la société civile et plus de 700 entreprises et entités du secteur des technologies, pour apporter une expertise multi-acteurs aux discussions internationales sur le sujet. Alors qu'une fenêtre de négociation est rendue possible, un soutien à l'interdiction des logiciels espions hautement intrusifs et à un moratoire mondial sur l'utilisation, la vente, l'exportation et le transfert de ces technologies porterait le risque d'isoler la position de la France, au moment où elle s'attache à construire un cadre consensuel sur la nécessité de réguler le marché des capacités cyber offensives disponibles sur le marché.