Illustration : montage CdJ d'après images sources K. Rosas et al.

POINT DE VUE

Logiciels espions : un danger pour les investigations de journalistes ?

Longtemps utilisés officieusement par les États ou les entreprises pour surveiller les journalistes, les logiciels espions sont en passe d'être officiellement autorisés par l'UE dans 32 types d'enquêtes. Serions-nous face au début de la fin des enquêtes journalistiques ? Par ***Catherine Zemmouri***

De tout temps, les journalistes ont accordé une grande attention aux actes d'espionnage les visant et la question s'est posée tout récemment de savoir comment ils devaient se comporter afin d'empêcher les logiciels espions d'accéder à leurs informations et à leurs sources ; d'autant que ce sont surtout les enquêtes sensibles et d'intérêt public qui sont souvent visées par l'usage de logiciels espions.

Les problèmes et les enjeux liés aux logiciels espions ont resurgi récemment avec une certaine acuité, après la découverte de l'utilisation du logiciel Pegasus par le gouvernement marocain contre notamment quelques journalistes français. Dans un contexte marqué par l'augmentation de l'espionnage et des gardes à vue de journalistes, souvent sous couvert de protection de secret défense, de risques sécuritaires ou encore d'enquête judiciaire, le logiciel Pegasus a provoqué une onde de choc au sein des journalistes, car ce logiciel a des conséquences particulièrement dommageables pour ces derniers. Sans compter que sous peu, l'application du Media Freedom Act européen risque d'aggraver la situation, puisqu'il autorise l'utilisation de logiciels espions par les gouvernements de l'UE contre les journalistes dans trente-deux cas.

Précisons que jamais encore, la France, n'avait accordé d'autorisation, même exceptionnelle, d'utiliser des logiciels espions contre les journalistes. Le MFAE introduit donc une première dans le système juridique français.

L'autorisation de l'UE ouvre une brèche qui limitera certes certains pays dans lesquels les régimes politiques sont peu respectueux du respect des droits des journalistes, comme la Hongrie ou la Pologne, et qui ne pourront plus espionner les journalistes que dans trente-deux cas. Mais pour les autres pays européens, le MFAE est une autorisation à espionner les journalistes qui n'existait pas auparavant.

Pour les autres pays européens, le Media Freedom Act européen est une autorisation à espionner les journalistes qui n'existait pas auparavant.

Dans les faits, les journalistes sont démunis face à de tels moyens techniques déployés. La meilleure façon d'éviter une surveillance par des logiciels espions serait, pour ces derniers, de ne pas être équipés de téléphones portables et d'ordinateurs. Une solution difficilement envisageable à l'ère de l'hyper connectivité. Un téléphone basique, sans internet, avec une carte prépayée, utilisable une seule fois, reste une solution mais cette technique dite du « burner » pourrait s'avérer néanmoins trop onéreuse. Et la généralisation du numérique a considérablement élargi le champ de la collecte de l'information dans le domaine du renseignement : téléphone, cookies, Ok Google qui vous écoute, etc., le défi est devenu très important pour les journalistes. Comment protéger ses informations et ses sources face à cette visibilité quasi permanente et instantanée ? Car les journalistes doivent poursuivre « leur mission de chien de garde de la démocratie » assignée par la CEDH dans différents arrêts.

Rappelons quelques-unes des affaires les plus importantes révélées par des enquêtes de journalistes afin de bien comprendre les enjeux. L'affaire du Mediator n'a été possible que par l'enquête du *Figaro* révélant que 500 à 1000 décès étaient liés à la prise de Benfluorex commercialisé sous le nom de Mediator par les laboratoires Servier de 1976 à 2009. L'affaire du sang contaminé que le *Canard enchaîné* a fait connaître constitue également un exemple de révélation dans l'intérêt public. En 2012 c'est Mediapart qui révèle l'affaire Cahuzac, du nom du ministre délégué au budget, qui avait détenu des fonds non déclarés sur un compte en Suisse. Les affaires de dopage à l'EPO de Lance Armstrong victorieux, révélées par L'Équipe en 2005 est un autre exemple. Le domaine du secret défense est également visé. En octobre 2018, une procédure pour compromission du secret défense national ouverte contre deux journalistes du *Monde* est classée sans suite. Les journalistes mis en cause décrivaient la préparation, en août 2013, d'un bombardement de bases militaires du régime de Bashar Al-Assad. Ce document était classé « confidentiel défense ». Le média Disclose est quant à lui à l'origine, après des mois d'enquête, de la révélation de l'utilisation d'armes françaises vendues à l'Arabie saoudite dans le conflit au Yémen.

Des enquêtes qui seraient difficiles à mener si des logiciels espions étaient utilisés contre les journalistes.

Pegasus, le cauchemar des journalistes d'investigation

Parmi toutes les techniques de surveillance la plus redoutable pour un journaliste est celle de l'usage d'un logiciel espion. Dans ce groupe, le logiciel Pegasus est considéré comme le plus malveillant.

L'affaire Pegasus, qui a éclaté en juillet 2021, est révélatrice des avancées continuelles en matière de technologie de surveillance. La société israélienne NSO a mis au point un système de surveillance qui ne se contente pas d'écouter les conversations mais qui opère un véritable « pillage » des données se trouvant dans le téléphone visé : Photos, textes, répertoire téléphonique, applications, échanges internet, mais aussi, et surtout, tout le contenu des messageries, dont les messages cryptés de type WhatsApp ou Signal. En fait, l'interception ne se déroule pas après envoi, elle se produit, au contraire, avant, au moment où le texte du message est tapé. Et le logiciel Pegasus peut aller encore plus loin puisqu' il

est capable de déclencher à tout moment une écoute via le micro du téléphone portable, de prendre des photos, ou encore de déclencher la caméra ou la géolocalisation de l'appareil.

Pegasus dispose d'autres avantages pour les autorités qui l'utilisent, d'abord il est invisible pour le propriétaire du téléphone portable visé. Il peut aussi s'installer dans le téléphone tout seul ! Ses nouvelles capacités lui permettent d'infecter un iPhone à l'aide de ce qui est appelé technologie « zéro clic », c'est-à-dire sans avoir besoin de piéger l'utilisateur. Le logiciel peut être installé à distance sans participation « active » du propriétaire du téléphone comme l'explique J. Hourdeaux dans un article publié par Mediapart[1]. Inutile de cliquer sur un lien malveillant, car en réalité le logiciel utilise les failles de sécurité du téléphone pour entrer dans le système du téléphone et « aspirer » les données. Cette nouvelle technologie dépasse donc toutes les précédentes.

Le consortium de journalistes à l'origine des recherches concernant l'affaire Pegasus, le réseau de journalistes de l'ONG Forbidden Stories[2], explique que près de deux cents journalistes étaient visés par ce logiciel espion dont certains résident en France comme Rosa Moussaoui, du journal *l'Humanité*, ou encore le directeur de Mediapart, Edwy Plenel. Mais aussi Dominique Simonnot, l'actuelle Contrôleuse générale des lieux de privation de liberté (CGPL), qui, jusqu'en 2020, était journaliste au *Canard enchaîné*, ou encore Bruno Delport, le directeur de TSF Jazz, qui postulait en 2019 à la présidence de Radio France. D'autres numéros de journalistes apparaissent également, notamment, du *Monde*, de France 2, de France 24.

L'entreprise NSO, comme le relate *Le Monde*, est devenue mondialement célèbre fin 2018. L'entreprise se trouve, en effet, indirectement impliquée dans un scandale majeur : l'assassinat, après utilisation du logiciel Pegasus, le 2 octobre, dans le consulat d'Arabie saoudite en Turquie, du dissident et journaliste et opposant saoudien Jamal Khashoggi. On peut même considérer que d'autres journalistes ont été tués, car leurs meurtriers ont pu utiliser le logiciel espion Pegasus, parmi eux : Javier Valdes, célèbre journaliste mexicain qui enquêtait sur les trafics de drogue dans son pays, tué le 15 mai 2017, selon Mediapart. Cecilio Pineda assassiné en mars 2017, quelques semaines après que son numéro de téléphone soit apparu dans la liste des journalistes qui semblent avoir été visés par le Gouvernement mexicain. Il avait régulièrement condamné les liens entre les élus locaux et les narcotrafiquants.

Tous les journalistes surveillés par le logiciel espion n'ont certes pas été tués, mais les conséquences n'en demeurent pas moins graves pour certains.

Tous les journalistes surveillés par le logiciel espion n'ont certes pas été tués. Mais les conséquences n'en demeurent pas moins graves pour certains, puisque beaucoup sont emprisonnés dans des pays comme au Maroc, en Arabie saoudite, en Russie, au Gabon et dans d'autres pays autoritaires ou dictatoriaux. Après les avoir mis sur écoute et avoir décrypté toutes les informations que comportaient leurs téléphones portables, le gouvernement du Maroc a par exemple purement et simplement inventé des accusations lorsqu'il ne trouvait aucune charge contre les journalistes qui enquêtaient sur la question des droits de la personne dans le pays. La plupart d'entre eux ont été arrêtés et purgent actuellement des peines de prison pour viols ou agressions sexuelles qui n'ont jamais été prouvées[3].

[1] « Pegasus : un outil de surveillance redoutable et hors contrôle », Mediapart [en ligne] mediapart.fr, 20.07.2021.

[2] La mission de Forbidden Stories est de poursuivre et de publier le travail d'autres journalistes qui sont menacés, emprisonnés ou ont été assassinés.

[3] Ainsi selon RSF et Amnesty International : Hicham Mansouri (10 mois de prison, aujourd'hui en exil en France, mais toujours surveillé par les services marocains sur notre territoire), Omar Brousky, Hamid El Mahdaoui, Souleimane Raissouni (5 ans de prison), Taoufik Bouachrine (12 ans de prison), Omar Radi (6 ans de prison), Maati Monjib (trois mois de prison, libéré après

En Inde, ce sont trente journalistes, dont cinq d'investigation, dix chargés de l'information internationale et huit spécialistes en politique, qui ont été les cibles du logiciel espion. Certains d'entre eux avaient enquêté sur le contrat controversé des trente-six avions Rafale vendus en 2016 par la France au gouvernement indien. En Hongrie, pays membre de l'Union européenne, la situation est identique. On retrouve dans la liste des numéros ciblés par Pegasus, dix avocats ainsi que de nombreuses personnalités, dont Zoltan Varga, le patron d'un grand groupe de médias indépendant, et deux journalistes de Direkt36, site d'investigation indépendant basé à Budapest.

À la suite de ces révélations, la Fédération internationale des journalistes a lancé un appel aux journalistes, leur demandant de faire preuve d'une vigilance accrue pour protéger leurs données. Elle a demandé aux États d'inscrire dans leur législation nationale le principe de l'inviolabilité des communications des journalistes et l'interdiction de l'usage de logiciels espions. Edward Snowden pour sa part demande que la vente de logiciels espions soit régulée à travers le monde[4].

Il revient aux États de voter les lois encadrant l'espionnage à l'aide de logiciels espions pour protéger les journalistes.

Selon un article publié dans le *New York Times* de mars 2019, les autorités mexicaines auraient déboursé quinze millions de dollars US pour l'achat du logiciel Pegasus. En d'autres termes, avec une somme faible pour un État, le pays s'équipe selon *Le Monde*, d'une technologie qui dépasse tout ce que le KGB a pu inventer jusqu'alors pour surveiller des journalistes.

La société NSO s'engage pourtant officiellement à ce que les pays demandeurs de sa technologie ne portent pas atteinte aux droits de la personne et qu'elle soit utilisée dans le cadre de la lutte contre le terrorisme ou contre le crime organisé. Mais il n'en est rien d'après l'enquête menée par *Le Monde* et l'organisation Forbidden Stories. Au Mexique, après avoir permis l'arrestation de multiples narcotrafiquants, dont le très célèbre et dangereux Joaquim Guzman, alias « El Chapo », en 2016, le logiciel Pegasus a été utilisé par la suite dans de nombreuses affaires de surveillance de journalistes, activistes des droits de la personne et opposants politiques. En 2020, il s'est même retrouvé utilisé par les narcotrafiquants eux-mêmes, des membres de la police mexicaine ayant semble-t-il discrètement revendu Pegasus à des cartels de la drogue.

En réalité comme tous les défenseurs de journalistes et des droits de la personne l'ont réaffirmé au moment de l'affaire Pegasus, il revient aux États de voter les lois encadrant l'espionnage à l'aide de logiciels espions pour protéger les journalistes. A défaut les juges seront la clé de résolution des problèmes lorsque des plaintes seront déposées. La France est un exemple puisqu'une enquête a été ouverte dans l'affaire Pegasus par le Parquet de Paris le 20 juillet 2022. Une réponse plus globale et politique est espérée mais l'arrivée du MFAE risque fort de changer la donne et de contrer les espoirs de ces derniers, notamment en Europe.

Le dangereux Freedom Media Act européen

La démocratie repose sur le principe fondamental de la liberté d'expression, principe qui garantit à chaque individu le droit de s'exprimer librement, de partager ses opinions et de participer activement à la vie publique. Il ne peut exister de démocratie sans liberté d'expression. Et il n'existe pas de liberté d'expression sans protection des enquêtes journalistiques et des sources du journaliste. L'Union européenne a toujours pleinement adhéré

une grève de la faim), Hajar Raissouni (1 an de prison).

[4] Amnesty international fait partie des nombreuses ONG à exiger un encadrement législatif des ventes de logiciels espions. Pegasus : révélations choc sur un système mondial de surveillance numérique. Communiqué de presse de la Présidente d'Amnesty International France, C. Coudriou, 21.07.2021.

aux valeurs de la démocratie et de la liberté d'expression depuis sa création. Et lorsque Bruxelles a commencé les discussions pour un Media Freedom Act européen à l'américaine en 2022[5], il a toujours été question de respecter la liberté d'expression et l'anonymisation des sources des journalistes : « *Aucun journaliste ne devrait être espionné en raison de son activité* », c'est contre de telles dérives, résumées par la vice-présidente de la Commission Vera Jourova, qu'entendait lutter initialement le règlement européen sur la liberté des médias.

Les règles européennes et le Media Freedom Act européen ont introduit des avancées indéniables dans certains domaines notamment contre les poursuites-baillons ou encore à propos de la législation sur la liberté des médias soutenant l'indépendance éditoriale et le pluralisme des médias, et renforçant la transparence et l'équité qui vise à contrer la montée des extrémistes et le risque d'ingérence étrangère dans les scrutins électoraux.

La France et plusieurs autres États membres ont insisté pour inclure un recours général aux logiciels espions « au nom de la sauvegarde de la sécurité nationale ».

Mais ces avancées, aussi importantes soient-elles, ne suffisent pas. Et l'UE, qui devait apporter des améliorations en matière de protection des sources du journaliste, a fini par céder aux pressions du monde politique et de la France, pour autoriser une surveillance des journalistes par l'utilisation de logiciels espions. Et force est de constater que la nouvelle règle introduite par le Media Freedom Act européen est dangereuse pour la protection des enquêtes menées par les journalistes sur deux points.

L'espionnage par logiciel espion des journalistes français rendu possible par l'UE

D'abord il autorise les États membres de l'UE à surveiller les journalistes en utilisant des logiciels espions. Et après une bataille de plusieurs mois, cette possibilité vise désormais trente-deux situations listées. Et pendant les négociations, la France et plusieurs autres États membres ont insisté pour inclure un recours général aux logiciels espions « *au nom de la sauvegarde de la sécurité nationale* ». Sur la question, il y a donc eu un léger recul des hommes politiques européens, sous la pression des ONG et des syndicats de journalistes même si, rappelons-le, l'usage des logiciels espions à l'encontre des journalistes n'avait encore jamais été autorisé en France.

Cette règle inscrite dans le Media Freedom Act européen constitue une première, et est une catastrophe pour les journalistes, français notamment. Car les logiciels espions sont une atteinte à leur droit et même à leur devoir d'enquête sur des questions sensibles d'intérêt public. Sans ces enquêtes, il ne peut y avoir de révélations d'affaires, de condamnations et par conséquent de démocratie.

Les logiciels espions sont également une entrave à la liberté d'expression et constituent donc une faille dans le système démocratique. Car si l'on donne la possibilité d'espionner des journalistes dans trente-deux situations, pourquoi ne la donnerait-on pas dans cent situations par la suite, voire de façon illimitée très vite ? La brèche est ouverte.

Dans les faits, la liste des trente-deux cas ouvrant droit à l'utilisation de logiciels espions par les gouvernements européens contre les journalistes comporte quasiment tout ce que le Code pénal français connaît

[5] Il a fallu un an et demi de négociations. Présenté le 16 septembre 2022 par la Commission européenne, le règlement sur la liberté des médias a fait l'objet d'un accord entre le Parlement européen et le Conseil de l'Union européenne le 15 décembre 2023. Il a ensuite été formellement adopté le 13 mars 2024 par les eurodéputés, puis le 26 mars 2024 par les États membres de l'UE. Après son entrée en vigueur le 7 mai 2024, plusieurs de ces mesures seront progressivement mises en place jusqu'à la pleine application du texte le 8 août 2025.

comme cause de sanctions graves ou moins graves. Par conséquent, nous sommes en droit de nous demander si ce Freedom Media Act européen ne constituerait pas un blanc-seing donné aux gouvernements de l'UE pour espionner les journalistes de façon générale et permanente par des logiciels espions, sans avoir à se justifier ou presque, même si l'UE s'en défend.

Un blanc-seing donné aux gouvernements de l'UE pour espionner les journalistes de façon générale ?

Le MFAE tente néanmoins, en vain, de baliser l'usage de logiciels espions contre les journalistes en précisant que :

> Les logiciels de surveillance intrusifs ne devraient être déployés que lorsque cela a été justifié par une raison impérieuse d'intérêt général […] ou dans des cas exceptionnels et urgents […]. Ainsi s'agissant spécifiquement du déploiement du logiciel de surveillance intrusif, il convient de s'assurer que l'infraction a atteint un seuil de gravité […] que l'enquête et les poursuites relatives à cette infraction justifient, l'ingérence […] et que l'utilisation du logiciel intrusif est pertinente aux fins de l'établissement des faits liés à l'enquête […].

Ces limites sont posées, car, comme le rappelle l'UE : « *la protection des sources journalistiques* […] *permet de faire respecter l'État de droit.* » Le MFAE va même plus loin en énonçant que :

> Il est donc essentiel de protéger la capacité des journalistes à recueillir, vérifier et analyser les informations, en particulier les informations transmises ou communiquées de façon confidentielles […]. Les journalistes devraient pouvoir compter sur une solide protection des sources journalistiques et des communications confidentielles [...] y compris contre les ingérences indues et le déploiement de technologies de surveillance.

Que s'est-il donc passé au sein de l'UE pour affirmer de façon aussi assertive que les sources des journalistes doivent être protégées contre l'usage de logiciels espions avant d'autoriser l'utilisation de ces derniers dans trente-deux cas qui ne sont pas tous graves, et qui par ailleurs, sont beaucoup trop nombreux, trop larges et beaucoup trop flous dans leur définition juridique.

Le Media Freedom Act européen étant très récent[6], il semble judicieux de décliner les trente-deux crimes et délits énumérés à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise aux États membres[7]. Les trente-deux cas sont les suivants :

> Terrorisme. Participation à une organisation criminelle. Traite des êtres humains. Exploitation sexuelle des enfants et pédopornographie. Trafic illicite de stupéfiants et de substances psychotropes. Trafic illicite d'armes, de munitions et d'explosifs. Corruption. Fraude, y compris la fraude portant atteinte aux intérêts financiers des Communautés européennes au sens de la convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes. Blanchiment du produit du crime. Faux monnayage, y compris la contrefaçon de l'euro. Cybercriminalité. Crimes contre l'environnement, y compris le trafic illicite d'espèces animales menacées et le trafic illicite d'espèces et d'essences végétales menacées. Aide à l'entrée et au séjour irréguliers. Homicide volontaire. Coups et blessures graves. Trafic illicite d'organes et de tissus humains. Enlèvement, séquestration et prise d'otage. Racisme et xénophobie. Vol organisé ou avec arme. Trafic illicite de biens culturels, y compris antiquités et œuvres d'art. Escroquerie. Racket et extorsion de fonds. Contrefaçon et piratage de produits. Falsification de documents administratifs et trafic de faux. Falsification de moyens de paiement. Trafic illicite de substances hormonales et autres

[6] Entré en application le 7 mai 2024 pour les premières règles. Devra être totalement appliqué en 2025.

[7] JO L 190 du 18.07.2002, p. 1.

facteurs de croissance. Trafic illicite de matières nucléaires et radioactives. Trafic de véhicules volés. Viol. Incendie volontaire. Crimes relevant de la juridiction de la Cour pénale internationale. Détournement d'avion/navire. Sabotage.

Au vu de cette longue liste on peut se demander combien d'enquêtes n'auraient pas pu se faire du fait de l'application du MFAE et de l'espionnage autorisé pour connaître les sources et les informations du journaliste. Des milliers assurément. Non seulement des enquêtes visant des hommes ou des femmes politiques n'auraient pas pu aboutir, mais aussi des enquêtes visant des crimes contre des personnes : par exemple, une enquête en immersion dans un réseau pédophile. Ce type d'enquête a déjà été réalisé par des journalistes. Ils n'auraient peut-être pas pu finir leur reportage si le Media Freedom Act européen avait été appliqué, il y a quelques années. Pourront-ils toujours encore le faire demain ? Que ce soit en France ou dans l'un des États membres de l'UE ?

Dire que l'étau se resserre autour du travail d'enquête du journaliste est désormais un euphémisme.

La situation est identique pour des cas de détournement de fonds ou encore pour l'aide à l'entrée et au séjour irréguliers. Si l'on revient à l'exemple du réseau pédophile, il est difficilement concevable qu'un journaliste ne dénonce pas ce réseau à la fin du reportage, après la diffusion pour faire cesser ses activités. Mais si le Freedom Media Act européen est appliqué, l'enquête pourrait être avortée en raison de l'interception des informations avant la fin. De même, aurons-nous encore des milliers d'affaires politico-financières révélées ? Le MFAE ne risquerait-il pas d'engendrer la fin des enquêtes sur la corruption ?

Un juge potentiellement inutile dans le MFAE

Ensuite, le MFAE est dangereux pour les journalistes, car il ne prévoit l'intervention d'un juge que trop tard. On pourrait penser que ce contrôle devrait être effectué avant que le gouvernement ne déploie le logiciel espion dans l'un des trente-deux cas, mais il n'en est rien. En effet, le MFAE précise que tout usage de logiciel espion doit être « *confirmé ultérieurement par une autorité judiciaire ou une autorité décisionnelle indépendante et impartiale* ».

On le voit, les gouvernements européens peuvent mettre en place les logiciels pour espionner les journalistes sans se soucier, dans un premier temps, du respect des règles de protection du MFAE. Ce n'est qu'après coup qu'un juge sera sollicité. Ce qui signifie donc, bien souvent, trop tard. Les informations et le nom des sources du journaliste seraient connus du gouvernement et du juge. Sans compter qu'aucun délai n'est imposé aux gouvernements pour saisir un juge ou une autorité compétente. Dans ce cas rien n'empêche les autorités à attendre dix ans avant de s'inquiéter de savoir si les écoutes des journalistes étaient régulières au moment où elles ont été déployées dix ans plus tôt.

Dire que l'étau se resserre autour du travail d'enquête du journaliste est désormais un euphémisme. Le travail, déjà difficile, risque de devenir impossible dans certains cas, une fois que le MFAE sera appliqué en France dans quelques mois. ■

Catherine Zemmouri est journaliste et chercheuse au CARISM de l'Université Paris 2 Panthéon-Assas.