Pegasus : l'espionnage à l'ère numérique

Stéphane FOSSE
fosse.fr

23 juin 2024

Copyleft : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier
selon les termes de la Licence Art Libre

Résumé

L'été 2021 marque un tournant dans l'histoire de la cybersurveillance avec les révélations sur Pegasus, un logiciel espion conçu par la société israélienne NSO Group. Cette étude analyse le scandale Pegasus sous l'angle technique, politique et juridique. Du fonctionnement du logiciel aux conséquences judiciaires récentes, ce document explore comment cette affaire soulève des questions fondamentales sur l'équilibre entre sécurité nationale et protection des libertés individuelles dans notre société numérique.

Table des matières

1 Une affaire qui secoue le monde

L'été 2021. Le consortium Forbidden Stories, avec l'appui technique d'Amnesty International, dévoile un système d'espionnage d'une ampleur sans précédent. Au cœur de cette tempête médiatique : Pegasus, un logiciel conçu par la société israélienne NSO Group, capable de s'infiltrer dans n'importe quel smartphone et d'en extraire toutes les données sans laisser de traces.

Huit ans après les affaires PRISM et Xkeyscore, cette révélation a de nouveau bouleversé notre vision de la surveillance numérique. D'un niveau d'intrusion jamais atteint, cette technologie cible journalistes, militants des droits humains, avocats, et même chefs d'État. Loin de la lutte contre le terrorisme invoquée par ses créateurs, Pegasus s'avère être un instrument de répression aux mains de régimes autoritaires.

Ce document explore cette affaire sous trois angles. D'abord technique : comment fonctionne ce logiciel espion sophistiqué ? Ensuite politique : quelles sont les conséquences sur les relations internationales ? Enfin juridique : quelles avancées dans les procédures en cours contre NSO Group depuis 2021 ?

2 Aux origines de Pegasus

2.1 NSO Group : de l'unité 8200 au marché de la surveillance

NSO Group naît en 2010 à Herzliya, en Israël, sous l'impulsion de trois entrepreneurs : Niv Carmi, Shalev Hulio et Omri Lavie, dont les initiales forment le nom de la société. Ce détail n'est pas anodin : tous trois sont d'anciens membres de l'unité 8200, l'élite du renseignement militaire israélien spécialisée dans le renseignement d'origine électromagnétique [1].

Au fil des années, l'entreprise suit un parcours financier chaotique. D'abord soutenue par un groupe d'investisseurs mené par Eddy Shalev du fonds Genesis Partners (1,8 million de dollars pour 30% des parts), elle est rachetée en 2014 par la société américaine Francisco Partners pour 145 millions de dollars. En 2019, le fonds britannique Novalpina Capital prend le contrôle de NSO pour près d'un milliard de dollars, avant de perdre la main en juillet 2021 suite à des différends internes, au moment même où éclate le scandale Pegasus [2].

2.2 Un outil de surveillance ultra-sophistiqué

Pegasus représente le nec plus ultra des logiciels espions. Conçu à partir de 2013, il cible les smartphones sous iOS et Android. Sa particularité est son fonctionnement totalement invisible pour sa victime. Une fois installé, il contourne tous les systèmes de sécurité et accède à l'intégralité du contenu du téléphone : messages, emails, photos, mots de passe, géolocalisation... Il peut même activer à distance le microphone et la caméra [3].

Son mode d'infection a évolué au fil du temps. Les premières versions nécessitaient une action de l'utilisateur, comme cliquer sur un lien malveillant. Mais les versions récentes utilisent des méthodes d'infection « zéro-clic » où aucune interaction n'est requise. Par exemple, en mai 2019, une faille dans WhatsApp permettait l'injection du logiciel via un simple appel, même sans réponse [4].

La sophistication technique de Pegasus le rend pratiquement indétectable. Certaines versions se logent uniquement dans la mémoire vive du smartphone, ne laissant aucune trace lors de l'extinction de l'appareil. Son architecture s'appuie sur trois niveaux : une station de travail, un serveur d'infection et une infrastructure cloud, le tout formant ce que NSO appelle le « Pegasus Anonymizing Transmission Network » (PATN) [5].

3 Le scandale Pegasus : révélations et impact

3.1 L'enquête qui a tout révélé

Le 18 juillet 2021, le « Projet Pegasus » éclate au grand jour. Fruit d'une collaboration entre Forbidden Stories, Amnesty International et un consortium de 17 médias internationaux, cette enquête révèle l'utilisation massive du logiciel espion contre des cibles civiles dans le monde entier [6].

L'analyse d'une liste de 50 000 numéros de téléphone ciblés par des clients de NSO dévoile l'ampleur stupéfiante de cette surveillance :

— Plus de 180 journalistes visés dans 20 pays ;

— 600 personnalités politiques ;

— 85 militants des droits humains ;

— 65 chefs d'entreprise ;

— 13 chefs d'État et de gouvernement, dont Emmanuel Macron.

Les investigations techniques menées par le Security Lab d'Amnesty International confirment la présence de Pegasus sur de nombreux appareils examinés. Cette expertise prouve que le logiciel n'est pas qu'une menace théorique mais un outil de surveillance bien réel et massivement déployé [5].

3.2 Pegasus et la France : un cas emblématique

Les révélations concernant la France illustrent parfaitement la nature géopolitique de cette affaire. On apprend que le Maroc aurait espionné des journalistes français comme Edwy Plenel (Mediapart), mais aussi des membres du gouvernement, y compris le président Emmanuel Macron et l'ex-Premier ministre Édouard Philippe [7].

En septembre 2021, une enquête du journal Le Monde révèle que les téléphones de cinq ministres français comportent des traces du logiciel espion [8]. Face à ces faits, la France ouvre une enquête judiciaire. Parallèlement, on découvre que les services de renseignement français avaient été approchés par NSO en 2019, mais que la décision de ne pas acheter Pegasus avait été prise « en haut lieu » fin 2020 [9].

3.3 Conséquences humaines et politiques

Au-delà des chiffres, l'affaire Pegasus a eu des conséquences tragiques. Au Mexique, le journaliste Cecilio Pineda a été assassiné quelques semaines après avoir été ciblé par le logiciel espion. En Arabie Saoudite, l'entourage du journaliste Jamal Khashoggi a été surveillé avant et après son assassinat [10].

Pour les victimes, c'est une violation intolérable de leur intimité. « Toute notre vie devient consultable par des gens qui ne vous veulent pas du bien », témoignait la journaliste Lenaïg Bredoux de Mediapart [11].

Sur le plan diplomatique, plusieurs crises éclatent. L'Algérie condamne l'utilisation du logiciel par le Maroc et se dit « profondément préoccupée » [12]. En Europe, on découvre que la Hongrie et la Pologne ont également utilisé Pegasus contre des opposants politiques, ce qui soulève des questions sur le respect de l'État de droit au sein même de l'Union européenne [13].

4 Développements récents de l'affaire (2022-2025)

4.1 Poursuites judiciaires : l'étau se resserre

Depuis 2021, NSO Group fait face à une avalanche de poursuites judiciaires. WhatsApp et sa maison mère Meta ont été parmi les premiers à attaquer en justice. En mars 2024, une avancée majeure survient lorsqu'une cour fédérale américaine ordonne à NSO Group de remettre à WhatsApp les codes sources de Pegasus et d'autres logiciels espions dans le cadre du litige en cours [14].

En septembre 2024, Apple surprend en abandonnant sa poursuite contre NSO Group, initiée en 2021. L'entreprise de Cupertino justifie ce retrait par des risques accrus de révéler des données sensibles sur les vulnérabilités de ses systèmes et par l'évolution du paysage des menaces [15].

Mais le coup le plus dur pour NSO tombe en décembre 2024 : la justice américaine reconnaît la société coupable d'avoir illégalement piraté environ 1 400 utilisateurs de WhatsApp. Le tribunal rejette l'argument de NSO selon lequel elle ne serait pas responsable des actions de ses clients. Pour John Scott-Railton, chercheur au Citizen Lab, cette décision est « historique » avec « d'énormes implications pour l'industrie des logiciels espions » [16].

4.2 Sanctions et difficultés économiques

En novembre 2021, le Département du Commerce américain place NSO Group sur liste noire, interdisant aux entreprises américaines de faire affaire avec elle. Cette sanction, justifiée par des activités « contraires à la sécurité nationale », porte un coup dur à la réputation et aux finances de l'entreprise israélienne [17].

Ces difficultés entraînent des bouleversements internes. En août 2022, NSO change de PDG : Yaron Shohat remplace Shalev Hulio et annonce un plan de licenciement d'environ 100 employés. Selon la presse israélienne, l'entreprise tente de se réorienter vers les pays de l'OTAN pour restaurer sa crédibilité [18].

Malgré ces efforts, la situation financière de NSO reste précaire. En 2023, son site web devient inaccessible par moments, et selon certaines sources, l'entreprise aurait perdu de nombreux contrats, notamment en Indonésie [19].

4.3 L'évolution du marché de la cybersurveillance

L'affaire Pegasus a eu un impact considérable sur le marché mondial de la cybersurveillance. En mars 2023, onze pays dont la France, les États-Unis et le Royaume-Uni publient un engagement commun visant à encadrer et limiter la « prolifération » de logiciels espions commerciaux [20].

Parallèlement, de nouvelles menaces émergent. En août 2024, des experts en sécurité révèlent que des codes similaires à ceux de Pegasus ont été réutilisés par des agences liées à la Russie, illustrant la prolifération incontrôlée des outils de surveillance vers des acteurs autoritaires [21].

Plus inquiétant encore, un marché noir de faux Pegasus se développe. En mai 2024, des enquêteurs découvrent que des escrocs vendent sur des forums du code généré aléatoirement en le faisant passer pour celui du célèbre logiciel espion, parfois à prix d'or [22].

5 Réflexions sur l'avenir de la surveillance numérique

5.1 Le dilemme sécurité versus liberté

L'affaire Pegasus illustre parfaitement le dilemme auquel nos sociétés font face : comment concilier impératifs de sécurité nationale et protection des libertés individuelles ? NSO Group affirme que ses produits sont destinés à lutter contre le terrorisme et la criminalité organisée. Mais les faits démontrent qu'ils ont été massivement détournés contre la société civile [23].

Ce cas soulève des questions fondamentales : qui surveille les surveillants ? Comment garantir qu'une technologie aussi intrusive ne sera pas utilisée à des fins de répression politique ? L'absence de cadre juridique international contraignant laisse la porte ouverte à tous les abus.

5.2 Vers une régulation mondiale ?

Face aux dérives révélées par l'affaire Pegasus, plusieurs initiatives voient le jour. L'ONU, par la voix de sa Haute-Commissaire aux droits de l'homme, appelle à un moratoire sur la vente de technologies de surveillance. Le Parlement européen met en place une commission d'enquête sur l'utilisation de Pegasus dans l'Union européenne [24].

Des experts plaident pour un traité international contraignant, qui établirait des normes claires pour l'utilisation de ces technologies et des mécanismes de contrôle indépendants. D'autres proposent la création d'un registre mondial des logiciels espions, sur le modèle des registres d'armes conventionnelles [25]. Mais toutes ces mesures n'empêcheront jamais d'agir dans l'illégalité.

6 Conclusion

Quatre ans après les premières révélations, l'affaire Pegasus continue de faire des vagues. Les décisions de justice récentes, notamment la condamnation de NSO Group aux États-Unis en décembre 2024, sont un pas de plus dans la lutte contre les abus de la surveillance numérique.

Ce scandale aura eu le mérite de lever le voile sur une industrie opérant dans l'ombre. Il a révélé l'existence d'un marché florissant de l'espionnage clé en main, accessible à des États aux intentions douteuses. Plus fondamentalement, il nous force à repenser l'équilibre entre sécurité et libertés à l'ère numérique.

L'affaire Pegasus s'inscrit dans une problématique de militarisation du cyberespace. Quand un logiciel espion devient une arme de guerre, comme Pegasus est parfois décrit, c'est tout l'édifice des droits numériques qui vacille. Notre vigilance collective s'impose face à cette nouvelle forme de pouvoir, invisible mais omniprésente.

Références

[1] Wikipédia, NSO Group, 2025.

[2] Wikipédia, NSO Group - Historique financier, 2025.

[3] J. Cheminat, Comment fonctionne le logiciel espion Pegasus ? *Le Monde Informatique*, Juillet 2021.

[4] J. G., Pegasus : NSO Group coupable du piratage de WhatsApp, *Generation-NT*, Décembre 2024.

[5] Amnesty International, Rapport concernant la méthodologie technique employée pour détecter le logiciel Pegasus de NSO Group, Juillet 2021.

[6] Forbidden Stories, The Pegasus Project, 2021.

[7] Espionnage de journalistes et d'opposants : l'affaire « Pegasus » provoque l'indignation, *Le Monde*, Juillet 2021.

[8] Les téléphones de cinq ministres français comportent des traces du logiciel espion Pegasus, sept. 2021.

[9] L. de Raguenel, La France a failli acheter le logiciel espion israélien Pegasus, *Europe 1*, oct. 2021.

[10] Amnesty International, Pegasus: révélations sur un système mondial de surveillance, Juillet 2022.

[11] J. Monin, Enquête Le projet Pegasus : un logiciel espion utilisé par des États pour cibler des politiques, des journalistes, des avocats... y compris des Français, *France Info*, Juillet 2021.

[12] Pegasus : l'Algérie, « profondément préoccupée », condamne l'utilisation du logiciel par le Maroc, *Le Monde*, Juillet 2021.

[13] Aleksandra Krzysztoszek, Pologne : plus de 500 personnes victimes du logiciel espion Pegasus sous l'ancien gouvernement conservateur, *Euractiv Pologne*, Avril 2024.

[14] R. Lakshmanan, U.S. Court Orders NSO Group to Hand Over Pegasus Spyware Code to WhatsApp, *The Hacker News*, mars 2024.

[15] R. Naraine, Apple Suddenly Drops NSO Group Spyware Lawsuit, *Security Week*, sept. 2024.

[16] N. Gavetière, Le jugement contre NSO Group : justice rendue ou victoire symbolique ? *Tech Generation*, Décembre 2024.

[17] Wikipédia, NSO Group - Sanctions, 2025.

[18] O. Bellin, NSO Group (Pegasus) change - à nouveau - de PDG et licencie, *Solutions Numériques*, Août 2022.

[19] Wikipédia, Pegasus (logiciel espion) - Développements récents, 2025.

[20] Wikipédia, NSO Group - Régulation internationale, 2025.

[21] Wikipédia, Pegasus (logiciel espion) - Prolifération du code, 2025.

[22] G. Swain, Du faux code source de Pegasus se diffuse sur le dark web, *Le Monde Informatique*, Mai 2024.

[23] « L'affaire Pegasus montre parfaitement les faiblesses de l'Europe en matière de cyberagressions », *Le Monde*, Juillet 2021.

[24] Parlement Européen, Enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents, Juin 2023.

[25] Amnesty International, États-Unis. Une décision de justice fait avancer l'obligation de rendre des comptes pour les victimes d'un logiciel espion de NSO Group, mars 2024.

[26] L. Richard et S. Rigaud, Pegasus : how a spy in your pocket threatens the end of privacy, dignity, and democracy. New York : Henry Holt et Company, jan. 2023.