

PEGASUS & LE GOUVERNEMENT FRANÇAIS

Synthèse des reproches citoyens — du moins grave au plus grave

Contexte : Pegasus est un logiciel espion militaire développé par l'entreprise israélienne NSO Group. Capable d'infecter un téléphone à l'insu de son propriétaire — y compris sans aucune action de sa part (« zero-click ») —, il permet d'accéder à l'intégralité du contenu : messages, appels, caméra, micro, historique de localisation. En juillet 2021, le consortium Forbidden Stories (17 médias internationaux, dont Le Monde, Radio France et Mediapart) a révélé son utilisation massive contre des journalistes, avocats, militants et chefs d'État. Plus de 1 000 Français figuraient sur la liste des cibles potentielles.

Reproches classés du moins grave au plus grave

1. Absence de commission d'enquête parlementaire en France

- Contrairement à l'Espagne, l'Allemagne et le Parlement européen (commission PEGA créée en février 2022), la France n'a ouvert aucune commission d'enquête parlementaire sur l'affaire Pegasus, laissant les victimes sans tribune institutionnelle.
- Laurent Richard, directeur de Forbidden Stories, a jugé « assez étonnant » ce silence politique alors que le sujet provoquait « un vrai débat dans le monde entier ».

2. Lenteur et opacité de l'enquête judiciaire française

- Le parquet de Paris n'a confié l'enquête à un juge d'instruction qu'un an après les révélations (juillet 2022). L'information judiciaire ouverte porte sur de nombreuses infractions potentielles, mais est dirigée « contre X », sans mise en cause nommée à ce jour.
- Cinq ans après les révélations, aucune condamnation n'a été prononcée. Pendant ce temps, le Maroc — principal pays soupçonné — poursuit en diffamation les médias français ayant enquêté (Le Monde, Mediapart, Radio France), renversant ainsi la charge symbolique.

3. Non-protection des victimes françaises de la société civile

- Environ 1 000 ressortissants français ont été ciblés : journalistes (Edwy Plenel/Mediapart), militants, avocats, universitaires, responsables politiques de tous bords. L'État n'a pas organisé d'information systématique de ces victimes ni mis en place de mesures de protection.
- Des victimes de la société civile, comme la militante Claude Mangin, déclarent se sentir « complètement abandonnées » par l'État français face à l'espionnage dont elles ont fait l'objet.

4. Raison d'État : protection des intérêts diplomatiques au détriment des victimes

- En dépit des révélations, la France n'a jamais désigné publiquement le Maroc comme responsable. Emmanuel Macron, dont le propre téléphone avait été ciblé, n'a pas décroché son téléphone pour demander des explications au roi Mohammed VI. La diplomatie commerciale et géopolitique avec Rabat a été jugée prioritaire.
- La France a préféré exercer une pression discrète sur Israël (négociations secrètes pour que les numéros français soient « protégés » dans les futurs contrats NSO) plutôt que de demander des comptes au pays soupçonné d'avoir commandé l'espionnage.
- En avril 2026, l'Espagne a saisi Eurojust pour forcer la coopération judiciaire, déploré le silence de Paris : huit mois après avoir demandé accès aux données techniques recueillies par l'ANSSI, Madrid n'avait reçu aucune réponse de la France.

5. Atteinte à la liberté de la presse et au secret des sources journalistiques

- Pegasus a permis l'espionnage intégral des téléphones de journalistes français d'investigation : accès aux sources, carnets de contacts, communications chiffrées. C'est une destruction du secret des sources — protection fondamentale dans toute démocratie — réalisée par un gouvernement étranger sur le territoire français.
- Au total, selon le consortium Forbidden Stories, les téléphones d'au moins 180 journalistes dans 20 pays ont été attaqués entre 2016 et juin 2021. Parmi les victimes identifiées figuraient Edwy Plenel (Mediapart) et des journalistes de Radio France.

6. Espionnage du Président et de membres du gouvernement : atteinte à la souveraineté nationale

- Le téléphone d'Emmanuel Macron, de l'ancien Premier ministre Édouard Philippe et de quinze membres du gouvernement (dont Florence Parly, ministre des Armées, Jean-Michel Blanquer, Sébastien Lecornu, etc.) ont été ciblés ou infectés. L'ANSSI a confirmé l'infection du téléphone de Florence Parly.
- Cet espionnage d'État à État constitue une atteinte directe à la souveraineté nationale, aux secrets de la défense et à la sécurité des délibérations gouvernementales. Il a été qualifié d'« extrême gravité » par le Premier ministre Jean Castex devant l'Assemblée nationale.

7. Complicité dans une infrastructure mondiale de répression : du Maroc à Khashoggi

- Pegasus a été utilisé par des régimes autoritaires pour assassiner ou faire taire des opposants : le téléphone de la fiancée du journaliste Jamal Khashoggi avait été infecté quatre jours avant son assassinat dans le consulat saoudien d'Istanbul. NSO a vendu Pegasus à des pays comme l'Arabie saoudite, le Rwanda, la Hongrie, le Mexique ou les Émirats.
- En préservant ses relations bilatérales avec certains de ces États clients, et en ne sanctionnant pas NSO Group, le gouvernement français s'inscrit objectivement dans une complicité de fait avec cette infrastructure mondiale de répression, qualifiée par Amnesty International de « crise internationale des droits humains ».
- Le Parlement européen a adopté en novembre 2023 (par 425 voix contre 108) une résolution dénonçant « l'absence de suites législatives » données par la Commission à ses propres recommandations sur Pegasus, pointant l'urgence d'agir face aux menaces pour « la démocratie et l'État de droit ».

Conclusion : Le scandale Pegasus révèle un gouvernement français incapable de protéger ses citoyens, ses journalistes et sa propre souveraineté face à l'espionnage étranger, choisissant la raison d'État et les intérêts commerciaux sur l'obligation de réponse démocratique, laissant victimes et journalistes sans protection effective cinq ans après les révélations.

Enquêtes journalistiques fondatrices

- **Forbidden Stories / Amnesty International** — Le Projet Pegasus (juillet 2021) : l'enquête originale de 17 médias internationaux sur 50 000 numéros ciblés. — forbiddenstories.org
- **Amnesty International** — Rapport technique sur Pegasus (Amnesty Tech Security Lab) et communiqué « Comment réagir après ces révélations » — amnesty.fr
- **Franceinfo** — « Pegasus, et après ? Comment la France a mis la pression sur Israël plutôt que sur le Maroc » (nov. 2021) — franceinfo.fr
- **Franceinfo** — Dossier complet « Projet Pegasus » (tous articles, de 2021 à 2026) — franceinfo.fr/monde/projet-pegasus
- **Afrik.com** — « Affaire Pegasus : Macron, Sánchez et Mohammed VI au cœur d'un scandale d'espionnage d'État » (avr. 2026) — afrik.com

Documents parlementaires & institutionnels

- **Assemblée nationale** — Question au gouvernement d'Alexis Corbière sur Pegasus (juillet 2021) — assemblee-nationale.fr (PDF)
- **Parlement européen** — Commission d'enquête PEGA : rapport final sur Pegasus (rapport Sophia In't Veld, mai 2023) — europarl.europa.eu
- **Conseil de l'Europe** — APCE, rapport « Le logiciel espion Pegasus et la surveillance secrète opérée par l'État » (doc. 15825, 2023) — assembly.coe.int
- **Espagne / Eurojust** — Saisine d'Eurojust face au silence de la France (déc. 2025–avr. 2026) — moroccomail.fr

Livres de référence

- **Laurent Richard & Sandrine Rigaud**, *Forbidden Stories : Quand des journalistes risquent leur vie pour informer*, Don Quichotte, 2019. Les fondateurs du consortium qui a révélé Pegasus racontent leur méthode d'enquête collaborative.
- **Olivier Tesquet**, *À la trace : enquête sur les nouveaux territoires de la surveillance*, Premier Parallèle, 2021. Analyse approfondie des technologies de surveillance commerciale, dont Pegasus, et de leurs usages contre les citoyens.

Documentaires & vidéos

- **Arte** — « Spy Merchants » (Marchands d'espions, 2022) : documentaire sur l'industrie européenne et israélienne des logiciels espions, incluant NSO Group. — arte.tv
- **Forbidden Stories (YouTube)** — Mini-documentaires et présentations du Projet Pegasus — youtube.com/@forbiddenstories

Ressources ONG et chercheurs spécialistes

- **Citizen Lab (Université de Toronto)** — Rapports techniques sur les infections Pegasus dans le monde — citizenlab.ca
- **Access Now** — Rapports sur l'utilisation de Pegasus contre des défenseurs des droits, avec guide de détection Mobile Verification Toolkit (MVT) — accessnow.org