



# « ON COMMENCE PAR LE VERDICT »

AU CŒUR DE L'APPAREIL DE SURVEILLANCE MAROCAIN  
SYNTHÈSE

**AMNESTY**  
INTERNATIONAL



**Amnesty International est un mouvement rassemblant 10 millions de personnes qui fait appel à l'humanité en chacun et chacune de nous et milite pour que nous puissions toutes et tous jouir de nos droits humains. Notre vision est celle d'un monde dans lequel les dirigeants et dirigeantes tiennent leurs promesses, respectent le droit international et sont tenus de rendre des comptes. Indépendante de tout gouvernement, de toute idéologie politique, de tout intérêt économique et de toute religion, Amnesty International est essentiellement financée par ses membres et des dons de particuliers. Nous avons la conviction qu'agir avec solidarité et compassion aux côtés de personnes du monde entier peut rendre nos sociétés meilleures.**

© Amnesty International 2026

Sauf mention contraire, le contenu de ce document est sous licence Creative Commons (Attribution – Pas d'Utilisation Commerciale – Pas de Modification 4.0 International).

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.fr>

Pour plus d'informations, veuillez consulter la page relative aux autorisations sur notre site :

[www.amnesty.org/fr](http://www.amnesty.org/fr).

Lorsqu'une entité autre qu'Amnesty International est détentrice du copyright, le matériel n'est pas sous licence Creative Commons.

Édition originale publiée en 2026

par Amnesty International Ltd

Peter Benenson House, 1 Easton Street  
London WC1X 0DW, Royaume-Uni

Index : MDE 29/1481/2026

Langue originale : anglais

[amnesty.org/fr](http://amnesty.org/fr)



Image de couverture : © Rectangle/Evan Grothjan

**AMNESTY**  
INTERNATIONAL



# SYNTHÈSE

**« Il existe des lois écrites, mais elles ne sont pas appliquées. Il y a des lois mais personne ne les respecte. Ils se fichent des autorisations juridiques, des mandats. Parfois ils peuvent même rattraper et rédiger les documents *a posteriori*. Il y a une impunité totale. Les choses sont faites à l'envers. On commence par le verdict. »**

*Safir, ancien membre de la Direction générale de la surveillance du territoire (DGST)*

« Un test », « un cobaye » : c'est ainsi que les agent-e-s des services de renseignement intérieur du Maroc – la Direction générale de la surveillance du territoire (DGST) – ont qualifié Maâti Monjib, défenseur des droits humains et universitaire, quand ils l'ont choisi pour être l'une des premières cibles du logiciel espion Pegasus, fourni par l'entreprise NSO Group, en 2017. Cependant, pour Maâti Monjib, les conséquences ont été tout sauf théoriques. Le fait que la DGST s'en soit prise à lui a confirmé ce qu'il soupçonnait depuis longtemps : il était surveillé par les autorités marocaines pour son travail en faveur des droits humains et ses écrits universitaires. Toute sa vie numérique s'en est trouvée révélée aux autorités : ses messages, ses appels, la caméra de son téléphone, ses données de localisation, ses contacts, et d'autres informations encore. À l'époque, Maâti Monjib faisait l'objet de poursuites pénales et de mesures de répression pour son travail. En 2015, il avait comparu en justice pour avoir reçu des fonds de l'étranger destinés à financer la formation de journalistes, et il s'était vu interdire de quitter le Maroc. Quelques années plus tard, il a été condamné à une peine d'un an d'emprisonnement. En 2020, il a de nouveau été inculpé de charges forgées de toutes pièces l'accusant de blanchiment d'argent et de détournement de fonds. Amnesty International a alors demandé sa libération immédiate et sans conditions. Pendant toute cette période, Maâti Monjib a été confronté à des campagnes de dénigrement incessantes dans les médias proches du pouvoir et en ligne. Bien qu'ayant été finalement gracié en 2024, il a continué d'être harcelé. Encore dernièrement, en 2025, des vidéos de lui l'accusant de boire de l'alcool, de fumer la chicha et de « prendre du bon temps avec sa maîtresse » ont circulé en ligne. Maâti Monjib pense que cette stratégie visait non seulement à le réduire au silence, mais aussi à faire peur à d'autres personnes pour qu'elles se taisent. Comme il le dit en paraphrasant un proverbe marocain : « Tape le grand, les petits auront peur. »

Maâti Monjib est loin d'être le seul dans ce cas. Pour le seul fait d'exercer leurs droits, les défenseur-e-s des droits humains marocains sont régulièrement victimes d'une combinaison de mesures associant surveillance illégale, campagnes de dénigrement et harcèlement judiciaire ou poursuites pénales. Les agent-e-s de la DGST agissent sans contrôle judiciaire ni obligation de rendre des comptes et prennent pour cible en secret

et en toute impunité les personnes qui expriment des opinions dissidentes. L'éventail d'outils qu'ils déploient est vaste, mais leur objectif est clair : faire chanter, discréditer, humilier et, si nécessaire, emprisonner celles et ceux qui font entendre leur voix pour défendre les droits humains au Maroc.

Ce rapport offre la description la plus détaillée et la plus complète jamais établie à ce jour de l'écosystème de surveillance qui permet aux autorités marocaines de recourir à des tactiques répressives pour harceler, discréditer et au bout du compte réduire au silence les défenseur-e-s des droits humains. Il s'appuie sur de nouveaux témoignages de personnes ayant travaillé au sein des services de renseignement marocains et ayant participé à la surveillance illégale de défenseur-e-s des droits humains, sur des documents divulgués à la suite de fuites (données de surveillance, archives gouvernementales internes contenant des informations sur les cibles, et documentation d'entreprises vendant des technologies de surveillance) et sur des enquêtes journalistiques menées directement par des partenaires de recherche d'Amnesty International.

Le Maroc a fait partie des premiers pays où l'on a découvert que des militant-e-s et des journalistes avaient été pris pour cible par des logiciels espions sophistiqués, puisque des preuves d'attaques au moyen d'un logiciel espion fourni par la société Hacking Team ont été révélées dès 2012. La société civile marocaine a de nouveau été identifiée parmi les cibles visées partout dans le monde par le logiciel espion Pegasus en 2019, et l'ampleur de la surveillance exercée par le Maroc sur les défenseur-e-s des droits humains a été mise au jour dans le cadre du Projet Pegasus en 2021. Ces antécédents attestés d'utilisation abusive de logiciels espions et d'outils de surveillance font du Maroc un cas unique, à partir duquel il est possible d'analyser comment les États utilisent tout un éventail de technologies de surveillance pour s'attaquer aux personnes qui critiquent le pouvoir et restreindre le travail de la société civile.

L'écosystème de surveillance marocain repose sur des outils de haute technologie, dont des logiciels espions hautement intrusifs comme Pegasus, ainsi que sur des techniques plus anciennes, telles que les filatures, les écoutes et tout ce qu'il y a entre les deux. Des appareils personnels sont infiltrés. Des personnes sont filmées et enregistrées à leur insu en détention, dans leur bureau ou dans leur voiture personnelle, et même dans leur chambre à coucher. Les appels téléphoniques des personnes visées sont systématiquement enregistrés et espionnés. Leurs données de localisation sont suivies, révélant leurs déplacements quotidiens et leurs contacts, entre autres. Des boutiques de téléphonie vendent des téléphones mobiles préinfectés par des logiciels malveillants par la DGST. Des voisin-e-s sont recrutés comme informateurs ou informatrices pour rendre compte des activités et déplacements quotidiens des défenseur-e-s des droits humains. Toutes ces tactiques touchent non seulement les défenseur-e-s visés, mais aussi leurs familles, leurs amis et leurs réseaux professionnels, au Maroc comme à l'étranger. En résumé, les défenseur-e-s des droits humains marocains n'ont nulle part où se cacher et aucun moyen d'échapper au réseau de surveillance tous azimuts de l'État.

Tous les détails les plus intimes de la vie des défenseur-e-s des droits humains deviennent par conséquent un livre ouvert sous les yeux des autorités, et sont exploités pour les réduire au silence. Certaines données, dont des vidéos et des enregistrements audio à caractère personnel, intime ou sexuel, peuvent être enregistrées et parfois communiquées aux médias proches du pouvoir, qui mènent des campagnes de dénigrement publiques visant à salir la réputation des militant-e-s et à les discréditer aux yeux du grand public marocain. Les femmes défenseuses des droits humains en particulier, ou les femmes ayant des liens avec des cibles masculines de premier plan, sont soumises à des manœuvres visant à les humilier publiquement pour des transgressions réelles ou présumées des normes sociales conservatrices. Ces campagnes peuvent durer des années et sont promues en ligne par une armée de commentateurs-trices liés au gouvernement afin d'en accroître la portée et la visibilité. Elles sont si connues que les médias qui les diffusent le plus couramment sont qualifiés localement de « médias de la diffamation ».

Outre la surveillance illégale et les campagnes de dénigrement, les défenseur-e-s des droits humains sont régulièrement la cible de harcèlement judiciaire et d'inculpations motivées par des considérations politiques et/ou forgées de toutes pièces, d'arrestations, de placements en détention et de peines d'emprisonnement prononcées à la suite de procès inéquitables et sur la base d'un cadre juridique contraire aux normes internationales. Certain-e-s ont été poursuivis pour des actes protégés par les droits à la liberté d'expression ou d'association ou pour des infractions non reconnues par le droit international, notamment des délits d'expression définis en termes vagues, utilisés pour poursuivre les personnes exprimant des opinions dissidentes ou tenant d'autres propos légitimes. Dans certains cas, des pressions sont exercées sur les défenseur-e-s des droits humains pour qu'ils fassent de faux témoignages contre d'autres personnes.

Les attaques contre les défenseur-e-s des droits humains ne s'arrêtent pas aux frontières du Maroc. Celles et ceux qui sont en exil, ou qui s'expriment depuis l'étranger, continuent de faire l'objet de mesures de surveillance et de campagnes de dénigrement. Même des diplomates étrangers et d'autres représentant-e-s des autorités d'autres pays ont été visés.

Plus généralement, la combinaison de toutes ces tactiques a un important effet dissuasif sur les autres défenseur-e-s des droits humains, et sur toute personne dans la société en général qui serait tentée d'exprimer des idées dissidentes. Le prix à payer par les opposant-e-s marocains est sans cesse plus élevé, car ils n'ont aucun moyen de savoir quand ils sont observés et enregistrés, exposent leurs familles et amis à des risques inconnus, et craignent d'être publiquement humiliés voire emprisonnés s'ils font entendre leur voix.

Pourtant, beaucoup continuent de s'exprimer et tentent de demander des comptes aux responsables qui sont au pouvoir. Ce rapport présente leurs histoires, qui soulignent combien il est urgent que le Maroc mette un terme à l'impunité dont jouit la DGST, réforme ses lois et ses pratiques et respecte, protège et mette en œuvre les droits fondamentaux des journalistes et des défenseur-e-s des droits humains.

## **L'UTILISATION DE LA SURVEILLANCE ILLÉGALE AU MAROC**

La surveillance d'une personne à son insu n'est pas en soi une violation des droits humains. Elle peut être menée en toute légalité sous réserve de respecter un certain nombre de garanties définies dans le Pacte international relatif aux droits civils et politiques (PIDCP), auquel le Maroc est partie, concernant la protection des droits au respect de la vie privée, à la liberté d'opinion et à la liberté d'expression. Le Comité des droits de l'homme de l'ONU a établi que le droit au respect de la vie privée nécessitait la mise en place de systèmes de supervision solides et indépendants des opérations de surveillance, d'interception et de piratage. Dans sa résolution 73/179, l'Assemblée générale des Nations unies a souligné que la surveillance des communications numériques devait être conforme aux obligations internationales relatives aux droits humains et reposer sur un cadre juridique accessible à tous, clair, précis, complet et non discriminatoire.

Même lorsqu'elle est menée conformément aux procédures juridiques nationales, la surveillance est illégale si ces procédures portent atteinte ou contreviennent aux normes internationales relatives aux droits humains. Elle n'est par exemple pas légale si elle est menée sans les autorisations et la supervision judiciaires exigées par les procédures réglementant son usage.

En vertu du droit international relatif aux droits humains, le Maroc doit non seulement s'abstenir de commettre des violations des droits humains, mais aussi protéger la population des atteintes perpétrées par des acteurs privés. Par ailleurs, il doit veiller à ce que ses opérations de surveillance soient légales, qu'elles soient menées sur son territoire ou à l'étranger. L'utilisation de logiciels espions et d'autres outils de surveillance à des fins de répression transnationale est de plus en plus citée comme motif de préoccupation par un nombre croissant d'autorités et d'expert-e-s de l'ONU.

Au Maroc, la surveillance est menée par la DGST, souvent sans autorisation juridique, et dans l'objectif illégal d'attaquer des défenseur-e-s des droits humains pour leur travail. Elle ne touche pas seulement les défenseur-e-s eux-mêmes, mais aussi leurs familles, leurs avocat-e-s et leurs réseaux sociaux et professionnels. Cette surveillance n'est pas soumise à une supervision indépendante et est couramment mise en œuvre au mépris des procédures juridiques nationales.

En vertu du droit international et des normes en la matière, l'ingérence dans la vie privée n'est autorisée que si elle respecte les obligations de légalité, de nécessité et de proportionnalité, et si elle est menée dans un but légitime. La surveillance des défenseur-e-s des droits humains en raison de leur travail en faveur des droits fondamentaux est donc illégale aux termes du droit international relatif aux droits humains et des normes y afférentes, qu'elle respecte ou non les procédures juridiques nationales.

Pour se conformer à leur obligation de respecter le droit à la vie privée, les autorités doivent absolument disposer de garanties, notamment juridiques, capables d'empêcher l'utilisation abusive des technologies de surveillance dans la pratique. L'absence de supervision judiciaire satisfaisante, de mesures d'obligation de rendre des comptes ou d'accès à un recours effectif entraîne non seulement des violations du droit au respect de la vie privée des personnes visées par les opérations de surveillance, mais aussi un effet dissuasif qui incite les journalistes, les militant-e-s, les défenseur-e-s des droits humains et de nombreuses autres personnes à restreindre leur parole, à limiter leurs signalements ou à mettre leur militantisme en sourdine, ce qui a pour effet de réduire l'espace civique pour l'ensemble de la population.

Si la responsabilité principale de respecter le droit relatif aux droits humains revient à l'État marocain, les entreprises privées, tant nationales qu'internationales, ont aussi la responsabilité de ne pas provoquer des atteintes aux droits humains ni y contribuer. Cette obligation existe indépendamment du droit national.

La compatibilité des mesures de surveillance avec le droit relatif aux droits humains dépend non seulement de la loi et des pratiques des organismes d'État, mais aussi des outils spécifiques utilisés. La surveillance de masse, menée par exemple au moyen d'outils comme ceux vendus par Amesys ou Verint, ou *via* la

coopération extrajudiciaire d'opérateurs de télécommunication, est contraire au droit relatif aux droits humains et aux normes en la matière. Beaucoup des logiciels espions modernes et hautement intrusifs utilisés par les autorités marocaines, comme Pegasus (de NSO Group) et Remote Control System (de la société Hacking Team), sont, de par leur conception même, fondamentalement incompatibles avec les droits fondamentaux. Amnesty International a demandé une interdiction mondiale de ces formes de logiciels espions hautement intrusifs car ils permettent un accès illimité aux appareils et leur utilisation ne peut pas faire l'objet d'un contrôle indépendant.

Enfin, la vie privée et d'autres droits fondamentaux peuvent être violés par l'utilisation de divers outils, même si ceux-ci ne sont pas considérés comme des outils de « surveillance » au sens strict par leurs fournisseurs ou utilisateurs. C'est le cas, entre autres, des outils de criminalistique numérique et des IMSI-catchers (qui permettent de suivre les téléphones mobiles). La légalité de la surveillance ne dépend pas non plus du niveau de sophistication technique des appareils utilisés. Même le simple acte d'enregistrer ou d'écouter une cible doit être réalisé conformément au droit international relatif aux droits humains et aux normes connexes.

## **PEGASUS : COMMENT LE LOGICIEL ESPION LE PLUS CONNU AU MONDE A ÉVOLUÉ ET COMMENT LE MAROC L'A UTILISÉ CONTRE DES DÉFENSEUR·E·S DES DROITS HUMAINS ET DES JOURNALISTES**

Depuis des années, le logiciel espion Pegasus de NSO Group est utilisé pour faciliter des atteintes aux droits humains à grande échelle partout dans le monde. Pour rédiger ce rapport, Amnesty International s'est appuyée sur des documents marketing et techniques internes de NSO Group qui n'avaient jamais été rendus publics jusqu'à présent et ont été révélés dans le cadre d'une longue procédure intentée au civil par WhatsApp et Meta aux États-Unis. Ces documents offrent le tableau le plus complet à ce jour de la manière dont le système Pegasus est construit, mis en œuvre et entretenu.

Cette nouvelle analyse fournit des éléments précieux en matière d'obligation de rendre des comptes concernant les logiciels espions, montrant notamment à quel point le système utilisé par les clients gouvernementaux nécessite une maintenance et un support permanents de NSO Group pour pouvoir continuer de fonctionner. Ces documents nouvellement divulgués confirment aussi de façon indépendante l'authenticité et l'exactitude des données recueillies à la suite de fuites qui ont été à la base de la première enquête du Pegasus Project.

Cette meilleure compréhension de Pegasus a permis à Amnesty International de poursuivre et consolider ses précédentes recherches sur l'utilisation de ce logiciel espion au Maroc. Son nouveau rapport établit que, malgré les démentis officiels, les autorités marocaines ont eu recours à Pegasus entre 2017 et 2021, voire plus tard. L'organisation décrit comment l'utilisation de ce logiciel au Maroc a évolué parallèlement aux progrès de la technologie elle-même. Les preuves numériques montrent qu'une variété de « vecteurs » (exploitations de failles et techniques d'infection) ont été utilisés pour attaquer les appareils des défenseur·e·s des droits humains, notamment : des attaques « un clic », qui nécessitent généralement que la victime clique sur un lien malveillant ; des attaques « zéro clic », qui peuvent infecter subrepticement une cible sans qu'il n'y ait besoin de cliquer sur un lien ni même de faire une quelconque action ; et des attaques par injection réseau, qui nécessitent d'utiliser le réseau de Maroc Telecom.

Ce rapport s'appuie aussi sur les documents internes de NSO Group mentionnés plus haut pour mettre en évidence les mesures prises par cette entreprise pour enregistrer l'infrastructure d'attaque unique spécifique à chaque client. Cette découverte valide la méthode de la communauté de responsabilité en reliant différents groupes d'attaques de logiciel espion au même opérateur. C'est particulièrement important en ce qui concerne l'utilisation de cet outil par les autorités marocaines, car cela permet d'établir que le même client est responsable non seulement d'attaques contre les défenseur·e·s des droits humains au Maroc, mais aussi d'opérations de surveillance illégale menées au moyen de Pegasus contre des militant·e·s et journalistes marocains vivant à l'étranger, ainsi que contre certains militant·e·s, journalistes, diplomates et autres représentant·e·s des autorités non marocains.

# COMMENT UN RÉSEAU NÉBULEUX DE SOCIÉTÉS DE SURVEILLANCE AIDE LE MAROC À METTRE EN ŒUVRE TOUT UN ÉVENTAIL DE TECHNIQUES DE SURVEILLANCE

Si Pegasus occupe une place importante dans les opérations des autorités marocaines compte tenu des capacités et des effets des logiciels espions hautement intrusifs, il n'est qu'un outil numérique parmi les nombreux autres qui composent l'écosystème répressif de surveillance du Maroc. Le gouvernement marocain a recours à tout un éventail de techniques et d'outils achetés, sans aucun droit de regard du grand public, auprès de différentes entreprises basées en Israël, dans l'Union européenne et aux États-Unis. Il s'appuie aussi sur la coopération extrajudiciaire d'au moins un opérateur national de télécommunication.

Ce rapport montre que, outre les contrats avec NSO Group, deux organes de sécurité marocains, la DGST et le Conseil supérieur de la défense nationale (CSDN), avaient depuis au moins 2009 des contrats avec l'entreprise de logiciels espions italienne Hacking Team, qui a depuis été rachetée et rebaptisée Memento Labs. Le Maroc était l'un des principaux clients du logiciel espion Remote Control System (RCS) vendu par cette entreprise.

Des recherches menées par d'autres organisations de la société civile ont aussi révélé des cas d'utilisation au Maroc du logiciel espion FinSpy, produit par le réseau d'entreprises germano-britannique composé de Gamma Group et de FinFisher.

Outre les technologies de surveillance ciblée, le Maroc a eu recours à un certain nombre de technologies de surveillance de masse, qui permettent le suivi, l'interception, le stockage ou l'analyse sur une grande échelle d'une énorme quantité de données. Par exemple, depuis décembre 2009, il utilise le système Eagle (ensuite rebaptisé Cerebro) fourni par la société française de télécommunication et de défense Amesys (devenue par la suite Nexa Technologies, puis Trovicor Intelligence, et enfin Datafusion en 2024). Cette technologie permet de surveiller le trafic Internet (IP) à l'échelle d'un pays. Le projet, désigné par Amesys sous le nom de code « Popcorn », prévoyait le déploiement au Maroc de Cerebro, une technologie d'interception de masse des données Internet.

Ce rapport fait également état de l'achat en 2014 par le Maroc du système Reliant 12 de l'entreprise états-unienne Verint, qui permet la collecte et l'analyse de données relatives aux communications téléphoniques, aux fournisseurs d'accès à Internet sur mobiles et au trafic Internet.

La DGST utilise aussi des IMSI-catchers, dispositifs conçus pour imiter une antenne de téléphonie mobile et ainsi intercepter les données des appareils situés à proximité, y compris provenant d'applications de messagerie cryptées, avant qu'elles ne soient transmises, ce qui permet aux agent-e-s d'espionner les téléphones des militant-e-s et de surveiller les défenseur-e-s des droits humains.

La DGST a par ailleurs recours à l'outil Universal Forensic Extraction Device (UFED) de la compagnie israélienne Cellebrite. Cet outil de surveillance permet d'accéder à la totalité des données d'un appareil lorsqu'il se trouve physiquement entre les mains d'un opérateur. Les autorités ont profité de situations comme la détention ou des transits à l'aéroport pour accéder illégalement aux appareils de défenseur-e-s des droits humains à leur insu.

Le Maroc est également client de l'entreprise de cyber-renseignement Cognyte, qui a été créée en 2021 en tant qu'entité distincte issue de la société états-unienne Verint Systems et dont les outils permettent aux clients de contrôler de faux comptes sur les réseaux sociaux (des « avatars ») afin de collecter des renseignements à propos des utilisateurs et utilisatrices de ces réseaux ou de lancer des attaques d'ingénierie sociale.

Selon *Safir*, ancien agent de la DGST, l'une des composantes essentielles des capacités de surveillance de la DGST est la coopération d'un opérateur national de télécommunication. Cet homme a expliqué que les agent-e-s de la DGST avaient un accès direct aux données et aux communications de l'ensemble du réseau, et notamment aux appels, qu'ils pouvaient écouter ou retranscrire à volonté. Les capacités de surveillance décrites correspondent aux fonctionnalités offertes par l'outil Reliant de Verint, un système de surveillance de masse qui a été vendu aux autorités marocaines au milieu des années 2010, selon les registres des ventes internes de Verint. Ces registres mentionnent également Maroc Telecom comme acheteur potentiel des produits d'interception réseau de l'entreprise, dans le cadre du système plus global. Les enquêtes de criminalistique numérique ont confirmé que le réseau de Maroc Telecom avait été utilisé pour faciliter des attaques de logiciels espions par une technique connue sous le nom d'« injection réseau ».

L'accès non réglementé aux infrastructures et aux données de télécommunication privées a aussi permis à la DGST de réaliser des attaques par injection réseau pour installer des logiciels espions et suivre librement

les données de localisation. En fournissant des informations techniques d'identification à la DGST en dehors de toute procédure judiciaire, cet opérateur a également facilité les opérations de surveillance illégale menées par celle-ci.

La DGST et d'autres organismes utilisent aussi des outils moins sophistiqués sur le plan technologique, comme des micros ou des caméras cachés dans des logements, des voitures, des bureaux, des espaces publics et des lieux de détention. Des traceurs GPS permettent de suivre en permanence la localisation de la cible, que les agent-e-s de la DGST peuvent consulter sur une interface dédiée. Ces techniques sont utilisées en combinaison avec le recrutement de personnes en chair et en os chargées de rendre compte des activités des défenseur-e-s des droits humains faisant l'objet d'une surveillance illégale qui se trouvent dans leur quartier ou auxquels elles ont accès, par exemple des employé-e-s de cafés, des commerçant-e-s locaux ou des voisin-e-s.

Par ailleurs, les agent-e-s de la DGST procèdent à une surveillance vidéo par le biais des réseaux de caméras publiques, et peuvent accéder aux images de caméras privées grâce à un outil appelé NightHawk. Cet appareil de la taille d'une petite valise est produit par l'entreprise de cyber-renseignement israélienne Interionet.

Pour déployer tout cet éventail d'outils, la DGST s'appuie sur des organismes partenaires et sur de multiples techniques. Par exemple, le logiciel espion RCS a été déployé par infection physique des appareils, souvent *via* des clés USB, par des attaques menées, par exemple, pendant des transferts à l'aéroport ou par infection physique dans des cybercafés.

Des logiciels espions ont aussi été préinstallés sur des appareils mobiles qui ont ensuite été placés dans des magasins et vendus aux cibles.

S'il ne fait aucun doute que la mise en œuvre de pratiques de sécurité numérique renforcées peut rendre plus difficile la surveillance des défenseur-e-s des droits humains par la DGST, il n'en reste pas moins presque impossible d'échapper à ce vaste écosystème de surveillance compte tenu de la multitude de techniques utilisées.

## **L'UTILISATION DE CAMPAGNES DE DÉNIGREMENT POUR DISCRÉDITER LES DÉFENSEUR-E-S DES DROITS HUMAINS**

Ce rapport établit qu'un des principaux objectifs de la surveillance illégale des défenseur-e-s des droits humains est de les discréditer publiquement.

Dans plusieurs des cas étudiés, des informations privées recueillies par la DGST dans le cadre de ses opérations de surveillance contre des défenseur-e-s des droits humains ont par la suite fait l'objet d'une couverture médiatique et ont été utilisées dans des campagnes de dénigrement coordonnées contre les personnes concernées. Ces campagnes ont souvent été menées par des médias politiquement proches du pouvoir, comme Chouf TV, Barlamane et Le360, et un certain nombre d'entre elles ont inclus la diffusion de photos et de vidéos privées des cibles. Des campagnes de dénigrement à caractère sexuel ont été utilisées pour tenter de discréditer en particulier des femmes défenseuses des droits humains ou des femmes proches de journalistes et de défenseur-e-s des droits humains de premier plan. Bien qu'Amnesty International n'ait pas été en mesure de vérifier de façon indépendante la source des informations révélées par ces médias, la nature des contenus, notamment les images intimes et les communications privées, ainsi que l'absence apparente d'autres moyens plausibles par lesquels ces médias auraient pu se procurer ces contenus, laissent fortement à craindre que des informations obtenues au moyen de systèmes de surveillance aient été révélées ou transmises aux médias par les autorités marocaines, ou mises à leur disposition de toute autre manière.

Ces campagnes sont amplifiées en ligne. Des exemples de campagnes coordonnées de comportements non authentiques visant des défenseur-e-s des droits humains marocains sur les réseaux sociaux ont été identifiées à deux reprises par Meta, la maison mère de Facebook. Selon le témoignage d'une personne bien informée, ces campagnes sont soutenues par des commentateurs-trices financés par l'État, dont le rôle est de commenter les publications afin d'accroître la visibilité des campagnes de dénigrement en ligne.

Beaucoup de ces campagnes se sont poursuivies alors même que les défenseur-e-s des droits humains concernés avaient été emprisonnés, libérés ou graciés, ou même avaient quitté le Maroc.

En transmettant ou divulguant des données de surveillance aux médias, ou en soutenant directement les campagnes de dénigrement visant à harceler les défenseur-e-s des droits humains, le Maroc contrevient à son obligation de respecter le droit de ces défenseur-e-s au respect de leur vie privée. Par ailleurs, en vertu

du droit international relatif aux droits humains, les autorités marocaines doivent aussi protéger et mettre en œuvre les droits des défenseur-e-s des droits humains en prenant des mesures pour les protéger des campagnes de dénigrement menées par des acteurs privés, ainsi que pour créer un environnement sûr et favorable leur permettant de mener à bien leur travail dans le respect de leurs droits.

## HARCÈLEMENT JUDICIAIRE ET RÉPRESSION

Parallèlement à la surveillance illégale et aux campagnes de dénigrement diffamatoires, les défenseur-e-s des droits humains sont régulièrement la cible de poursuites judiciaires fondées sur des accusations motivées par des considérations politiques et/ou forgées de toutes pièces, d'arrestations, de placements en détention et de peines d'emprisonnement prononcées à la suite de procès inéquitables, et/ou poursuivis pour des actes que le droit international interdit de sanctionner.

Beaucoup de ces procès sont entachés de violations des droits des détenu-e-s et des droits fondamentaux garantissant un procès équitable. Souvent, les défenseur-e-s des droits humains sont confrontés à des accusations forgées de toutes pièces ou à des chefs d'inculpation érigeant en infraction leurs activités légitimes, en violation du droit relatif aux droits humains. Les militant-e-s sahraouis et les personnes ayant participé au mouvement de protestation du Hirak, né dans la région du Rif, ont été particulièrement pris pour cible en raison de leurs activités protestataires et militantes, qui leur ont valu des poursuites pour « atteinte à la sûreté intérieure de l'État ».

Ce rapport fait aussi état de cas dans lesquels les autorités ont exercé des pressions sur des défenseur-e-s des droits humains pour qu'ils fassent de faux témoignages contre d'autres défenseur-e-s.

Si certains des défenseur-e-s des droits humains ainsi visés ont été libérés ou graciés, beaucoup se trouvent toujours en détention.

## CONCLUSION

Depuis des décennies, des organisations de défense des droits humains recueillent des informations attestant d'une répression de la société civile au Maroc. Les journalistes et les militant-e-s, en particulier, travaillent dans un environnement extrêmement restreint et sont confrontés à diverses pratiques autoritaires, dont la surveillance illégale et le harcèlement judiciaire, souvent accompagnées de campagnes de dénigrement. Ces tactiques visent à réduire la dissidence au silence, à attaquer la liberté des médias, à affaiblir l'espace civique et à renforcer le pouvoir des autorités.

Ce rapport montre que les pratiques de surveillance de la DGST s'appuient maintenant sur un vaste éventail d'outils de surveillance numériques, et détaille comment ces outils ont permis aux autorités marocaines de s'ingérer dans tous les aspects de la vie des défenseur-e-s des droits humains. L'utilisation de ce type d'outils numériques constitue un pilier central du techno-autoritarisme : elle permet aux gouvernements de renforcer leurs capacités de contrôle en bafouant les droits de chacun-e au respect de la vie privée et à la liberté de réunion et d'expression. Les témoignages des défenseur-e-s des droits humains interrogés dans ce rapport montrent clairement les conséquences humaines de ces formes intrusives de surveillance.

Ce rapport explique également comment une diversité d'entreprises ont facilité et permis ces pratiques techno-autoritaires en continuant de fournir au Maroc des technologies numériques de surveillance très sophistiquées, tout en fermant les yeux sur les preuves établissant que ces outils avaient été utilisés pour commettre des violations des droits humains. Par exemple, depuis 2017, Amnesty International a publié plusieurs enquêtes sur les attaques illégales menées contre la société civile marocaine au moyen du logiciel espion Pegasus, attaques qui se sont poursuivies au moins jusqu'en novembre 2021. NSO Group prétend que son logiciel espion Pegasus sert uniquement à « enquêter sur des faits de terrorisme et de criminalité ». Or, les nombreuses enquêtes menées par Amnesty International et d'autres organisations de la société civile du monde entier ont démontré qu'il avait en réalité été utilisé à maintes reprises par des gouvernements contre des défenseur-e-s des droits humains, des journalistes et d'autres membres de la société civile. Ces recherches montrent que, au moins en ce qui concerne le Maroc, les membres de la société civile n'ont pas été simplement des victimes occasionnelles mais au contraire la principale cible de la DGST à partir du moment où elle a acquis ce logiciel espion, puisqu'ils ont représenté près des deux tiers des personnes visées durant les quatre premiers mois de son déploiement. Le rapport établit également que l'implication de NSO Group ne s'arrête pas à l'étape de l'achat. Le logiciel espion Pegasus n'est pas géré de façon autonome par le gouvernement client mais nécessite une maintenance et un support de l'entreprise pour continuer de fonctionner.

La pratique combinée de la surveillance illégale, du harcèlement judiciaire et des campagnes de dénigrement a un effet dissuasif important sur les défenseur-e-s des droits humains, ainsi que sur la société en général. L'instrumentalisation des technologies joue un rôle central dans la triple menace suivante : les défenseur-e-s des droits humains et les journalistes n'ont aucun moyen de savoir quand ils sont observés et enregistrés, exposent leurs familles et amis à des risques inconnus, et craignent d'être publiquement humiliés voire emprisonnés s'ils font entendre leur voix. En conséquence, beaucoup ont peur de le faire, et l'environnement devient de plus en plus hostile pour les opinions dissidentes.

Pourtant, nombre d'entre eux continuent de s'exprimer et tentent de demander des comptes aux responsables qui sont au pouvoir. Ce rapport présente leurs histoires, qui soulignent combien il est urgent que les autorités marocaines mettent un terme à l'impunité dont jouit la DGST, réforment leurs lois et pratiques, et fassent du Maroc un endroit sûr pour les journalistes et les défenseur-e-s des droits humains.

Les conclusions de ce rapport montrent que les autorités marocaines ne font pas le nécessaire pour protéger et mettre en œuvre les droits fondamentaux des défenseur-e-s des droits humains, tels que garantis par le droit international. Il illustre également le rôle essentiel joué par les lanceurs et lanceuses d'alertes dans la révélation des atteintes aux droits humains.

L'utilisation combinée, par les autorités marocaines, de la surveillance illégale, du harcèlement judiciaire et de la répression entraîne la violation de nombreux droits humains, notamment des droits au respect de la vie privée et à la liberté d'expression, d'association et de réunion pacifique.

Elle a aussi un profond effet dissuasif, provoquant chez les personnes visées des préjudices psychologiques, sociaux et professionnels, et dissuadant les autres ainsi que la société en général d'exercer leurs droits fondamentaux en toute légalité.

*Un mois avant la publication du présent rapport, Amnesty International a écrit aux autorités marocaines pour leur communiquer une synthèse de ses conclusions et les inviter à y répondre. Les autorités marocaines n'ont pas répondu.*

*Avant la publication de ce document, Amnesty International a également écrit aux entreprises mentionnées dans le rapport pour leur communiquer ses principales conclusions concernant leurs activités. Verint a répondu en indiquant : « Verint s'est séparée de cette branche d'activité le 1<sup>er</sup> février 2021. Les demandes des médias doivent être adressées à Cognyte Software Ltd. » Amnesty International n'a reçu de réponse d'aucune des autres entreprises.*

## PRINCIPALES RECOMMANDATIONS

### AUX AUTORITÉS MAROCAINES :

- Libérer les personnes emprisonnées pour des faits relevant de l'exercice légal de leurs droits fondamentaux.
- Cesser immédiatement de surveiller les défenseur-e-s des droits humains et les journalistes qui exercent en toute légalité leurs droits humains et respecter et garantir leur droit au respect de la vie privée.
- Entreprendre les réformes législatives nécessaires pour mettre en place un cadre relatif aux droits humains réglementant la surveillance, qui permette d'empêcher les atteintes aux droits humains dans la pratique, notamment celles commises par la DGST et d'autres organes de sécurité. Tant qu'un tel cadre réglementaire n'aura pas été mis en place, il conviendra d'appliquer un moratoire sur l'achat, la vente, le transfert et l'utilisation d'équipements de surveillance.
- Diligenter une enquête indépendante, efficace et systémique sur la DGST, y compris sur tous les cas de surveillance illégale signalés, demander des comptes aux responsables et offrir un recours effectif aux victimes, notamment de véritables voies de réparation judiciaire, pour les préjudices physiques et psychologiques qu'elles ont subis, ainsi que pour la perte de leurs moyens de subsistance.
- Mettre un terme à toute forme de participation par des agent-e-s gouvernementaux à des campagnes de dénigrement diffamatoires contre des défenseur-e-s des droits humains et des

journalistes, notamment sur les réseaux sociaux, et prendre des mesures pour protéger ces personnes de telles campagnes dans les médias.

#### **À TOUS LES ÉTATS :**

- Ne pas accorder d'autorisations d'exportation au Maroc de logiciels espions, outils de criminalistique numérique et autres technologies portant atteinte à la vie privée tant qu'une enquête approfondie, indépendante et efficace n'aura pas été menée sur la surveillance illégale de journalistes, de militant-e-s politiques et de défenseur-e-s des droits humains, et tant qu'un système de garanties capable d'empêcher les atteintes aux droits humains dans la pratique ne sera pas en place.
- Interdire aux entreprises de produire, vendre, transférer ou assurer le support des logiciels espions hautement intrusifs, dont les fonctionnalités ne peuvent pas être restreintes et dont l'usage ne peut pas faire l'objet d'un contrôle indépendant.

#### **AUX ÉTATS DEPUIS LESQUELS SONT MENÉES DES ACTIVITÉS D'EXPORTATION, DE VENTE OU DE COURTAGE DE TECHNOLOGIES DE SURVEILLANCE ET AUTRES TECHNOLOGIES PORTANT ATTEINTE À LA VIE PRIVÉE :**

- Enquêter sur l'exportation, la vente, le transfert ou le courtage des technologies impliquées dans les violations signalées dans ce rapport, et annuler les licences d'exportation s'il existe des preuves ou des risques importants que ces technologies soient liées à des atteintes aux droits humains.
- Empêcher les entreprises de procéder au courtage à destination du Maroc de technologies de surveillance et d'autres technologies portant atteinte à la vie privée, ou de faciliter la vente, le transfert ou le support de telles technologies dans ce pays, tant qu'une enquête approfondie, indépendante et efficace n'aura pas été menée sur la surveillance illégale de journalistes, de militant-e-s politiques et de défenseur-e-s des droits humains, et tant qu'un système de garanties capable d'empêcher les atteintes aux droits humains dans la pratique ne sera pas en place.

#### **AUX ENTREPRISES IMPLIQUÉES DANS LA FOURNITURE AU MAROC DE TECHNOLOGIES DE SURVEILLANCE ET D'AUTRES TECHNOLOGIES PORTANT ATTEINTE À LA VIE PRIVÉE :**

- Cesser toutes leurs activités de vente, d'exportation, de transfert ou de courtage de technologies de surveillance à destination du Maroc, ainsi que tout autre support en la matière, tant qu'une enquête approfondie, indépendante et efficace n'aura pas été menée sur la surveillance illégale de journalistes, de militant-e-s politiques et de défenseur-e-s des droits humains, et tant qu'un système de garanties capable d'empêcher les atteintes aux droits humains dans la pratique ne sera pas en place.
- Mettre en œuvre des mécanismes solides de réparation sous diverses formes, dont l'indemnisation des cibles de surveillance illégale.

#### **AUX OPÉRATEURS DE TÉLÉCOMMUNICATION (TÉLÉPHONIE MOBILE OU INTERNET) DU MAROC :**

- Faire preuve de la diligence requise en matière de droits humains afin d'identifier, de prévenir et d'atténuer les conséquences négatives de leurs activités sur les droits humains et de rendre des comptes, notamment en ce qui concerne la surveillance, en particulier en évaluant soigneusement les risques qu'implique le partage illégal de données et en rendant publiques ces évaluations des risques.
- Mettre au point des mécanismes accessibles, sûrs et efficaces de traitement des plaintes relatives aux technologies de surveillance et à leur usage. Ces mécanismes doivent être disponibles dans tous les pays et des mesures doivent être prises pour qu'ils soient accessibles à toutes et tous.

**AMNESTY INTERNATIONAL  
EST UN MOUVEMENT  
MONDIAL DE DÉFENSE DES  
DROITS HUMAINS.  
LORSQU'UNE INJUSTICE  
TOUCHE UNE PERSONNE,  
NOUS SOMMES TOUS ET  
TOUTES CONCERNÉ·E·S.**

**NOUS CONTACTER**



[info@amnesty.org](mailto:info@amnesty.org)



+44 (0)20 7413 5500

**PRENDRE PART À LA CONVERSATION**



[www.facebook.com/AmnestyGlobal](https://www.facebook.com/AmnestyGlobal)



[@Amnesty](https://twitter.com/Amnesty)

# « ON COMMENCE PAR LE VERDICT »

## AU CŒUR DE L'APPAREIL DE SURVEILLANCE MAROCAIN

### SYNTHÈSE

Ce rapport analyse l'écosystème de surveillance qui permet aux autorités marocaines de recourir à des tactiques répressives pour harceler, discréditer et au bout du compte réduire au silence les défenseur·e·s des droits humains. Il décrit le rôle joué par les services marocains de renseignement intérieur – la Direction générale de la surveillance du territoire (DGST) – dans les opérations de surveillance menées contre la société civile. Ces opérations sont souvent accompagnées de campagnes de dénigrement dans les médias proches du pouvoir. Les pratiques techno-autoritaires utilisées par la DGST, telles que détaillées dans ce rapport, sont rendues possibles et facilitées par diverses entreprises. Ce rapport contient aussi une analyse exhaustive du système du logiciel espion Pegasus, et de la manière dont il a été utilisé par les autorités marocaines pour attaquer des défenseur·e·s des droits humains et des journalistes, aussi bien au Maroc que dans d'autres pays.