



« UNE PRISON NUMÉRIQUE »

SURVEILLANCE ET RÉPRESSION DE LA SOCIÉTÉ CIVILE EN SERBIE

SYNTHÈSE

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 2020

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>

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

www.amnesty.org/fr.

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

L'édition originale en langue anglaise de ce document a été publiée en 2020

par Amnesty International Ltd, Peter Benenson House,

1 Easton Street,

Londres WC1X 0DW, Royaume-Uni.

Index : EUR 70/8814/2024

L'édition originale a été publiée en anglais

amnesty.org/fr



Photo de couverture : Composition créée par Amnesty International avec des photos fournies par Svi Će et Dragan Gmizic

**AMNESTY
INTERNATIONAL**



SYNTHÈSE

En février 2024, Slaviša Milanov, journaliste indépendant qui couvre l'actualité locale de Dimitrovgrad (Serbie), a été conduit au poste de police après ce qui semblait être un contrôle routier de routine.

Une fois libéré, le journaliste a remarqué que son téléphone, qu'on lui avait demandé de laisser à l'accueil du poste, réagissait bizarrement et que les données mobiles et le wifi avaient été désactivés. Conscient que cela pouvait être un signe de piratage et qu'en Serbie les journalistes étaient susceptibles d'être surveillés, Slaviša Milanov a demandé au Security Lab d'Amnesty International d'analyser son téléphone.

L'équipe a fait deux découvertes inattendues. Premièrement, des indices techniques ont révélé qu'un produit de Cellebrite avait été utilisé pour débloquer le téléphone. Il s'agissait d'un outil criminalistique utilisé par des services de police aux quatre coins du monde, qui leur permet d'extraire toutes les données d'un appareil. Cellebrite affirme avoir mis en place des mesures strictes pour éviter que ce produit soit employé à mauvais escient, mais cette découverte montre bien qu'il a été utilisé sur le téléphone d'un journaliste en dehors de toute procédure légale. Slaviša Milanov n'a donné le mot de passe de son appareil Android à personne et personne ne le lui a demandé. Les autorités ne lui ont pas fait savoir qu'elles souhaitaient fouiller son téléphone et elles n'ont donné aucun motif juridique pour justifier cette fouille. Slaviša Milanov ignore quelles données ont été extraites de son appareil.

La deuxième découverte est encore plus étonnante. Amnesty International a trouvé des éléments indiquant que le téléphone avait été piraté à l'aide d'un logiciel espion jusqu'alors inconnu, que l'équipe a baptisé « NoviSpy ». NoviSpy permet d'extraire d'un téléphone infecté des données personnelles confidentielles et d'allumer le microphone ou la caméra de l'appareil à distance. Des indices montrent que le logiciel espion a été installé lorsque le téléphone de Slaviša Milanov était entre les mains de la police serbe et que cette infection n'aurait pas été possible sans l'utilisation de Cellebrite pour débloquer l'appareil. Deux technologies hautement intrusives ont été utilisées pour attaquer le téléphone d'un journaliste indépendant, dévoilant pratiquement toute sa vie numérique aux autorités serbes.

Mais l'histoire ne s'arrête pas là. Amnesty International a poursuivi ses recherches, qui ont révélé l'ampleur de la surveillance numérique en Serbie. Les autorités y utilisent au moins trois différentes sortes de logiciels espions et se servent régulièrement de la technologie de criminalistique numérique de Cellebrite, particulièrement sophistiquée, à mauvais escient.

Ce rapport est une étude de cas sur la surveillance technologique et les tactiques numériques déployées par les autorités serbes pour contrôler et réprimer la société civile. La Serbie est un exemple typique de système dans lequel des outils de ce genre peuvent faciliter la répression numérique et qui peut se reproduire dans d'autres pays et d'autres contextes, ce qui est sans doute déjà le cas.

La publication de ce rapport coïncide avec une intensification de la répression et un accroissement de l'hostilité envers la liberté d'expression et le débat dans le pays. La Serbie a été le théâtre de plusieurs grandes vagues de manifestations contre le gouvernement depuis 2021. Les autorités y réagissent de plus en plus durement, en menant des campagnes de dénigrement virulentes et soutenues contre des organisations non gouvernementales (ONG), des médias et des journalistes critiques et en harcelant juridiquement les citoyen·ne·s qui s'organisent pacifiquement et s'engagent dans des activités politiques dissidentes.

Pour ce rapport, Amnesty International a interviewé longuement des membres de la société civile serbe et effectué des recherches de criminalistique numérique très techniques pour exposer les pratiques de surveillance mise en œuvre par les autorités du pays. En révélant ces tactiques, Amnesty International cherche à donner à la société civile les moyens de demander des comptes pour les actes de surveillance

illégaux dont elle est victime tout en levant le voile du secret et en réduisant l'asymétrie qui en résulte en termes d'accès à l'information. L'opacité de la surveillance numérique et le sentiment de toute-puissance et d'impunité peuvent encourager un appareil d'État répressif à adopter ce genre de pratiques, qui ont des conséquences dévastatrices sur la santé de la société dans son ensemble.

Le rapport montre que la Serbie utilise couramment des logiciels espions intrusifs, dont le logiciel Pegasus de NSO Group et un nouveau système produit en Serbie et visant les appareils Android, que nous dévoilons ici pour la première fois sous le nom de NoviSpy. La police serbe et les services de renseignements nationaux, connus dans le pays sous le sigle BIA (Bezbedonosno-informaciona Agencija), ont utilisé le logiciel espion NoviSpy et des outils de criminalistique de Cellebrite contre des militant-e-s de groupes de réflexion indépendants, des manifestant-e-s pacifiques et des journalistes indépendants.

Utilisés conjointement, ces outils démultiplient les capacités de l'État pour collecter des données, soit en secret, avec des logiciels espions, soit ouvertement, en utilisant les technologies d'extraction de données de téléphones mobiles de Cellebrite de manière illégale et illégitime. Les autorités serbes emploient systématiquement ces outils contre les manifestant-e-s pacifiques, qui sont déjà trop souvent incriminés injustement pour leur militantisme. Cette surveillance numérique et ces collectes de données pratiqués illégalement contre la société civile violent le droit au respect de la vie privée et à la protection des données personnelles des personnes visées et ont de profondes répercussions sur d'autres droits et libertés, tels que la liberté d'expression, d'association et de réunion pacifique.

Le rapport s'appuie sur des interviews approfondies menées auprès de 13 personnes qui ont été directement ciblées par un logiciel espion, un produit d'extraction de données mobiles ou une autre forme de surveillance numérique et de 28 membres de la société civile de différentes régions de Serbie, dont la précieuse contribution nous permet de mieux comprendre les difficultés croissantes auxquelles ils se heurtent. Ces témoignages sont corroborés par l'analyse technique détaillée des téléphones mobiles d'une dizaine de militant-e-s et de journalistes réalisée par le Security Lab d'Amnesty International, qui a utilisé des outils de criminalistique numérique mis au point par Amnesty International, notamment la boîte à outils de vérification mobile (Mobile Verification Toolkit, MVT) et AndroidQF, pour collecter et analyser les indices matériels dévoilés dans ce rapport.

LES LOGICIELS ESPIONS QUI MENACENT LA SOCIÉTÉ CIVILE SERBE

Le rapport brosse dans le détail un historique de l'utilisation ou de l'acquisition de logiciels espions extrêmement intrusifs (de Finfisher, NSO Group et Intellexa, notamment) par les autorités serbes au cours des dix dernières années.

L'étude montre que le logiciel espion NoviSpy a été installé en cachette sur le téléphone d'au moins trois militant-e-s et un journaliste indépendant alors qu'ils se trouvaient dans les locaux de la police serbe ou de la BIA pour une entrevue à caractère informatif. Les téléphones ont été infectés à un moment où ils avaient soi-disant été déposés dans un casier. Cette tactique particulièrement trompeuse consistant à installer un logiciel espion en cachette pendant un entretien semble être courante. Des éléments techniques portent à croire que NoviSpy a été installé sur des dizaines, voire des centaines d'appareils au cours des dernières années. Et ce piratage ne se limite sans doute pas au ciblage illégal de la société civile.

En octobre 2024, une personne qui militait au sein de l'ONG Krokodil, basée à Belgrade, a été invitée à se rendre au bureau de la BIA pour apporter des informations concernant une attaque contre son organisation. Pendant l'entretien, son téléphone est resté sans surveillance hors de la salle d'audition. Le Security Lab d'Amnesty International a par la suite découvert des éléments indiquant que c'est à ce moment-là que le logiciel espion Android NoviSpy avait été installé sur le téléphone. Moins sophistiqué que les logiciels espions du commerce comme Pegasus, NoviSpy donne néanmoins aux autorités serbes de grandes capacités de surveillance une fois installé sur le téléphone de la victime. Outre Slaviša Milanov et la personne membre de Krokodil, Amnesty International a trouvé des éléments attestant que le logiciel avait été installé ou failli être installé sur le téléphone d'au moins deux autres militant-e-s de la société civile serbe.

NSO Group, qui a développé le logiciel Pegasus, n'a pas confirmé que la Serbie faisait partie de sa clientèle. Le groupe a néanmoins déclaré qu'il « prend très au sérieux la responsabilité qui lui incombe de respecter les droits fondamentaux et est fermement déterminé à éviter de causer la moindre incidence négative sur les droits humains, d'y contribuer, ou d'y être directement lié » et qu'il compte « examiner attentivement toute allégation faisant état d'une utilisation à mauvais escient de [ses] produits. »

LIENS ENTRE LE LOGICIEL ESPION NOVISPY ET LA BIA

L'analyse des échantillons de l'application NoviSpy trouvés dans les appareils infectés a révélé que tous communiquaient via des serveurs hébergés en Serbie, pour obtenir des instructions et extraire des données. L'un de ces échantillons était notamment configuré pour se connecter à une plage d'adresses IP directement associée à la BIA. Les recherches ont également montré que les données de configuration intégrées dans cet échantillon étaient associées à un-e employé-e de la BIA en particulier, qui avait participé aux tentatives de la Serbie de se procurer un logiciel espion Android auprès de Hacking Team, une entreprise de logiciels espions qui n'existe plus.

Ces importantes erreurs de sécurité et le fait que, dans de nombreux cas, le logiciel espion ait été installé pendant des entretiens avec des agents de la BIA permettent à Amnesty International d'attribuer avec un degré élevé de certitude ces campagnes d'espionnage aux autorités serbes et en particulier à la BIA.

UTILISATION ABUSIVE DES OUTILS DE CRIMINALISTIQUE NUMÉRIQUE DE CELLEBRITE

Le rapport révèle également que la technologie d'extraction de Cellebrite est fréquemment utilisée de manière illégitime pour télécharger des données personnelles des téléphones de journalistes et de personnes ayant organisé des manifestations. Grâce aux données obtenues à l'aide de ces outils, les autorités peuvent cartographier les réseaux de relations des mouvements de protestation, récupérer des conversations cryptées sur des applications comme Signal et Telegram et extraire des informations stockées dans le *cloud*. La possibilité de télécharger ce qui constitue, au fond, toute la vie numérique d'une personne à l'aide de l'UFED de Cellebrite et d'autres outils criminalistiques similaires pose d'énormes risques en matière de droits humains si ces outils ne sont pas soumis à un contrôle strict. En Serbie, le contrôle judiciaire de ces outils est insuffisant et l'utilisation que fait l'État des produits criminalistiques de Cellebrite met gravement en péril les droits fondamentaux.

Dans au moins deux cas sur lesquels Amnesty International a recueilli des informations, les autorités serbes ont utilisé l'UFED de Cellebrite et des exploits associés pour contourner en cachette les paramètres de sécurité d'un téléphone et l'infecter avec le logiciel espion NoviSpy. Ces infections, qui ont également été menées pendant des entretiens avec la police ou la BIA, n'auraient pas été possibles sans l'utilisation d'une technologie aussi sophistiquée que l'UFED de Cellebrite pour contourner le chiffrement des dispositifs. La sphère militante s'inquiète depuis longtemps de ces logiciels espions installés pendant des entretiens avec la police, mais Amnesty International pense que c'est la première fois que des techniques criminalistiques permettent de constater des infections rendues possibles par l'utilisation de la technologie de Cellebrite.

Cette étude a également révélé une faille de jour zéro sur Android permettant une élévation de privilèges utilisée par l'UFED de Cellebrite, dont la réparation a permis de protéger des millions d'appareils. Amnesty International a identifié cet exploit en collaboration avec l'équipe de recherche en sécurité de Google, en analysant attentivement les journaux d'exploitation criminalistique trouvés sur le téléphone d'une personne détenue par les autorités serbes après avoir organisé une manifestation.

RÉPRESSION CONTRE L'ESPACE CIVIQUE EN SERBIE

Cette surveillance numérique se déroule dans un contexte de répression croissante et de régression de la liberté d'expression. Depuis 2021, le pays a été le théâtre de nombreuses manifestations contre le gouvernement, que les autorités ont réprimées de plus en plus durement. Les attaques de l'État contre la société civile se sont nettement intensifiées après les manifestations massives organisées dans tout le pays en juillet et août 2024 contre l'extraction de lithium et l'accord passé entre la Serbie et l'Union européenne (UE) sur l'accès aux matières premières. En août, TV Informer, chaîne progouvernementale très regardée, a diffusé de longs reportages selon lesquels une quarantaine d'ONG « financées par l'étranger », qualifiées de « mercenaires », menaient « une guerre particulière contre la Serbie » sur l'ordre de bailleurs de fonds extérieurs. De hauts responsables, dont le président, des membres du Parlement et la gouverneure de la banque centrale, ont par la suite mis de l'huile sur le feu en se faisant l'écho de ces déclarations diffamatoires.

Au même moment, des militant-e-s qui avaient participé aux manifestations contre l'extraction du lithium ou qui en avaient parlé ont été arrêtés et poursuivis pour des chefs d'inculpations infondés mais très graves comme celui d'« incitation au renversement violent de l'ordre constitutionnel », infraction pénale passible de huit ans d'emprisonnement. D'après des militant-e-s et des avocat-e-s interrogés pour ce rapport, la police

fonde souvent ces poursuites sur des messages publiés sur les réseaux sociaux, des propos tenus ou sur le simple fait que les personnes visées aient participé à des manifestations. Selon Civic Initiatives, au moins 33 personnes ont été arrêtées ou détenues pendant les manifestations du mois d'août et soumises à de longs interrogatoires, des fouilles de leur domicile et des saisies de leurs téléphone et ordinateur. Au moment de la publication de ce rapport, aucune de ces personnes n'était officiellement inculpée.

Amnesty International s'est entretenue avec neuf militant-e-s ayant fait l'objet d'une détention ou d'un interrogatoire entre juillet et novembre 2024 et dont le téléphone ou l'ordinateur a été saisi par la police et soumis à des recherches approfondies, dont une extraction de données numériques, afin de permettre au ministère public de décider d'engager ou non des poursuites. Les militant-e-s soupçonnent que ces mesures intrusives, qui semblent être légales en Serbie, ont davantage pour objectif de permettre à la police et aux services de sécurité d'en savoir plus sur leurs réseaux de relations et leurs intentions que de mener des poursuites.

UNE SURVEILLANCE NUMÉRIQUE MAL ENCADRÉE JURIDIQUEMENT ET PEU CONTRÔLÉE

La loi serbe prévoit l'application de mesures exceptionnelles (notamment la surveillance secrète des communications) et précise les circonstances dans lesquelles ces mesures peuvent être prises. Mais elle ne reconnaît pas ou ne réglemente pas suffisamment le déploiement de technologies de pointe telles que les logiciels espions et d'autres outils de criminalistique numérique permettant de collecter de nombreuses données personnelles. Cette lacune laisse la porte ouverte aux abus, notamment à des fins politiques.

Les dispositions génériques régissant l'application de mesures exceptionnelles figurant dans différentes lois ne sont pas suffisamment claires et ne prévoient pas de véritables garanties contre l'utilisation à mauvais escient de technologies de surveillance numérique, qui sont bien plus intrusives et moins ciblées que les techniques de surveillance des communications classiques (les écoutes téléphoniques, par exemple). Même un mécanisme de contrôle judiciaire préalable tel qu'une décision de justice précisant les mesures de surveillances pouvant être appliquées, leur durée exacte et leur cible ne constituerait pas une protection efficace contre les outils de surveillance numériques les plus sophistiqués, en particulier les logiciels espions, qui permettent d'avoir un accès total et incontrôlé aux données, messages, images, fichiers et métadonnées d'un appareil.

D'autant que, dans un contexte où le gouvernement semble avoir une influence excessive sur les tribunaux et le parquet et où la captation de l'État soulève des inquiétudes, les moyens de contrôler l'application de ces mesures spéciales, qui peuvent sembler suffisants en théorie, sont inutiles ou inefficaces dans la pratique.

Nous avons fait part des conclusions de ce rapport au gouvernement serbe, qui n'a pas souhaité faire de commentaire.

UN EFFET DISSUASIF

La surveillance numérique a non seulement des conséquences dévastatrices sur le droit au respect de la vie privée, mais elle affecte aussi profondément les droits à la liberté d'expression, d'association et de réunion pacifique. Des personnes de la sphère du militantisme serbe ont expliqué à Amnesty International que, lorsqu'elles avaient appris qu'elles avaient été surveillées, elles s'étaient senties agressées, vulnérables et seules et qu'elles avaient changé ou envisagé de changer de comportement. Certaines sont devenues plus réticentes à évoquer publiquement des problèmes controversés, et d'autres ont décidé de faire profil bas, voire d'abandonner toute forme de militantisme.

Lorsque Slaviša Milanov a appris qu'il avait été pris pour cible, il s'est demandé avec inquiétude si certaines de ses sources étaient en danger. Il a dû changer sa manière de faire des recherches et de contacter des sources pour ses articles :

« Je ne peux plus utiliser de téléphone ni de courriels. Je dois trouver d'autres façons de parler avec les gens, y compris quand c'est en personne. En général, je le fais uniquement dans des lieux publics et en groupe, ce qui n'est évidemment pas idéal. »

Pour « Goran », un militant victime de Pegasus qu'Amnesty International a interviewé, l'attaque a été source de profonds questionnements sur son travail.

« UNE PRISON NUMÉRIQUE »

SURVEILLANCE ET RÉPRESSION DE LA SOCIÉTÉ CIVILE EN SERBIE

Amnesty International

« J'ai remis en question mon engagement dans l'organisation. Je me suis demandé si je devais continuer, quelles conséquences cela aurait sur l'organisation, et j'ai envisagé d'arrêter. Une attaque comme celle-ci touche ton intégrité et ton attitude face au travail. Tu te demandes si tu es prêt à continuer malgré tout. Je me posais mille questions. »

« Goran » n'a pas quitté son organisation, mais il a dû mettre en place de nombreuses mesures de sécurité, à la fois dans sa vie personnelle et dans ses activités militantes.

« Si le gouvernement peut faire ce qu'il m'a fait, il peut aussi s'attaquer à quelqu'un d'autre. J'ai réalisé que les activités de toutes les organisations de la société civile étaient constamment surveillées par les autorités et que nous devons rester vigilants. »

Les organisations sont déjà soumises à de nombreuses pressions, et gérer des problèmes de sécurité numérique est une tâche supplémentaire qui les détourne de leur activité principale, a expliqué un-e militant-e de Krokodil à Amnesty International.

« Faire face à tant d'attaques à la fois nous occupe beaucoup et risque de nous affaiblir au point que nous ne pourrions plus fonctionner du tout... C'est probablement l'objectif. »

RESPONSABILITÉ DES ENTREPRISES ET AUTRES ACTEURS EN MATIÈRE DE DROITS HUMAINS

C'est aux États que revient la responsabilité première de faire respecter le droit relatif aux droits humains, mais les autres acteurs de la société, et notamment les entreprises, ont l'obligation de respecter les droits fondamentaux – où qu'elles opèrent dans le monde et dans le cadre de l'ensemble de leurs activités. Les entreprises doivent en particulier faire preuve de la diligence requise pour identifier, prévenir et atténuer les risques auxquels elles pourraient contribuer en matière de droits humains. Amnesty International estime qu'en Serbie, un certain nombre d'entreprises ont failli à leurs obligations dans ce domaine.

Par ailleurs, le ministère des Affaires étrangères norvégien, qui a offert l'UFED de Cellebrite à la Serbie, et le Bureau des Nations unies pour les services d'appui aux projets (UNOPS), qui a géré le don du gouvernement norvégien au ministère de l'Intérieur serbe, ont contrevenu au principe de diligence requise en omettant d'évaluer et d'atténuer les risques que cette technologie pouvait poser en matière de droits humains ou de fournir des garanties pour éviter une utilisation abusive. Sachant que la surveillance numérique est peu réglementée en Serbie, que des inquiétudes ont été soulevées quant à l'indépendance de la justice et que des menaces envers la société civile et les journalistes indépendants ne cessent d'être signalées, le gouvernement norvégien et l'UNOPS avaient la responsabilité d'effectuer les contrôles nécessaires avant de fournir une technologie aussi intrusive aux institutions serbes. En omettant de le faire, ils ont permis à la Serbie d'exercer une surveillance illégale et de porter atteinte aux droits au respect de la vie privée et à la liberté d'expression, d'association et de réunion pacifique de la population.

Le ministère des Affaires étrangères norvégien a réagi aux révélations de ce rapport en déclarant qu'il trouvait « très inquiétant que des outils de criminalistique numérique, acquis dans le cadre d'un projet financé par la Norvège, puissent avoir été utilisés à mauvais escient contre des membres de la société civile en Serbie ». Il a ajouté que « si ce fait était avéré, [cela] constituerait une violation manifeste des principes fondamentaux qui sous-tendent l'aide au développement norvégienne et de l'objectif accordé de cette aide aux autorités serbes ». Le ministère a précisé que l'UNOPS, qui était responsable de toutes les activités entrant dans le cadre de ce projet, devait mener une enquête approfondie sur ces allégations.

Cellebrite avait elle aussi la responsabilité de faire preuve de la diligence nécessaire pour que son produit n'ait pas de conséquences néfastes sur les droits humains. Sur son site Internet, l'entreprise affirme qu'elle prend « toutes les mesures nécessaires pour interdire l'utilisation ou l'accès » à ses solutions lorsqu'elles sont employées « d'une manière qui n'est pas conforme [au droit international], qui ne respecte pas [leurs] conditions d'utilisation ou qui n'est pas alignée sur les valeurs d'entreprise de Cellebrite ». Pourtant, toutes les informations disponibles à l'heure actuelle indiquent que Cellebrite n'a pas fait tout ce qui était en son pouvoir pour préserver les droits humains en Serbie. Comme le démontrent les recherches menées par Amnesty International dans le pays, l'utilisation du produit de Cellebrite a eu des répercussions négatives sur les droits fondamentaux de militant-e-s et de journalistes serbes. Et Cellebrite n'y est pas pour rien.

La firme n'a pas respecté les obligations qui lui incombent au titre des Principes directeurs relatifs aux entreprises et aux droits de l'homme, qui imposent aux sociétés privées de prévenir et d'atténuer les préjudices potentiels et réels que peuvent subir les défenseur-e-s des droits humains. Des politiques et des procédures plus efficaces sont donc nécessaires pour obliger les entreprises à faire preuve de la diligence

« UNE PRISON NUMÉRIQUE »

SURVEILLANCE ET RÉPRESSION DE LA SOCIÉTÉ CIVILE EN SERBIE

Amnesty International

requis en la matière. Par ailleurs, lorsqu'il s'avère qu'une société a contribué à de tels préjudices, celle-ci doit offrir des voies de recours aux personnes touchées.

Comme expliqué plus en détail dans le rapport complet, Cellebrite a répondu brièvement aux questions que nous lui avons envoyées au cours de l'étude en déclarant qu'elle n'était pas une entreprise de surveillance et ne vendait pas de technologies de cybersurveillance ni de logiciels espions. Cellebrite a décrit son produit comme « un outil d'investigation numérique [qui] dote les organes d'application des lois de la technologie nécessaire pour protéger et sauver des vies, accélérer la justice et préserver la confidentialité des données ». La firme a précisé que ses produits étaient « réservés à un usage légal et [nécessitaient] un mandat ou une autorisation pour être utilisées par forces de l'ordre pour mener des enquêtes dans le cadre de la loi lorsqu'une infraction a été commise. »

Avant la publication du rapport, Amnesty International a partagé les conclusions de celui-ci avec Cellebrite. « Nos solutions d'investigation numérique n'installent pas de logiciels malveillants et n'effectuent pas de surveillance en temps réel dans la même veine que les logiciels espions ou d'autres types de cyberattaques », a répondu la firme.

« Nous remercions Amnesty International de nous avoir signalé cette utilisation possiblement abusive de notre technologie. Nous prenons au sérieux toutes les allégations selon lesquelles un client pourrait avoir utilisé notre technologie d'une manière allant à l'encontre des conditions d'utilisation figurant explicitement et implicitement dans l'accord que nous avons passé avec celui-ci. »

« Nous avons ouvert une enquête sur les accusations exposées dans ce rapport. Si elles s'avéraient exactes, nous serions prêts à appliquer les sanctions qui conviennent, et notamment à mettre fin aux relations entre Cellebrite et les entités concernées. »

L'analyse détaillée des obligations de l'entreprise en matière de droits humains figure dans le rapport complet, et les réponses de Cellebrite y sont disponibles en annexe.

CONCLUSION ET RECOMMANDATIONS

Les révélations de ce rapport montrent bien comment un appareil d'État répressif peut combiner différentes pratiques de surveillance pour atteindre ses objectifs. Nos recherches font également la lumière sur des tactiques de surveillance émergentes telles que l'utilisation généralisée d'outils de criminalistique numérique intrusifs pour collecter des données concernant des manifestant-e-s pacifiques qui n'ont été inculpés d'aucune infraction. L'amélioration de la sécurité des dispositifs rendant les exploitations « zéro clic » et autres attaques à distance trop onéreuses, voire impossibles, les autorités risquent d'opter de plus en plus pour infecter les appareils avec des logiciels espions qu'elles installent physiquement. Certains États ont d'ailleurs proposé d'adopter des lois permettant aux autorités de s'introduire en secret chez les personnes visées pour installer des logiciels espions sur leurs dispositifs.

La Serbie doit s'engager à cesser immédiatement d'utiliser des logiciels espions hautement intrusifs et à mener rapidement des enquêtes indépendantes et impartiales sur tous les cas de surveillance numérique illégale qui lui ont été signalés. Le pays doit également prendre des mesures concrètes pour que les technologies numériques ne soient pas utilisées pour violer les droits humains. Il doit notamment mettre en place un cadre juridique prévoyant de véritables garanties de procédure, des systèmes de contrôle judiciaire efficaces et des mécanismes de réparation pour les victimes, et faire appliquer ce cadre strictement.

Cellebrite et les autres entreprises de criminalistique numérique qui conçoivent des technologies hautement intrusives et les fournissent aux organes d'application des lois et aux services de sécurité doivent appliquer rigoureusement les contrôles préalables requis pour que leurs produits ne soient pas utilisés de manière à contribuer à des violations des droits humains. Cellebrite doit enquêter sur la façon dont sa technologie a été employée en Serbie afin de détecter les conséquences néfastes que celle-ci pourrait avoir eues sur les droits des personnes. Elle doit traduire en actes son engagement à « prendre toutes les mesures nécessaires », y compris en ne renouvelant pas les licences concernées, afin d'empêcher toute entité malveillante d'utiliser ses solutions de manière non conforme au droit international.

La liste complète de nos recommandations est disponible à la fin du rapport.

**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



+44 (0)20 7413 5500

PRENDRE PART À LA CONVERSATION



www.facebook.com/AmnestyGlobal



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

« UNE PRISON NUMÉRIQUE »

SURVEILLANCE ET RÉPRESSION DE LA SOCIÉTÉ CIVILE EN SERBIE

SYNTHÈSE

Le présent rapport fait état de la surveillance technologique et des tactiques numériques déployées par les autorités serbes pour contrôler et réprimer la société civile. Il montre que la Serbie utilise couramment des logiciels espions intrusifs, dont le logiciel Pegasus de NSO Group et un nouveau système produit en Serbie et visant les appareils Android, que nous dévoilons ici pour la première fois sous le nom de NoviSpy. Il fait la lumière sur l'utilisation généralisée et à mauvais escient qui est faite des outils criminalistiques UFED de Cellebrite contre les écologistes et les personnes qui organisent des manifestations.