DOCUMENT DE RECOMMANDATIONS ADRESSÉES À L'UNION EUROPÉENNE EN VUE DE METTRE FIN À LA SURVEILLANCE CIBLÉE ILLÉGALE

Le Projet Pegasus a révélé comment des États ont ciblé des journalistes, des avocats et des personnalités politiques en ayant recours à un logiciel espion vendu par l'entreprise de cybersurveillance NSO Group. Le projet a exposé les répercussions néfastes des activités du secteur insuffisamment réglementé de la cybersurveillance sur les droits et le bien-être des personnes ciblées illégalement mais aussi de leurs amis, de leurs familles et de leurs collègues. Il a également mis en évidence les effets extrêmement déstabilisants de la cybersurveillance en matière de droits humains et de sécurité des environnements numériques en général. Les conclusions de l'enquête démontrent en particulier que les droits à la vie privée et à la liberté d'expression de personnes ont été bafoués de manière flagrante. Il est également important de souligner que l'utilisation non contrôlée des technologies de surveillance réduit le champ d'action des personnes qui œuvrent en faveur des droits humains et aggrave rapidement les menaces numériques qui pèsent sur elles. Les effets de celles-ci commencent par ailleurs à se faire sentir aussi hors ligne.

À la suite de ces révélations, la Haute-Commissaire aux droits de l'homme, ainsi que plusieurs experts des Nations unies ont appelé à l'adoption de mesures de manière urgente afin de lutter contre le problème de la surveillance ciblée illégale, et notamment à un moratoire sur la vente et le transfert des technologies de surveillance.

Les révélations du Projet Pegasus réfutent toutes les affirmations de NSO Group selon lesquelles ces attaques sont rares et liées à une utilisation peu scrupuleuse de sa technologie. Bien que l'entreprise affirme que son logiciel espion est utilisé exclusivement à des fins d'enquêtes pénales et liées au terrorisme, il est clair que sa technologie favorise des atteintes systématiques à grande échelle, dont NSO Group semble être complice.

Amnesty International souhaite attirer l'attention sur son rapport intitulé Uncovering the Iceberg : The digital surveillance crises wrought by states and the private sector, ainsi que sur une déclaration commune de plusieurs ONG appelant à l'adoption, au niveau de l'Union européenne, d'une nouvelle règlementation rigoureuse en matière de contrôle des exportations et à l'ouverture d'une enquête sur le rôle des États membres de l'Union européenne par rapport aux éléments révélés par le Projet Pegasus.

Dans le présent document, Amnesty International reprend les mesures essentielles à adopter de manière urgente afin que le secteur de la cybersurveillance soit mieux réglementé, que les auteurs de violations des droits humains soient amenés à rendre des comptes et qu'un contrôle plus indépendant soit exercé sur ce secteur opaque. Compte tenu des impacts nombreux et variés de ces révélations, nous appelons l'Union européenne et ses États membres à recourir à la fois aux instruments de politique interne et étrangère à leur disposition afin de remédier aux atteintes et de mettre en place une réglementation rigoureuse et efficace pour encadrer le secteur de la cybersurveillance.

Parmi ces mesures figurent notamment les recommandations suivantes adressées à l'Union européenne et à ses États membres.

Recommandations de mesures à adopter au sein de l'Union européenne

- **Les États membres doivent immédiatement instaurer un moratoire sur la vente, le transfert et l'utilisation des technologies de cybersurveillance.** Compte tenu de l'ampleur des révélations, il est urgent de suspendre les activités s'appuyant sur des technologies de surveillance de l'ensemble des États et des entreprises dans l'attente de l'adoption d'un cadre légal respectueux des droits humains.

- **Les États membres de l'Union européenne doivent offrir des recours effectifs aux victimes de surveillance ciblée illégale et veiller à ce que les auteurs de violations soient amenés à rendre des comptes. En outre, les États membres doivent s'engager à réformer les lois existantes qui font obstacle à l'octroi de réparations aux victimes de surveillance illégale et veiller à ce que des voies de recours judiciaires et non judiciaires soient concrètement disponibles.**

- **Les États membres de l'Union européenne doivent adopter et appliquer des lois imposant à toutes les entreprises de respecter les droits humains et de mettre en place des mesures de diligence raisonnable en matière de droits humains, conformément aux Principes directeurs des Nations unies.** Les entreprises doivent se voir imposer l'obligation d'identifier, de prévenir et d'atténuer les incidences négatives effectives et potentielles de leurs activités et dans l'ensemble de leur chaîne de valeur.

- **Dans leur législation nationale, les États membres doivent adopter et appliquer des textes imposant des protections contre les violations des droits humains et les atteintes résultant de la surveillance numérique illégale.** Ces textes devraient être conformes à l'arrêt de la Cour européenne des droits de l'homme de 2015 dans l'affaire Roman Zakharov c. Russie ainsi qu'aux Principes nécessaires et proportionnés et prévoir des mécanismes d'obligation de rendre des comptes, des motifs de recours et autres dispositions visant à offrir des voies de recours aux victimes d'atteintes résultant de la surveillance.

- **Les États membres et la Commission européenne doivent veiller à l'application rigoureuse des nouvelles règles en matière de contrôle des exportations entrées en vigueur le 9 septembre 2021 avec la refonte du règlement relatif aux biens à double usage.** Ils doivent notamment prendre des mesures immédiates en vue d'une part de faire valoir les obligations liées à la diligence raisonnable en matière de droits humains découlant du règlement relatif aux biens à double usage et d'autre part afin de construire un marché des technologies de cybersurveillance transparent dont les acteurs seront tenus de respecter de véritables protections en matière de droits humains.

    - Le nouveau règlement dispose que la Commission devra publier un rapport annuel adressé au Parlement et au Conseil. Ces rapports devront à tout le moins préciser les informations suivantes : nombre de demandes de licences par article, nom de l'exportateur, description de l'utilisateur final, de la destination et de l'utilisation prévue, agence gouvernementale impliquée, valeur de la licence et décision d'octroi ou de refus de la licence et justification de cette décision.

    - En outre, les mesures d'examen analytique des transactions mises en œuvre par les États membres devraient inclure une évaluation de la nature stratégique des articles et des risques qu'ils pourraient représenter pour les droits humains. Les autorités nationales devraient rendre compte de la mise en œuvre des obligations et des responsabilités en matière de diligence raisonnable et inciter les entreprises à informer le public de la portée, de la nature et des conclusions des procédures de diligence raisonnable en matière de droits humains qu'elles ont établies.

    - Les États membres doivent veiller à ce que les pays exportateurs offrent des recours

effectifs pour les violations des droits humains commises au moyen des technologies transférées. Les orientations qui seront publiées conformément aux dispositions de l'article 26, paragraphe 1 du règlement 2021/821/EU relatif aux biens à double usage devront préciser les exigences relatives aux programmes internes de conformité et à la diligence raisonnable attendue des exportateurs en vertu du règlement relatif aux biens à double usage sur la base des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme (Principes directeurs des Nations unies) et des Principes directeurs de l'OCDE à l'intention des entreprises multinationales.

- **Le Conseil et les États membres de l'Union européenne doivent répondre aux préoccupations liées au recours à des technologies de surveillance illégales par la Hongrie dans le cadre de la procédure en cours au titre de l'article 7 du Traité de l'Union européenne.** Ils doivent exhorter les autorités hongroises à remédier aux violations des droits fondamentaux et de l'état de droit.

- **Compte tenu de la surveillance ciblée illégale exercée en Hongrie, la Commission européenne devrait enquêter sur l'usage abusif des technologies de surveillance numérique par les autorités hongroises et déterminer si d'autres États membres de l'Union européenne ont également commis de telles atteintes.** Cette enquête devrait déterminer si la Hongrie et d'autres États membres respectent leurs obligations en vertu des traités de l'Union européenne, de la Charte des droits fondamentaux de l'Union européenne, du règlement général sur la protection des données, de la directive en matière de protection des données dans le domaine répressif et de la directive « vie privée et communications électroniques ». S'il est établi que la Hongrie déroge à ses obligations, la Commission européenne devra engager une procédure d'infraction.

- **La Commission européenne doit immédiatement diligenter une enquête portant sur l'ensemble des licences d'exportation accordées par l'Union européenne et ses États membres, et notamment en ce qui concerne l'autorisation générale d'exportation de l'Union européenne EU005 qui couvre les logiciels conçus pour le fonctionnement de matériels de contrôle et d'interception, et veiller à ce que les États membres de l'Union européenne retirent toutes les licences de commercialisation et d'exportation dans les situations où il existe un risque substantiel que ces technologies puissent faciliter des violations des droits humains.** NSO Group est implantée au Luxembourg et selon son propre rapport sur la transparence et la responsabilité 2021 (2021 Transparency and Responsibility Report), l'entreprise exporte également ses produits depuis la Bulgarie et Chypre. **S'il s'avère qu'en octroyant certaines licences, des États membres ont enfreint les normes régissant les exportations, la Commission européenne devra engager des procédures d'infraction.**

- **Le Parlement européen doit mener une concertation entre comités et entre partis afin d'évaluer convenablement les éléments internes et externes en jeu et exiger une réaction appropriée de la part de l'Europe.** Le Parlement européen et ses membres doivent exhorter la Commission européenne, le Conseil et les États membres de l'Union européenne à recourir aux instruments de politique interne et étrangère dont ils disposent pour remédier à ces atteintes et mettre en œuvre une réglementation rigoureuse et efficace visant à encadrer le secteur de la surveillance, notamment en reprenant l'ensemble des recommandations contenues dans ce document.

Recommandations de mesures à adopter par l'Union européenne et ses États membres dans le cadre de leur politique étrangère

- **L'Union européenne et ses États membres doivent adopter une position claire par rapport aux révélations du Projet Pegasus, y compris à travers des déclarations officielles.** Les atteintes exposées par le Projet Pegasus sont nombreuses et diverses et la véritable ampleur du ciblage opéré dépasse probablement le champ des cas révélés à ce jour. Compte tenu de son ambition de s'imposer en tant que puissance initiatrice de normes au niveau mondial, l'Union européenne peut et doit jouer un rôle en faveur de la protection des droits fondamentaux et du respect de l'état de droit dans le domaine numérique, sur son territoire et en dehors. Ces

principes trouvent leurs racines dans l'obligation, inscrite à l'article 21 du Traité de Lisbonne, qui incombe à l'Union européenne et à ses États membres de protéger et de promouvoir les droits fondamentaux partout dans le monde. En outre, ils sont conformes aux dispositions des Conclusions du Conseil relatives à « Façonner l'avenir numérique de l'Europe », du plan d'action de l'Union européenne en faveur des droits de l'homme et de la démocratie ainsi que des orientations de l'Union européenne dans le domaine des droits de l'homme. Des dirigeants de l'Union européenne, tels que la présidente de la Commission Ursula von der Leyen et le haut représentant Josep Borrell, ont déjà souligné l'importance de protéger la société civile et de préserver le droit à la vie privée et à la liberté d'expression en ligne à l'ère numérique. Dans leurs déclarations à venir, l'Union européenne et ses États membres doivent :

  - exprimer leur préoccupation à la suite des révélations des médias faisant état de l'utilisation courante et systématique du logiciel espion de NSO en vue de cibler des journalistes, des militants et des dirigeants de gouvernements et insister sur le fait que de telles pratiques sont inacceptables et enfreignent les droits à la liberté d'expression et de réunion pacifique et le droit à la vie privée ;

  - insister sur le fait que ces révélations mettent en évidence la nécessité d'introduire de manière urgente davantage de transparence dans le secteur de la surveillance et de renforcer la responsabilité juridique de ses acteurs ;

  - insister sur le fait que ces cas sont représentatifs de la progression, partout dans le monde, du recours à des attaques numériques et à la surveillance ciblée par des gouvernements cherchant à réduire au silence et à intimider des défenseurs des droits humains, des journalistes et des membres de la société civile ;

  - appeler les États à prendre des mesures de manière urgente en vue de renforcer la réglementation du secteur de la cybersurveillance et l'obligation de rendre des comptes lorsque des violations des droits humains sont commises et afin d'exercer un meilleur contrôle sur ce secteur insuffisamment réglementé.

- **Les États membres de l'Union européenne doivent organiser des rencontres bilatérales et entreprendre des démarches auprès des autorités compétentes dans les États tiers identifiés dans le cadre du Projet Pegasus en tant que client présumés de NSO Group :** le Projet Pegasus a identifié des personnes d'intérêt sélectionnées en tant que cibles potentielles dans les pays suivants : Arabie saoudite, Azerbaïdjan, Bahreïn, Émirats arabes unis, Hongrie, Inde, Kazakhstan, Mexique, Maroc, Rwanda et Togo. L'Union européenne et ses États membres doivent demander aux autorités de ces pays d'apporter des clarifications, et en particulier :

  - appeler les autorités compétentes à mener sans délai des enquêtes indépendantes, transparentes et impartiales sur tous les cas de surveillance illégale révélés par le Projet Pegasus et, le cas échéant, engager des démarches judiciaires pour offrir réparation aux victimes et demander des comptes aux responsables, conformément aux normes internationales relatives aux droits humains ;

  - souligner que le recours de la part d'un État à un logiciel espion à des fins de surveillance est légal uniquement lorsqu'il respecte un certain nombre de critères stricts, définis par le droit international relatif aux droits humains, et que cette surveillance doit être prévue par la loi et nécessaire, proportionnée et limitée dans le temps.

  - demander à ces États de remplir leurs obligations et engagements en vertu du droit international relatif aux droits humains, et notamment du Pacte international relatif aux droits civils et politiques et de la Déclaration des Nations unies sur les défenseurs des droits de l'homme ;

- évoquer avec les représentants des autorités au plus haut niveau les cas individuels de défenseurs des droits humains, de journalistes et de militants ciblés et offrir à ces personnes un appui politique, technique et autre, conformément aux orientations de l'Union européenne concernant les défenseurs des droits de l'homme, aux orientations de l'Union européenne relatives à la liberté d'expression et au plan d'action de l'Union européenne en faveur des droits de l'homme et de la démocratie.

- **Les États membres de l'Union européenne doivent appeler l'État d'Israël et les gouvernements de tous les pays exportateurs tiers à retirer immédiatement toutes les licences de commercialisation et d'exportation accordées à NSO Group et à mener une enquête indépendante, impartiale et transparence visant à déterminer l'ampleur de la surveillance numérique illégale.** Celle-ci devrait comporter une évaluation exhaustive du régime d'octroi des licences et prévoir sa refonte en conséquence en vue de garantir qu'il soit adapté en droit et en pratique et qu'il fasse barrage à de nouvelles atteintes aux droits humains liées à l'exportation d'équipements de cybersurveillance depuis leurs territoires. Enfin, les conclusions cette enquête devraient être rendus publics et des mesures devraient être prises en vue d'empêcher la perpétration de nouvelles atteintes. Ces États doivent également prendre les mesures qui s'imposent pour veiller à ce que NSO Group :

    - mette un terme immédiatement pour l'ensemble des États à l'utilisation, à la maintenance et à la vente de Pegasus dans l'attente d'une réglementation rigoureuse en matière de droits humains visant à encadrer convenablement la vente, le transfert et l'utilisation des technologies de surveillance ;

    - offre une indemnisation adaptée ou d'autres formes de réparation aux victimes d'une surveillance illégale exercée au moyen de produits de NSO Group ;

    - prenne des mesures proactives pour veiller à ne pas entraîner ni favoriser des violations des droits humains – notamment celles évoquées dans le cadre de l'enquête du Projet Pegasus – et pour y remédier si elles se produisent. Pour s'acquitter de cette responsabilité, NSO Group est tenu de faire preuve de diligence raisonnable en matière de droits humains et de faire le nécessaire pour que les défenseurs des droits humains, les journalistes et les membres de la société civile ne soient plus la cible d'une surveillance illégale.

- **Les États membres de l'Union européenne doivent s'investir dans les principales initiatives multilatérales, notamment au sein du Conseil des droits de l'homme des Nations unies, de l'Assemblée générale des Nations unies et lors des cycles d'examen périodique universel, visant à élaborer des normes rigoureuses en matière de droits humains afin d'encadrer le développement, la vente, le transfert et l'utilisation des équipements de surveillance et à définir des cibles inacceptables en matière de surveillance numérique.** Ils devraient à ce titre soutenir l'appel à un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies de surveillance.