



Fiche activité

# Surveillance numérique étatique et droits humains

© Amnesty International



**Éducation**  
aux droits humains

**AMNESTY**  
INTERNATIONAL



# Sommaire

|                                                          |           |
|----------------------------------------------------------|-----------|
| <b>Comprendre la surveillance de masse numérique</b>     | <b>3</b>  |
| <b>Analyse de vidéo</b>                                  | <b>3</b>  |
| Déroulement                                              | 4         |
| <b>Surveillance numérique étatique_“Affaire Pegasus”</b> | <b>6</b>  |
| <b>Etude de cas</b>                                      | <b>6</b>  |
| Déroulement                                              | 7         |
| <b>Imaginez un monde où...</b>                           | <b>9</b>  |
| <b>Annexe 1</b>                                          | <b>9</b>  |
| <b>Fiche “Histoire Pegasus”</b>                          | <b>10</b> |
| <b>Annexe 2</b>                                          | <b>10</b> |
| <b>Fiche d’analyse</b>                                   | <b>12</b> |
| <b>Annexe 3</b>                                          | <b>12</b> |
| <b>Badges rôles</b>                                      | <b>13</b> |
| <b>Annexe 4</b>                                          | <b>13</b> |

Ce livret propose deux activités permettant de sensibiliser les personnes participantes à la problématique de la surveillance numérique étatique, d’en comprendre les enjeux et d’analyser les impacts sur les droits humains.

# Comprendre la surveillance de masse numérique

## Analyse de vidéo

### Objectifs

- Susciter la réflexion collective sur la notion de « surveillance » et comprendre ce qu'est la surveillance de masse.
- Identifier les outils utilisés pour mettre en place une surveillance de masse numérique.
- Identifier les risques de la surveillance de masse pour les droits humains (vie privée, liberté d'expression, droit de réunion, non-discrimination, etc.).



**Durée**  
60 minutes



**Public**  
À partir de 14 ans  
De 10 à 20 personnes



### Matériel

- Vidéo projecteur et connexion internet.
- Vidéo introductive sur la surveillance de masse « *Dans leurs yeux : la France à l'heure de la reconnaissance faciale* » : <https://www.youtube.com/watch?v=JEE0cwOAKNg>
- Paperboard ou tableau.
- Feuilles / Post-it.



### Préparation

- Prendre connaissance des informations disponibles à la page : <https://www.amnesty.fr/liberte-d-expression/actualites/reconnaissance-faciale-neuf-questions-pour-comprendre>
- Installer le vidéoprojecteur et s'assurer que la vidéo fonctionne
- Préparer la salle pour que chaque personne puisse avoir une bonne visibilité de la projection.

### Déroutement

1. Présentez l'activité en expliquant aux personnes participantes qu'elle portera sur la surveillance de masse numérique et ses liens avec les droits humains.

En grand groupe, posez la question suivante :

- Selon vous, que veut dire "surveillance de masse" ?

N'hésitez pas à décomposer la phrase : *surveillance* puis *masse*.

Proposez la définition suivante, en la reliant aux réponses données : la surveillance, c'est l'observation ou l'espionnage des communications, des actions ou des déplacements d'une personne.

De masse : qui concerne l'ensemble de la population. Et si on ajoute "numérique", il s'agit du contrôle d'une population à l'aide d'outils numériques.

2. Proposez maintenant aux personnes participantes de comprendre les différentes formes que peut prendre la surveillance numérique. Pour cela, invitez le groupe à citer des outils ou technologies pouvant être utilisés à des fins de surveillance. Notez l'ensemble de leurs propositions sur un paperboard.

Complétez ensuite leurs réponses en apportant quelques exemples concrets. La surveillance numérique de masse peut notamment inclure :

- le contrôle des communications électroniques ;
- l'installation de caméras ;
- l'utilisation de systèmes de reconnaissance faciale ;
- la collecte de données biométriques ;
- ou encore le déploiement de drones.

3. Proposez maintenant au groupe de réfléchir plus spécifiquement à l'usage des caméras de surveillance et de la reconnaissance faciale. Pour alimenter la discussion, posez les questions suivantes :

- Pour vous, qu'est-ce que la reconnaissance faciale ?

(Par exemple : déverrouiller un téléphone, s'authentifier sur une application, être identifié dans un aéroport...).

Sur cette partie, n'hésitez pas à faire émerger ou préciser la différence entre :

- Reconnaissance faciale à des fins d'authentification, qui consiste à vérifier l'identité d'une personne en comparant son visage à sa propre donnée biométrique (comme pour déverrouiller un téléphone ou passer un contrôle à l'aéroport),
- Reconnaissance faciale à des fins d'identification, qui consiste à reconnaître une personne dans une foule en comparant son visage à une base de données.

- Quels avantages peuvent présenter les caméras de surveillance ?

(Exemples : sécurité, prévention de la criminalité, gestion et contrôle du trafic...)

- Quels désavantages ou risques peuvent découler de l'utilisation de la reconnaissance faciale via les caméras de surveillance ?

(Exemples : atteintes à la vie privée, dérives sécuritaires, discriminations, erreurs d'identification...)

## Surveillance numérique étatique et droits humains

Inscrivez les réponses aux deux dernières questions sur un paperboard sous forme de tableau à deux colonnes : Avantages / Désavantages.

**4.** A ce stade, annoncez au groupe que vous allez va regarder une vidéo d'Amnesty France d'environ 6 minutes pour mieux comprendre à quoi pourrait ressembler notre quotidien avec la reconnaissance faciale. Précisez qu'à la fin du visionnage, chaque personne pourra partager ce qui l'a le plus marqué. Invitez les personnes participantes à prendre des notes si elles le souhaitent et projetez la vidéo

**5.** Après un court moment de silence, invitez les personnes participantes à partager leurs réactions. Vous pouvez orienter la discussion avec quelques questions :

- Qu'est-ce qui vous a marqué ?
- Quelles émotions cette vidéo suscite-t-elle chez vous ?
- Quelle est, selon vous, la problématique principale soulevée ?
- Pourquoi la protection de la vie privée est-elle essentielle pour garantir d'autres droits fondamentaux, comme la liberté d'expression, la non-discrimination ou la liberté de réunion ?

**6.** Pour terminer, explique que les systèmes de reconnaissance faciale utilisés pour l'identification sont une forme de surveillance de masse et constituent, à ce titre, une violation du droit à la vie privée, garanti par l'article 12 de la Déclaration universelle des droits de l'homme : *"Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance."*

La reconnaissance faciale à des fins d'identification limite considérablement les droits à la liberté de réunion pacifique et à la liberté d'expression, car les individus se censurent lorsqu'ils savent être surveillés. De plus, ces systèmes touchent souvent plus durement certains groupes marginalisés, ce qui va contre l'égalité et la non-discrimination, droits fondamentaux de toute personne.



# Surveillance numérique étatique\_“Affaire Pegasus”

## Etude de cas

### Objectifs

- Comprendre la surveillance numérique ciblée et réfléchir à ses effets sur les droits humains.
- Analyser les dérives possibles liées à l’usage de technologies intrusives.



**Durée**  
50 minutes



**Public**  
À partir de 14 ans  
De X à X personnes



**Matériel**

- Paperboard ou tableau.
- Feuilles / Post-it.



**Préparation**

- Imprimer l’annexe 1 en format A3
- Imprimer 1 copie de l’annexe 2, 3 et 4 par le nombre de groupes que vous allez former (4 personnes par groupe). Par exemple, si vous avez 20 personnes participantes, imprimez 5 exemplaires de chaque annexe.

Attention : Cette activité ne peut être réalisée qu’après avoir traité les thématiques abordées dans l’activité précédente.

### Déroutement

1. Annoncez aux personnes participantes que vous allez poursuivre les réflexions autour de la surveillance numérique et ses impacts sur les droits humains mais en se concentrant sur la surveillance ciblée cette fois.

Pour mieux comprendre ce sujet, annoncez aux personnes participantes qu'elles vont travailler d'abord sur une activité qui fera appel à votre imagination, puis sur une étude de cas réelle.

À l'aide de l'affiche (voir annexe 1), illustrez la question suivante :

Imaginez un monde où :

- 50 000 téléphones sont potentiellement piratés avec un logiciel espion ou via des messages piégés pour accéder aux informations personnelles.
- 180 personnes journalistes répartis dans 20 pays différents sont des cibles d'espionnage potentiel dans le cadre de leur travail.
- Dans 40 pays, des personnes défenseuses des droits humains et militantes pourraient être surveillées quotidiennement par un logiciel espion.
- 14 responsables politiques et chefs d'État pourraient avoir été ciblés par un logiciel espion.
- 20 pays sont clients potentiels d'une entreprise qui commercialise un logiciel espion capable de tout cela.

Assurez-vous que tout le monde ait compris la définition de surveillance numérique ciblée : c'est le fait de

surveiller ou d'espionner des personnes ou des organisations précises en utilisant des outils numériques, sans le consentement des personnes. Cela peut, par exemple, passer par le piratage d'un téléphone avec un logiciel espion ou par l'envoi de messages piégés pour accéder aux informations d'une personne.

Posez les questions suivantes :

- Comment vous sentiriez-vous dans cette situation ?
- Pourquoi ce serait préoccupant ou dangereux ?
- Pensez-vous que cela pourrait arriver ? ...et pourtant, tout cela s'est vraiment passé !

Il s'agit de l'affaire Pegasus, un scandale mondial qui a révélé l'utilisation d'un puissant logiciel espion.

2. Pour découvrir cette affaire, invitez les personnes participantes à se diviser en groupes de 4 personnes. Distribuez à chaque groupe une fiche « histoire » (annexe 2) et une fiche d'analyse (annexe 3), à compléter. Précisez que l'objectif est de comprendre, en 20 minutes, ce qui s'est passé et d'analyser les répercussions sur les droits humains. Avant de commencer la lecture, précisez que chaque personne est invitée à participer à la réflexion et jouera un rôle désigné dans le groupe. Pour cela, distribuez à chaque groupe les rôles suivants (badges, annexe 4) :

- une personne lit le texte ;
- une personne contrôle le temps ;
- une personne note et lira les réponses ;
- une personne veille à ce que tout le monde participe aux discussions.

## Surveillance numérique étatique et droits humains

3. A la fin des 20 minutes, invitez chaque groupe à présenter brièvement les principaux éléments de leurs analyses. Notez sur un tableau ou un paperboard les points communs entre les groupes, afin de construire une vision collective de l'affaire Pegasus.

4. Clôturez l'activité en posant une dernière question :

- Qu'est-ce que cette affaire nous apprend ?

Aidez les personnes participantes à retenir que :

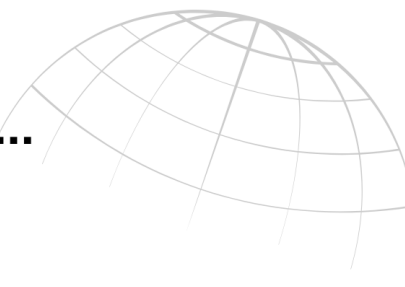
- Un outil numérique non contrôlé peut être utilisé de manière dangereuse et illégale.
- La surveillance ciblée met en danger plusieurs de nos droits (vie privée, liberté d'expression, etc.).
- Des réponses politiques et judiciaires sont nécessaires pour encadrer l'usage de ces outils.

Enfin, rappelez que si chaque personne a un rôle à jouer, les États ont la responsabilité principale de fixer des règles claires et de protéger les droits humains, aux côtés des décideurs et des entreprises qui conçoivent ou utilisent ces outils.

# Imaginez un monde où...

## Annexe 1

### Imaginez un monde où...



50 000 téléphones sont potentiellement piratés avec un logiciel espion ou via des messages piégés pour accéder aux informations personnelles.



180 personnes journalistes répartis dans 20 pays différents pourraient être des cibles d'espionnage potentiel dans le cadre de leur travail.



Dans 40 pays, des personnes défenseures des droits humains et militantes pourraient être surveillées quotidiennement par un logiciel espion.



14 responsables politiques et chefs d'État pourraient avoir été ciblés par un logiciel espion.



20 pays sont clients potentiels d'une entreprise qui commercialise un logiciel espion capable de tout cela.



# Fiche “Histoire Pegasus”

## Annexe 2

### *Pegasus : l'ombre d'un logiciel espion<sup>1</sup>*

En 2010, dans une zone industrielle au nord de Tel-Aviv, une petite entreprise israélienne de cybersécurité voit le jour : NSO Group. Ses fondateurs affirment vouloir développer des outils capables d'aider les gouvernements à lutter contre le terrorisme et le crime organisé.

Quelques années plus tard, entre 2011 et 2016, leurs ingénieurs mettent au point un logiciel espion : Pegasus. Invisible, indétectable, il peut s'introduire dans un téléphone portable sans que son propriétaire n'ait besoin de cliquer sur un lien. Une fois installé, le logiciel ouvre toutes les portes : messages, courriels, photos, localisation, appels, mais aussi caméra et micro, en temps réel.

En 2016, une première alerte retentit : les chercheurs de Citizen Lab (Université de Toronto) et l'entreprise Lookout découvrent que le militant des droits humains Ahmed Mansoor, basé aux Émirats arabes unis, a été ciblé grâce à Pegasus.

En mars 2017, un drame survient au Mexique : le journaliste Cecilio Pineda Brito, qui enquêtait sur le narcotrafic, est assassiné par des hommes armés. Son numéro figurait sur une liste de cibles de Pegasus.

En 2018, l'affaire prend une dimension internationale. Le journaliste saoudien Jamal Khashoggi est assassiné à Istanbul. Dans les jours qui suivent, Amnesty révèle que

---

<sup>1</sup> Ce texte a été élaboré à partir d'un travail de recoupement et de synthèse des informations provenant des sources suivantes :

<https://www.amnesty.fr/actualites/projet-pegasus-revelations-sur-un-systeme-mondial-de-surveillance/>  
<https://www.amnesty.org/fr/latest/news/2021/07/the-pegasus-project/>  
<https://securitylab.amnesty.org/fr/case-study-the-pegasus-project/>  
<https://www.amnesty.fr/actualites/projet-pegasus-revelations-mexique-logiciel-espion-nso-group/>  
<https://www.amnesty.fr/actualites/surveillance-revelations-sur-le-logiciel-espion-israelien-pegasus-nso-group/>  
<https://www.amnesty.fr/actualites/projet-pegasus-revelations-france-logiciel-espion-nso-group/>  
<https://www.amnesty.org/fr/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>  
<https://www.amnesty.org/fr/latest/news/2025/05/global-ruling-against-nso-group-in-whatsapp-case-a-momentous-win-in-fight-against-spyware-abuse/>

## Surveillance numérique étatique et droits humains

Pegasus avait été utilisé pour espionner sa fiancée, Hatice Cengiz, ainsi que plusieurs membres de sa famille.

En 2019, c'est au tour de WhatsApp de réagir : l'entreprise accuse NSO d'avoir utilisé une faille dans son application pour infecter 1 400 téléphones, appartenant notamment à des journalistes et des militant.es.

L'année 2021 marque un tournant : une vaste enquête journalistique, le *Pegasus Project*, révèle qu'une fuite contient 50 000 numéros de téléphone ciblés depuis 2016. Des journalistes, des militant.es, mais aussi des chefs d'État – dont Emmanuel Macron – apparaissent dans cette liste. En France, le parquet de Paris ouvre une enquête, et le président convoque un Conseil de défense exceptionnel.

Les conséquences s'enchaînent : en 2022, la Pologne admet officiellement avoir acheté Pegasus. Aux États-Unis, la Cour suprême autorise WhatsApp à poursuivre NSO Group.

En 2023 et 2024, d'autres révélations éclatent : en Espagne, l'ancien président catalan Pere Aragonès découvre qu'il a été espionné illégalement ; en Pologne, plus de 500 personnes sont identifiées comme victimes de Pegasus.

Finalement, en 2024 et 2025, la justice commence à frapper : Meta (propriétaire de WhatsApp) obtient plus de 167 millions de dollars de dommages et intérêts contre NSO. En Pologne, un ancien ministre de la Justice est arrêté pour son rôle dans l'utilisation illégale du logiciel.

# Fiche d'analyse

## Annexe 3

### 1. Comprendre l'affaire

Qu'est-ce que Pegasus et qui l'a développé ?

Comment fonctionne ce logiciel espion ?

Qui a été potentiellement visé par Pegasus ?

Pourquoi est-ce un problème pour les droits humains ?

### 2. Les acteurs et actrices de l'affaire

Quels sont les personnes/organisations/structures impliquées ? (États, entreprises, journalistes, personnes militantes, citoyennes, victimes...)

Que vivent ou subissent ces personnes ?

### 3. Les droits humains concernés

Quels droits humains ont été menacés ou violés ? (Exemples : vie privée, liberté d'expression, liberté de réunion, non-discrimination, droit à un recours, sûreté...)

### 4. Les enjeux et les dérives

Quelles dérives de la surveillance cette affaire montre-t-elle ?

### 5. Chercher des solutions

Quelles solutions pourraient limiter ces dérives ? (Exemples : lois plus strictes, contrôle indépendant, transparence, rôle des médias...)

## Badges rôles

### Annexe 4

