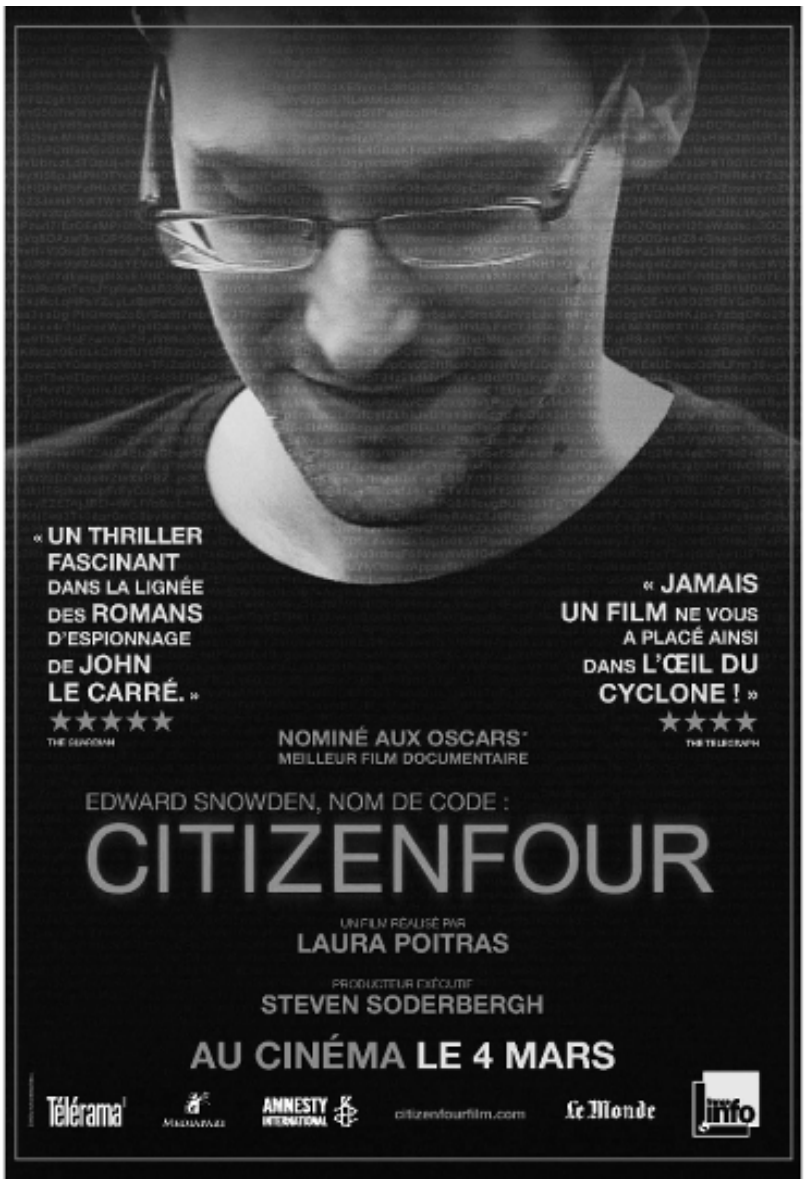
DOCUMENT INTERNE

Réf : SF 15 C4 04

# CITIZENFOUR

# un homme contre la surveillance de masse

***Dossier d'accompagnement pédagogique du film***




***« Mon objectif, c'est la transparence ».***

**Edward Snowden,**

# SOMMAIRE

## Citizenfour, un documentaire extraordinaire

## qui rejoint les préoccupations d'Amnesty International

Près de deux ans après les premières révélations de Snowden, *CITIZENFOUR*, revient avec brio sur la tension des jours qui ont suivi la publication des premiers documents, durant lesquels le lanceur d'alerte est resté reclus dans sa chambre d'hôtel alors que la tempête éclatait.

Le film, récompensé par l'Oscar du meilleur documentaire, dresse un réquisitoire aussi fouillé que terrifiant contre la surveillance de masse. Il ne devrait avoir aucun mal à convaincre les plus sceptiques qu'il est grand temps d'encadrer ces pratiques dans un contexte légal bien défini.

Derrière le scandale international des révélations de Snowden, il donne à comprendre les enjeux et risques immenses qu'un système de surveillance global, à l'ère numérique, hors de tout contrôle et de toute légalité, fait peser sur notre vie privée et sur nos libertés.

Il donne aussi à voir qui est Edward Snowden, ses motivations, et le cheminement intellectuel et moral qui l'a amené à mettre en péril le confort matériel de sa vie antérieure pour dénoncer des atteintes aux droits fondamentaux qui touchent potentiellement chaque citoyen à travers le monde.

Loin de l'image du traître et de l'espion dénoncé par le gouvernement des Etats-Unis, de nombreux gouvernements et acteurs de la communauté mondiale du renseignement, il apparaît pour ce qu'il est, un défenseur des droits humains, au sens le plus noble du terme, conscient des risques, ayant mûrement réfléchi ses choix, soucieux de protéger sa famille, ses proches, mais aussi les personnes qui pourraient être mises en cause dans les documents confidentiels qu'il produit. Le contraire de la propagande orchestrée par les acteurs qu'il met en cause.

Il s'agit enfin d'un documentaire exceptionnellement rare sur ce qu'est le travail d'enquête sur les droits humains, et le rôle de vigie démocratique que peuvent jouer les lanceurs d'alerte et les enquêteurs, qu'ils soient journalistes d'investigation, comme ici, juges, avocats ou membres d'organisations de défense des droits humains .

Dans le huis clos d'une chambre d'hôtel de Hong Kong entre Edward Snowden, alias Citizenfour, et les deux journalistes d'investigation, Glenn Greenwald et Laura Poitras, chacun est conscient de la portée planétaire des documents qui vont être portés à la connaissance du public, au mépris des risques que chacun encourt.

Edward Snowden est passible désormais de plusieurs dizaines d'années de prison pour espionnage aux Etats-Unis. Le compagnon de Glenn Greenwald a été retenu et interrogé pour « terrorisme » parce qu'on le suspectait de transporter des documents confidentiels. Le journal le Guardian, dans lequel Glenn Greenwald publiait ses articles, a été sommé par les autorités britanniques de détruire les documents confiés par Snowden. Enfin, Laura Poitras, documentariste d'investigation, avait déjà été arrêtée des dizaines de fois par les autorités américaines pour son travail sur les dérives de l'Amérique post-11 septembre, dont Citizenfour constitue le dernier volet.

Pour toutes ces raisons, Amnesty International est fière de soutenir le film, qui rejoint nos préoccupations majeures, depuis de nombreuses années.

Le 7 juin, trois jours après les premières révélations, Amnesty International dénonçait avec force les atteintes sans précédent à la vie privée et le risque pour nos libertés constitué par le système de surveillance de masse mis en place par la National Security Agency (NSA) au lendemain du 11 septembre 2001.

« *La lutte contre le terrorisme ne doit pas servir de prétexte au gouvernement pour s'immiscer dans des affaires privées », « Le gouvernement américain doit prendre toutes les mesures nécessaires pour veiller à ce que personne ne soit soumis à des intrusions illégales ou arbitraires dans sa vie privée.* »

Les informations dénonçant une surveillance survenaient après le rejet par la Cour suprême des Etats-Unis, en février 2013, d'une affaire dans laquelle étaient mis en question les pouvoirs élargis permettant au gouvernement de pratiquer des écoutes téléphoniques sans mandat.

Concernant Edward Snowden, Amnesty International l'a immédiatement considéré comme un lanceur d'alerte qu'il fallait protéger. Le 2 juillet 2013, nous dénoncions ainsi la persécution judiciaire dont il était l'objet et les pressions des Etats-Unis sur d'autres gouvernements pour l'empêcher de demander l'asile.

« *Il est manifeste que ce qu'il a dévoilé intéresse la société dans son ensemble, et en tant que lanceur d'alerte ses actions se justifient. Il a attiré l'attention sur de vastes programmes illégaux de surveillance qui interfèrent incontestablement avec le droit de la personne au respect de sa vie privée.*
*« Les États qui tentent d'empêcher une personne de révéler un tel comportement illicite bafouent le droit international. La liberté d'expression fait partie des droits fondamentaux.*
*« Au lieu de se pencher sur ces infractions flagrantes, ou de les admettre, le gouvernement des États-Unis semble davantage déterminé à persécuter cet homme. Les actions visant à faire pression sur divers gouvernements afin qu'ils l'empêchent de demander l'asile sont déplorables.* »

Au-delà de la situation de Snowden, il est pour Amnesty International indispensable de renforcer la protection juridique des lanceurs d'alerte. Nous avons d'ailleurs participé à la rédaction des principes de Tshwane sur la Sûreté nationale et le droit à l'information, référence en matière de protection des lanceurs d'alerte.

Engagée sur l'ensemble de ces questions, Amnesty International lance le 18 mars 2015 une campagne de mobilisation de l'opinion publique visant à mettre fin à la surveillance de masse, et plus largement à exiger des gouvernements que les programmes de surveillance mis en place au nom de la sécurité soient conformes au droit international des droits humains, et respectent la vie privée de chacun.

Avec ses révélations, la volonté d'Edward Snowden était de permettre que l'opinion publique s'empare en toute connaissance de cause d'un débat fondamental pour les droits humains : Doit-on sacrifier nos libertés sur l'autel de la sécurité ? C'est ce que ce film magnifique permet.

A nous, citoyens, de nous en emparer.

*Vous pouvez voir la bande annonce du film sur www.amnesty.fr/node/14343*
*Retrouvez des reportages, vidéo, interviews sur Edward Snowden et les lanceurs d'alerte sur www.amnesty.fr/13601*

# A EDWARD SNOWDEN : PERSECUTE POUR AVOIR DENONCE DES VIOLATIONS MASSIVES DES DROITS HUMAINS

## 1. Qui est Edward Snowden ?

Né le 21 juin 1983, Edward Snowden a débuté sa carrière dans le renseignement en 2005, comme gardien de sécurité pour l'un des centres secrets de la NSA à l'université de Maryland. Malgré son manque de diplômes, ses compétences en sécurité informatique le font rapidement gravir les échelons dans la communauté du renseignement américain.
En 2007, il est en poste à Genève pour la CIA, sous couverture diplomatique. C'est à partir de ce moment qu'il commence à nourrir des doutes sur sa mission et les pratiques américaines en matière de renseignement.

Il expliquera avoir considéré organiser ses révélations au public plus tôt mais il décide d'attendre de voir si l'élection de Barack Obama en 2008 allait permettre de modifier les pratiques. Mais, selon lui, ce dernier « *a continué à pratiquer les mêmes méthodes que son prédécesseur.* »

***« Beaucoup de ce que j'ai vu à Genève m'a désillusionné sur la manière dont fonctionne mon gouvernement, et son impact sur la marche du monde. Je réalisais alors que je participais à un système faisant beaucoup plus de mal que de bien. »***
**Edward Snowden, dans une interview au Guardian**

En 2009, il quitte la CIA et rejoint divers sous-traitants privés de la NSA. Son dernier employeur est l'entreprise Booz Allen avec laquelle il travaille jusqu'en mai 2013, juste avant ses révélations.

## 2. Le temps des révélations

Le 20 mai 2013, il se rend à Hong-Kong, avec de très nombreux documents classés secrets, où il a donné rendez-vous à deux journalistes d'investigation américains : Glenn Greenwald, et Laura Poitras.
Le contact a été établi minutieusement, des mois à l'avance. C'est par leur intermédiaire que les documents seront publiés, à compter du 5 juin 2013.
Ils révèlent un système de collecte et de surveillance quasi-généralisée des communications mondiales mis en place par la NSA aux Etats-Unis et le Government Communications Headquarters (GCHQ), son équivalent au Royaume-Uni.
Ils révèlent aussi l'existence de l'alliance des Five Eyes (Cinq yeux), un arrangement secret de partage de renseignements mis en place entre les Etats-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande.
Ces programmes de surveillance espionnent une très grande part des communications numériques à travers le monde : des lois et décrets secrets obligent des géants de l'internet mondial comme Google, Microsoft, Yahoo, Facebook etc. à collaborer avec les services de renseignement américain.
Ces documents mettent au jour une violation à échelle mondiale du droit de chacun au respect de sa vie privée.

*Edward Snowden à Hong Kong transmet des informations aux journalistes. ©Laura Poitras*

## 3. La réaction des Etats-Unis : persécution et pression sur les autres pays

Immédiatement, les autorités américaines dénoncent publiquement E. Snowden comme un traitre et un espion. Il est inculpé le 14 juin d'avoir violé l'Espionnage Act (loi sur l'espionnage) et de vol de propriété du gouvernement américain.
Ces chefs d'inculpation le rendent passible de trente ans d'emprisonnement.
Les Etats-Unis formulent à Hong-Kong une demande d'extradition, ce qui pousse Snowden à s'enfuir pour la Russie. Alors que son passeport est révoqué, Edward Snowden se retouve bloqué dans la zone internationale de l'aéroport Cheremetyevo, à Moscou.
Il ne peut se rendre dans un autre pays, son passeport ayant été révoqué. Après un mois de tergiversation, les autorités russes accordent un droit de séjour temporaire d'un an à Edward Snowden. Le 8 août 2014, les autorités russes lui accordent un droit de séjour supplémentaire de 3 ans, jusqu'en août 2017.

## 4. Empêché de demander l'asile et de choisir son pays d'accueil.

Alors que plusieurs pays – la Bolivie, le Nicaragua, ou le Venezuela – se déclarent publiquement prêts à l'accueillir et à lui accorder l'asile, le gouvernement américain ne s'est pas arrêté là : il exerce sa puissance politique pour faire pression sur différents gouvernements afin d'empêcher Edward Snowden d'entrer sur leur territoire ou même d'utiliser leur espace aérien.
Des pays européens ont refusé de le laisser ne serait-ce que traverser leur espace aérien. Ainsi, le 3 juillet 2013, la France, avec l'Italie, le Portugal et l'Espagne, a refusé le survol de son espace aérien au président bolivien Evo Morales, par crainte – infondée – qu'Edward Snowden soit secrètement présent dans l'avion présidentiel.
Depuis, plusieurs gouvernements européens ont bloqué des projets, émanant même de parlementaires, visant à le convier à des conférences dans leur pays.

Les autorités françaises se sont également montréesréticentes à étudier la demande d'asile d'Edward Snowden. Le 4 juillet 2013, Manuel Valls, alors ministre de l'Intérieur, déclarait :
*« Cette demande, si elle est déposée, pose de nombreux problèmes juridiques. Pour ce qui me concerne, je n'y suis pas favorable. Les Etats-Unis sont un pays démocratique, avec une justice indépendante. M. Snowden est un agent des services américains, et c'est un pays ami avec lequel nous avons des relations. Si cette demande est faite, elle sera toutefois examinée. »*

## 5. Ce que demande Amnesty International pour Edward Snowden

Amnesty International considère Edward Snowden comme un lanceur d'alerte ayant permis de révéler au monde entier des violations massives de la vie privée et des libertés de chaque citoyen.
A ce titre, pour Amnesty International, les Etats-Unis, plutôt que de poursuivre Edward Snowden, devraient faire la lumière sur leurs agissements criminels et y mettre un terme.

Le gouvernement américain a inculpé Edward Snowden au titre de la Loi relative à l'espionnage, ce qui l'empêcherait de construire sa défense en invoquant l'intérêt général pour expliquer sa décision de lancer l'alerte en vertu du droit américain. L'illégalité des pratiques dénoncées par Snowden ne serait pas prises en compte.

Le fait enfin qu'il ait déjà été déclaré coupable par de nombreux officiels américains, avant même la tenue d'un éventuel procès ; le risque de conditions de détention inhumaines, comme pour le lanceur d'alerte Chelsea Manning, détenu à l'isolement et condamné à 35 ans de prison, fait courir le risque d'une procédure inéquitable.

Le fait que des politiciens américains influents réclament qu'on ne lui fasse pas de quartier ajoute foi aux craintes qu'il ne puisse bénéficier d'un procès équitable aux États-Unis. Des poursuites lancées contre Edward Snowden portaient sur ses révélations au sujet des violations des droits humains imputées au gouvernement américain, bafoueraient son droit à la liberté d'expression et reviendraient à le persécuter au motif de ses opinions politiques.

De hauts responsables gouvernementaux américains, dont John Kerry, le secrétaire d'État, ont qualifié Edward Snowden de « traître », faisant sérieusement douter de l'équité de tout procès dont il pourrait faire l'objet aux États-Unis.

La persécution dont est l'objet Edward Snowden doit lui permettre de demander l'asile auprès de tout pays de son choix.
Amnesty International appelle les gouvernements à ne pas l'empêcher de voyager pour chercher une protection. En interférant dans sa démarche, ils se rendent, de fait, complices de la sanction injuste et répressive dirigée contre lui par les États-Unis.

> ***Ma seule motivation est d'informer la population de ce qui est fait en son nom et de ce qui est fait à son encontre (…]. J'ai analysé méticuleusement chacun des documents que j'ai divulgués pour m'assurer qu'ils présentaient un intérêt légitime pour le public… Il y a de nombreux documents que je n'ai pas divulgués malgré l'immense impact qu'ils auraient pu avoir, car porter préjudice aux gens n'est pas mon objectif.***
> ***Mon objectif, c'est la transparence.***
>
> **Edward Snowden, 6 juin 2013**

# B SURVEILLANCE A L'ERE NUMERIQUE : MENACES SUR LA VIE PRIVEE ET LES LIBERTES

## 5 bonnes raisons de nous préoccuper de la surveillance de masse

**1. Avec la surveillance de masse, chaque citoyen est traité comme un criminel**

Les documents révélés par Edward Snowden nous montrent que toutes nos communications privées et toutes les traces numériques que nous pouvons laisser derrière nous sont scrupuleusement collectées et analysées par nos gouvernements. En procédant ainsi, ils contreviennent aux principes juridiques fondamentaux qui encadrent les pratiques de surveillance, à savoir qu'elle doit être ciblée, motivée par des preuves ou des éléments incriminants et ordonnée par une autorité parfaitement indépendante, telle qu'un juge. Au lieu de cela, ceux qui nous gouvernent considèrent chaque citoyen comme un criminel potentiel, et le moindre détail de notre vie privée devient suspicieux.

**2. La surveillance de masse ne permet pas de repérer les terroristes**

Nous entendons nos politiciens réclamer sans cesse davantage de moyens pour les agences de renseignement, prétextant qu'elles pourront ainsi interpeller plus de terroristes. Rien ne démontre aujourd'hui que la surveillance de masse permette d'arriver à ce résultat. Avant les récents attentats perpétrés à Paris, les services de renseignement avaient placé les auteurs des attaques sur des listes de surveillance, avant de les en retirer. Ce n'est pas en augmentant la quantité de données collectées que nous pourrons améliorer notre sécurité. En vérité, les gouvernements actuels collectent aujourd'hui des informations qu'ils n'auraient pas osé rêver obtenir il y a seulement dix ans. Ils continueront cependant à nous répéter qu'il faut aller plus loin. Il est temps de fixer des limites.

**3. La surveillance de masse outrepasse nos droits fondamentaux**

À l'heure actuelle, nos gouvernements nous imposent un choix qui n'en est pas un : la sécurité ou la liberté. Depuis des siècles, les sociétés ont dû trouver un équilibre entre ces deux notions et ont mis en place des règles strictes visant à protéger leurs citoyens, notamment la présomption d'innocence et la protection de la vie privée. Cela signifie que les gouvernements doivent disposer d'éléments incriminants avant de restreindre les libertés de quiconque. Il s'agit de concepts fondamentaux dont les partisans de la surveillance de masse souhaitent s'affranchir.

**4. La surveillance de masse peut être utilisée pour côntroler ce que nous faisons**

Nous entendons souvent « si tu n'as rien à te reprocher, tu n'as rien à cacher ». Cela revient à accorder une très grande confiance à nos dirigeants et à supposer qu'ils feront toujours les bons choix. Le gouvernement s'octroie un droit de regard sur la vie privée de ses citoyens, et ce à tout moment. Il s'agit là d'un pouvoir immense, qui peut mener à des abus considérables. Nous savons désormais que les données personnelles peuvent être utilisées pour cibler des journalistes, persécuter des militants, pratiquer la discrimination et le profilage des minorités et museler la liberté d'expression. À chacun aujourd'hui de se demander : « Je ne suis pas concerné, mais est-ce le cas de tous ? », « Aujourd'hui il n'y a pas d'abus, mais qu'en sera-t-il demain ? ».

**5. La surveillance de masse menace la liberté d'expression sur Internet**

À ses débuts, Internet était considéré comme un espace où il était possible de débattre ouvertement. Cette vision est aujourd'hui mise à mal. Les gouvernements voudraient nous convaincre que nos droits s'arrêtent dès que nous sommes sur Internet. Ils voudraient nous faire croire que dès que nous utilisons notre téléphone ou que nous consultons nos courriels, tout ce que nous pouvons dire ou faire leur appartient. Ces pratiques nous

seraient absolument intolérables dans notre vie « réelle », il n'y a pas de raison qu'il en soit autrement pour notre vie numérique.

## 1. Un vaste système de surveillance de masse hors de tout contrôle

*« Aujourd'hui chaque frontière que tu franchis, chaque achat que tu fais, chaque appel passé, chaque antenne-relais croisée, chaque ami, chaque site visité et chaque courriel rédigé sont entre les mains d'un système au pouvoir illimité, mais pas totalement sécurisé. »*
Edward Snowden, CITIZENFOUR

Les documents révélés par Edward ont constitué un tremblement de terre à l'échelle mondiale.

A partir du 4 juin 2013, le monde découvrait effaré les preuves de la mise en place, dans la foulée des attentats du 11 septembre, d'un système de surveillance électronique généralisée, à l'abri de tous les regards, et sans presqu'aucun garde-fou légal, sous l'impulsion de la National Security Agency, l'agence de sureté nationale américaine.

Rapidement, il est devenu clair que ce système, mis en place soi-disant pour lutter contre les menaces terroristes, visait en réalité à s'assurer le contrôle de l'ensemble des communications électroniques échangées par la population mondiale, des dirigeants « alliés » (la mise sur écoute du téléphone portable de la chancelière allemande Angela Merkel) aux communications internes de défenseurs des droits humains comme Amnesty International par exemple.

Les documents publiés et analysés par les journalistes montraient aussi que loin d'être le seul fait des Etats-Unis, cette surveillance des communications numériques était l'objet d'échanges et de partages avec d'autres pays, au premier chef l'alliance des « Five Eyes » (les Cinq yeux), composée des Etats-Unis, du Royaume Uni, du Canada, de l'Australie et de la Nouvelle-Zélande.

Bientôt, nous apprendrions que la mise en place de programmes de surveillance de masse n'était pas l'apanage de ces pays : d'après des documents publiés dans le journal le Monde en juillet 2013, la France a elle aussi mis en place des programmes de surveillance de masse, partagés avec le Royaume-Uni.

Ce que certains spécialistes des questions de surveillance avaient subodoré avant les révélations se révélait vrai :

A l'ère numérique, les capacités de surveillance de la population sont inégalées et risquent encore de s'accentuer avec les progrès technologiques dans un futur proche.

Aujourd'hui, en contrôlant les échanges électroniques d'une personne, sa géolocalisation satellite, voire, le contenu de son ordinateur, de sa tablette ou de son smartphone, on peut retracer avec une précision extrême les moindres faits et gestes de celle-ci.

Pour arriver au même résultat sur une personne avant internet, il aurait fallu : une filature physique quotidienne ; une perquisition quotidienne de son domicile ; la mise sur écoute de son téléphone et l'ouverture de l'ensemble de ces courriers.

Les capacités de collecte développées font que c'est ce qui se passe aujourd'hui, potentiellement **pour chacun d'entre nous**. De manière la plupart du temps totalement invisible et sans que nous sachions ce qui est fait de nos données personnelles.

Les conditions techniques pour la création d'un « Big Brother » sont aujourd'hui réunies, et si nous n'y prenons garde, en exigeant de nos gouvernements de mettre un terme à cette dérive liberticide, la surveillance à l'ère numérique constitue vraisemblablement la plus grande menace pour les droits humains des années à venir.

## 2. *Que dit le droit international des droits humains en matière de surveillance*

Notre vie privée est garantie 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, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

La surveillance des communications (du contenu et / ou des métadonnées*) constitue une atteinte à un certain nombre de droits humains, en particulier le droit au respect de la vie privée et à la liberté d'expression.

Elle peut être légitime dans certaines circonstances, si justement elle demeure l'exception, et qu'elle est encadrée par des principes de droit universellement reconnus.

Une surveillance ciblée ne peut se justifier que lorsqu'elle est :

- fondée sur un **soupçon raisonnable**, conformément à la loi,

- strictement **nécessaire** à la poursuite d'un **objectif légitime** (tel que la protection de la sécurité intérieure ou la lutte contre la grande criminalité),

- **proportionnelle** à l'objectif visé,

- **non discriminatoire**.

Amnesty International considère que la surveillance de masse ne répond pas à ces critères. Il n'existe donc pas de surveillance de masse compatible le respect des droits humains.

## 3. *Quelques concepts clés pour comprendre les recommandations d'Amnesty International*

- **Surveillance ciblée**

La surveillance ne peut être autorisée que lorsqu'elle cible un individu, un groupe déterminé d'individus, ou un lieu précis ayant un lien direct avec la réalisation d'un objectif légitime.

- **Extraterritorialité**

Selon Amnesty International, les programmes et mesures de surveillance des communications adoptés par les États portent atteinte aux droits au respect de la vie privée et à la liberté d'expression, **indépendamment du lieu** de la surveillance ou de l'endroit où se trouve(nt) le ou les individu(s) concerné(s).
Les obligations internationales en matière de droits humains s'appliquent hors du territoire national, selon l'État exerçant le pouvoir ou le contrôle effectif de la jouissance de ses droits par un individu.

- **Légalité**

Toute activité de surveillance des communications, qu'elle porte sur le contenu ou les métadonnées*, doit être autorisée conformément aux lois nationales, accessibles et prévisibles par tous.
Ces lois doivent être rédigées de manière suffisamment claire pour permettre aux citoyens de saisir les conditions et circonstances selon lesquelles les autorités ont le pouvoir de recourir à des mesures de surveillance des communications. Elles doivent notamment établir de façon suffisamment détaillée l'étendue et la portée, ainsi que les modalités d'exercice, de tout pouvoir accordé aux autorités concernées d'autoriser et de mettre en place des mesures de surveillance. Elles doivent également préciser les procédures de recours prévues.

- **Partage avec les gouvernements étrangers**

Le partage, spontané ou non, avec des gouvernements étrangers de données obtenues grâce à la surveillance des communications, doit s'inscrire dans un cadre légal conforme aux obligations des États en matière de droits humains.

- **Nécessité et proportionnalité**

Les mesures de surveillance doivent être strictement nécessaires et proportionnelles à la réalisation d'un objectif légitime au regard du droit international des droits de l'homme, comme par exemple l'application des lois ou la sécurité nationale. Elles devront se manifester de la façon la moins intrusive possible.

- **Garanties contre les abus**

Les critères de nécessité et de proportionnalité ne sont respectés que lorsqu'il existe des garanties adaptées et efficaces contre les abus et le recours arbitraire à la surveillance. Ces garanties incluent

- l'exigence de mandats émanant d'autorités indépendantes pour une surveillance ciblée,
- le contrôle, à intervalles raisonnables, de la légalité permanente de la surveillance (notamment le stockage des informations obtenues par la surveillance) par une autorité judiciaire indépendante,
- la limitation du nombre de motifs de perquisition et de leur utilisation, la limitation du transfert et du partage des données de communication entre les différents organes de l'Etat ou entre Etats, l'existence de critères stricts, notamment de délais de prescription, sur la durée pendant laquelle ces données peuvent être stockées, et l'existence de prescriptions claires concernant leur destruction.

- **Accès à l'information**

**L**e public devrait avoir accès aux informations pertinentes, notamment concernant le cadre juridique global de la surveillance des communications ; les entités habilitées à mener la surveillance ; les procédures conditionnant l'autorisation de la surveillance des communications, la sélection des cibles de la surveillance et l'utilisation, le partage, le stockage et la destruction des données de communication ; les statistiques relatives au recours à la surveillance.

- **Effectivité du contrôle judiciaire et parlementaire**

Tout régime de surveillance devrait être soumis à un contrôle judiciaire et parlementaire, et par l'exercice de pouvoirs de contrôle a priori et a posteriori conférés aux tribunaux.
Toutes les décisions doivent être prises et / ou contrôlées par **des organes indépendants et impartiaux**, et ce à chaque étape du processus, depuis l'approbation initiale de la surveillance au contrôle a posteriori de la légalité permanente des mesures de surveillance et du système qui les sous-tend.
Amnesty International est opposée aux tribunaux secrets tout en admettant qu'il existe des situations dans lesquelles la délivrance de mandats peut être amenée à être effectuée sans que le ou les individu(s) concerné(s) n'en soient informé(s). Dans des circonstances aussi exceptionnelles et strictement encadrées, la législation doit garantir qu'un défenseur de la vie privée indépendant soit nommé par l'autorité judiciaire afin de s'assurer du respect de la vie privée et des libertés civiles de l'individu.

- **Notification :** dans la plupart des cas (sauf par exemple en cas d'impossibilité manifeste), les États ont l'obligation positive d'aviser toutes les personnes soumises à une surveillance de la mesure dont elles ont fait l'objet, sur quelles bases, et de les informer des données collectées, ainsi que des recours éventuels pouvant être formés, ceci dès que ladite notification pourra être effectuée sans mettre en péril la réalisation de l'objectif légitime ayant motivé la surveillance.

- **Recours :** le droit relatif aux droits humains exige que les individus concernés aient accès à un recours en cas de violation de leurs droits humains. La législation doit accorder aux organes judiciaires de larges pouvoirs d'enquête afin de garantir aux individus soumis à des mesures de surveillance l'accès à des moyens de recours efficaces.

- **Destruction des données** de communication stockées : la législation doit garantir la destruction, dès que possible, des données de communication stockées, et au plus tard lorsque la réalisation de l'objectif légitime pour laquelle la surveillance a été autorisée cesse d'être strictement nécessaire.

- **Non-discrimination**

Les Etats doivent garantir que la jouissance du droit au respect de la vie privée et à la liberté d'expression est exempt de discrimination directe ou indirecte fondée sur la race, le sexe/le genre, l'orientation sexuelle, l'identité sexuelle, la religion ou les croyances, l'opinion politique ou toute autre opinion, l'origine ethnique, nationale ou sociale, le handicap ou d'autres facteurs.
La législation devrait, d'une manière générale, fournir à tous les mêmes niveaux de protection. En particulier, les distinctions et les différences de traitement fondées sur la nationalité ou le lieu doivent être raisonnables, objectives et reposer sur des motifs légitimes et impérieux. Les distinctions et différences globales de traitement entre citoyens et non-citoyens, résidents et non-résidents, ou entre les individus se trouvant sur le territoire national et ceux se trouvant à l'étranger ne rentrent en principe pas dans ce cadre.

- **Obligations positives**

Les Etats sont soumis à des obligations positives de protection des individus relevant de leur compétence, ou soumis à leur pouvoir et à leur contrôle, contre la surveillance illégale mise en place par des tiers (y compris les Etats étrangers). Ils doivent réglementer les agissements des acteurs privés afin de prévenir les atteintes disproportionnées au droit au respect de la vie privée et à la liberté d'expression. Les Etats ne doivent pas coopérer avec les Etats étrangers dans la soumission de personnes à des mesures de surveillance illégale, ni les accepter ou s'en rendre complices.

## 4. Les défenseurs des droits humains en première ligne

Les mécanismes de surveillance illégale ne visent pas que les ennemis de la sécurité, délinquants et terroristes. Ce sont trop souvent les journalistes, opposants politiques, dissidents et militants des droits humains qui se retrouvent ciblés. L'absence de mécanisme de contrôle indépendant laisse la porte ouverte à leur utilisation à des fins inacceptables.

AI s'est inquiétée dès 2008 des dérives de la surveillance et a notamment engagé des actions en justice :

- Aux Etats-Unis

Amnesty a contesté dès 2008 la constitutionnalité de la Loi relative à la collecte de renseignements sur des puissances ou ressortissants étrangers (Foreign Intelligence Surveillance Act – FISA).

Dans cette affaire, *Clapper c. Amnesty International USA*, Amnesty International et un ensemble d'autres organisations, d'avocats et de journalistes représentés par l'Union américaine pour les libertés publiques contestaient cette loi qui élargissai les pouvoirs du gouvernement en matière de surveillance sans mandat et exemptait une telle surveillance de tout contrôle significatif

En février 2013, la Cour suprême américaine a classé sans suites cette affaire, car les organisations demandeuses n'avaient pas pu démontrer qu'elles faisaient probablement l'objet d'une surveillance, surveillance impossible à démontrer dans les faits étant donné la nature très secrète de ce type d'opérations et du tribunal de la FISA les autorisant.

- Au Royaume-Uni

En décembre 2013, Amnesty International a porté plainte contre le gouvernement du Royaume-Uni, accusant les services du renseignement britanniques d'avoir accédé illégalement aux communications de l'organisation.

Des révélations d'Edward Snowden ont ensuite confirmé que des défenseurs des droits humains, y compris des salariés d'Amnesty International, ont très probablement été la cible d'une surveillance de la part des services d'espionnage américains et britanniques.

Lorsqu'on lui a demandé, en avril 2014, si l'Agence nationale de sécurité américaine (NSA) ou son équivalent britannique, le GCHQ, espionnaient activement les organisations de défense des droits humains telles qu'Amnesty International et Human Rights Watch, Edward Snowden a répondu : « *Absolument, cela ne fait aucun doute […]. La NSA a en fait visé spécifiquement les communications de dirigeants ou de membres du personnel de certaines organisations de défense des droits humains ou de la société civile.* »

Ces allégations confirment donc les craintes d'Amnesty International.

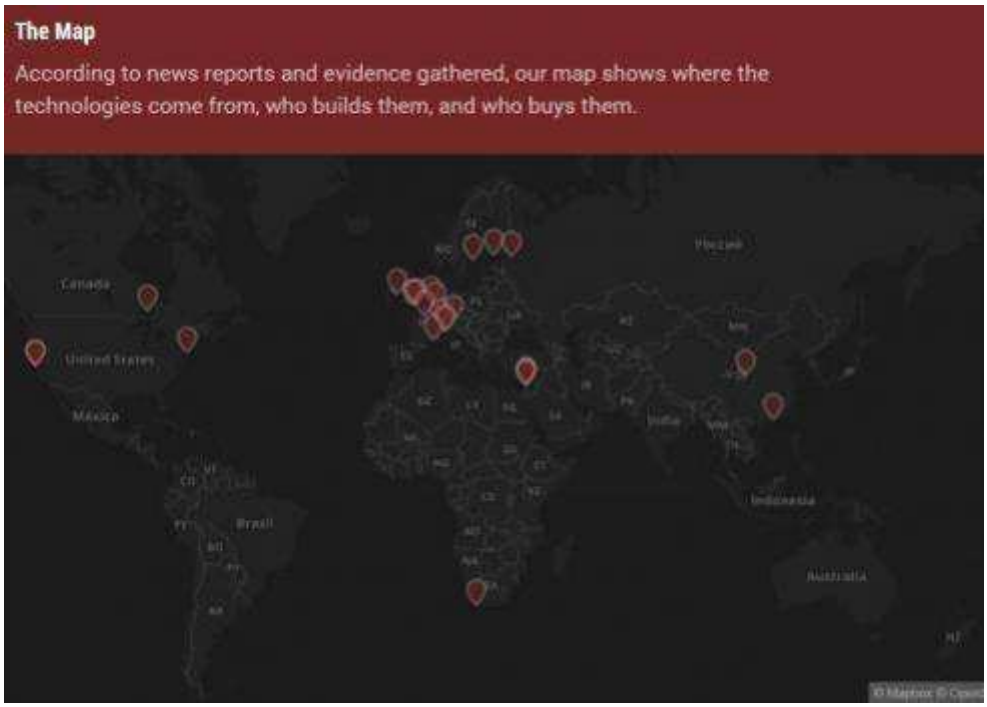
> ***« Le partage de ces informations avec d'autres États risque de mettre en danger des militants des droits humains dans le monde entier à très court terme. »***
> Michael Bochenek, Amnesty International.

Le 6 février 2015, Amnesty International et d'autres organisations ont remporté une victoire historique, le tribunal chargé de surveiller les pratiques des services de renseignements britanniques a reconnu que le partage de renseignements entre les États-Unis et le Royaume-Uni sur la surveillance des communications bafouait le droit relatif aux droits humains.

Cependant, ce même tribunal a ajouté que le partage de renseignements entre les États-Unis et le Royaume-Uni concernant la surveillance des communications était désormais légal, en raison de législations adoptées depuis.

Amnesty International désapprouve cette position, car la divulgation limitée de ces politiques gouvernementales est loin de garantir que le partage des renseignements est conforme aux obligations incombant au Royaume-Uni en termes de droits humains. Amnesty International prévoit de contester la décision de l'Investigatory Powers Tribunal auprès de la Cour européenne des droits de l'homme.

## 5. *Un commerce de la surveillance numérique hors de tout contrôle*




L'utilisation et le commerce de technologies de surveillance des télécommunications se sont développés de manière exponentielle ces dernières années alors que les gouvernements utilisent de plus en plus les logiciels et les équipements d'espionnage et les outils connexes pour bafouer le droit au respect de la vie privée et nombre de droits humains.

La Coalition contre l'exportation illégale de technologies de surveillance (CAUSE), dont Amnesty International est membre, estime que le commerce mondial des technologies de surveillance représente 4 milliards d'euros par an, et qu'il est en expansion. Elle demande que les gouvernements et les entreprises privées rendent des comptes pour les atteintes aux droits humains liées au commerce international des technologies de surveillance des communications, commerce en pleine croissance qui représente plus de 3,5 milliards d'euros.

# C LA FRANCE ET LA SURVEILLANCE DE MASSE- DERIVES ACTUELLES ET A VENIR

> « *Les nouvelles technologies numériques sont un outil formidable d'échange et de développement. Mais elles doivent aussi s'accompagner d'une protection efficace des données personnelles. Les révélations sur l'ampleur de la surveillance des communications ont suscité des préoccupations légitimes de la part de nos concitoyens. La France souhaite rappeler ici son attachement à la protection du droit à la vie privée, à la fois en ligne et hors ligne. Ce droit énoncé à l'article 17 du Pacte sur les droits civils et politiques est au fondement des droits à la liberté d'expression et la liberté d'opinion. (…)* »
> Représentant de l'Etat français devant le Conseil des droits de l'Homme des Nations Unies, septembre 2014

La surveillance électronique en France est régie par le Code de la sécurité intérieure de 2012. Les interceptions de sécurité doivent être autorisées par le premier ministre sur recommandation de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Dans un rapport de l'assemblée nationale en date du 30 avril 2013 il est fait état que *« depuis 2008 des progrès ont été réalisés en matière de mutualisation des capacités, notamment en ce qui concerne le renseignement d'origine électromagnétique, opéré par la DGSE au profit de l'ensemble de la communauté du renseignemen*t ».

La France serait le 5ème Etat du monde en terme de collecte de métadonnées* après les Etats Unis, le Royaume Uni, Israël et la Chine et le 2ème en Europe selon notamment Bernard Barbier le directeur de la DGSE jusqu'en 2010.

Le centre de surveillance principal est opéré par la DGSE à Paris qui concernerait des data interceptés et collectées sur une vingtaine de sites en France et à l'étranger (y compris des satellites et des câbles sous-marin de fibre optique)
Les services secrets français entretiennent de nombreuse coopération avec des services étrangers : plus de 200 selon le directeur de la DGSE en 2013 dont 50 qui appartiendrait à un cercle plus fermé de fréquente collaborations sans jamais ne les nommer.

A l'initiative des USA, les services secrets occidentaux auraient mis en place une base de données communes permettant à chaque Etat d'accéder aux données collectées.
D'après le Monde, « *la France bénéficie d'une position stratégique en matière de transport de données électroniques par les câbles sous-marins. Ce flux d'informations étranger-France, cette «matière première» comme la qualifie la NSA dans une note révélée par M. Snowden, fait l'objet d'une large interception par la DGSE* ».
Le 21 mars 2013, *Le Monde* s'appuyant sur des documents révélés par Edward Snowden dénonçait les pratiques des autorités françaises en matière de surveillance ainsi que la collaboration des services de renseignement avec l'opérateur Orange. Ni démenti, ni confirmé par les autorités françaises, ces révélations n'ont pas donné lieu à la mise en place d'une commission d'enquête ou autre mécanisme pour faire la vérité sur ces pratiques.
Parmi les méthodes de surveillance de masse conduites par la France, il existerait également des transferts massif de données entre les services français et la NSA américaine (accord LUSTRE) ainsi que la mise en place d'un dispositif d'interception des flux circulant sur les réseaux internationaux avec l'appui d'entreprises comme Alcatel-Lucent ou Amesys.

La France n'a pas réagi à ces révélations et a refusé de collaborer à la commission d'enquête du Parlement européen sur les révélations de Snowden (tout comme le Royaume Uni).

## 1. Des législations autorisant des programmes de surveillance illégale

Cette tendance à la mise en place de plus de surveillance s'inscrit dans une volonté du gouvernement qui remonte aux débats lors de la Loi de Programmation Militaire.

**Loi du n° 2013-1168 du 18 décembre 2013, relative à la programmation militaire**

L'article 20 introduit un système généralisé de captation des données électroniques et téléphoniques en vue de lutter contre les atteintes potentielles à la sûreté du territoire et des intérêts de la France.
Il permet à plusieurs ministères d'autoriser la surveillance en temps réel de tout citoyen. **Une simple demande administrative** suffirait donc pour que soient collectés des informations et documents de nature personnelle auprès des fournisseurs d'accès à Internet et opérateurs de télécommunication, mais aussi des hébergeurs et fournisseurs de services en ligne. Aucune garantie adéquate et aucun mécanisme de contestation n'est prévu pour assurer le respect des droits de ceux qui font l'objet de ces intrusions. Ce texte rend permanents des dispositifs de surveillance qui n'étaient jusqu'à présent que temporaires et exceptionnels.
La CNIL – Commission nationale informatique et libertés – qui n'avait pas été consultée sur cet article, déplore l'absence d'un débat public sur la mise en place d'une "société de surveillance" un débat qui aurait permis d'éclairer les citoyens sur les enjeux en cause et de prendre en compte la nécessaire protection des libertés individuelles et de la vie privée.

Aujourd'hui, les données que peuvent réclamer la police et la gendarmerie visent non les contenus des messages, mais « *les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date de la communication* »

L'autorisation formelle est prise « *par décision écrite du Premier ministre ou des personnes spécialement désignées par lui* », pour une durée maximale de 30 jours renouvelables.

**Loi du 13 novembre 2014 (dite de renforcement de la lutte contre le terrorisme)**

Cette loi permet aux services du Ministre de l'intérieur d'établir une liste des sites de propagande terroriste afin qu'ils soient bloqués, retirés ou déréférencés, sans aucune intervention du juge judiciaire

## 2. Futurs projets de loi avec incidences sur la surveillance :

**Après les attentas des 7 et 9 janvier 2015, le Premier ministre** a demandé au ministre de l'Intérieur de lui adresser "des propositions de renforcement" en matière de surveillance. Plusieurs projets sont attendus au cours du premier semestre 2015

- 1er semestre 2015 : Projet de loi sur les « libertés numériques »

- 1er semestre 2015 : loi sur le renseignement : la loi devra préciser les contours du «garde fou» chargé de définir le rapport entre sécurité et protections des libertés et rationaliser le contrôle administratif des pratiques des différents services.

- Juin 2015: nouvelle Loi de programmation militaire . La première actualisation était initialement prévue fin 2015 mais, a été avancée suite aux attentats de janvier.

Amnesty International sera particulièrement vigilante aux propositions discutées et ne manquera pas de rappeler aux décideurs leurs responsabilités en termes de protection des libertés.

Amnesty International lance le 18 mars 2015 une campagne contre la surveillance illégale.

Pour toute information, contactez dcuris@amnesty.fr

# Glossaire

- **Five Eyes**
  *Le terme Five Eyes* (*Cinq Yeux)*, désigne l'alliance des services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces pays sont reliés entre eux par l'accord UKUSA, un traité qui prévoit la coopération entre les différents services assurant la collecte de renseignements électromagnétiques.

- **Métadonnées** : toute information, autre que le contenu même de la communication, générée par l'utilisation des technologies de la communication. Si l'information ne contient pas nécessairement d'éléments à caractère personnel ou relatifs au contenu, elle renseigne sur les dispositifs utilisés, les utilisateurs desdits dispositifs et la façon dont ils sont utilisés (lieu, heures, adresses IP, durée de communication etc etc)

- **Surveillance des communications** : le contrôle, l'interception, la collecte, la sélection, la rétention, l'analyse, le partage ou toute autre utilisation d'éléments de communication de tout type, notamment le contenu des communications et leurs données (métadonnées).

- **Soupçon raisonnable** : Dans le contexte de la surveillance des communications, le soupçon raisonnable désigne l'existence d'un ensemble suffisant d'informations indiquant
  qu'un individu, un groupe, un lieu est lié à des agissements dont la prévention est justifiés par un objectif légitime,
  que l'obtention de données de communication est nécessaire à l'enquête sur lesdits agissements.

- **Surveillance de masse systématique** : contrôle, interception, collecte, stockage, analyse ou toute autre utilisation, à grande échelle et généralisés, d'éléments de communication ne visant aucun individu, groupe ou lieu identifiable et différenciable particuliers, et non fondés sur la notion de soupçon raisonnable.

***Quelques programmes de surveillance révélés par Snowden***

Verizon, X-Keystore, PRISM, Tempora … Ces termes auparavant secrets ont été mis à jour par Edward Snowden, autant de noms derrière lesquels se cachent les mécanismes de surveillance mis en place par les Etats-Unis et leurs alliés des Five Eyes.

- **Boundless informant** :

système informatique secret à visée internationale permettant à la National Security Agency (NSA) de connaître en temps réel, le niveau de surveillance appliqué à chaque pays.

- **PRISM**

programme de surveillance électronique mis en place par les Etats-Unis pour suivre de manière étendue l'activité en lige d'un très grand nombre de personnes. Il permet à la NSA de collecter des informations auprès d'entreprises américaine, dont la plupart des géants du Web. Le système collecte courriels, fichiers, photos, contenu des communications audio et vidéo par internet, informations sur les réseaux sociaux et des éléments comme la connexion à certains sites.

- **XKeystore** :

programme de surveillance de masse créé par la NSA et opéré conjointement avec les services de renseignements britanniques, canadiens, australiens et néo-zélandais. Il permettrait une « collecte quasi-systématique des activités de tout utilisateur sur Internet », grâce à plus de 700 serveurs localisés dans plusieurs dizaines de pays

XKeyscore a également la possibilité d'importer rétroactivement plusieurs jours de métadonnées échangées, ainsi que le contenu de communications

- **TEMPORA** :

programme de surveillance électronique du GCHQ, qui permet à l'agence britannique d'intercepter les données transitant par les câbles en fibre optique entre l'Europe et les États-Unis.

Les données interceptées seraient ainsi conservées dans une zone tampon durant trente jours, ce qui permettrait au GCHQ d'y « puiser » les données (courriels, messages Facebook, historiques de recherches d'internautes, etc.). Certains résultats de ces écoutes seraient transmis à l'Agence nationale de la sécurité américaine, la NSA