Ligue des droits de l'Homme
Section d'Aix-en-Provence

Les Échos de la LDH

N°28
JANVIER 2016

SOCIÉTÉ DE SURVEILLANCE = NON À UNE SUSPICION GÉNÉRALISÉE !

Dans un précédent numéro des Échos (n° 6, 2010-2011), nous alertions sur la menace pour les libertés publiques que représentait le développement de systèmes de surveillance de plus en plus généralisés. Nous parlions alors principalement de fichiers (STIC, Judex, Edwige, FNAEG), des puces d'identification à distance présentes sur beaucoup de nos documents (passeports, pass transport, nouvelles cartes d'identité), de la vidéo-protection. Or voici que depuis peu et principalement depuis les révélations du lanceur d'alerte Edward Snowden en juin 2013 le monde a découvert – sidéré et scandalisé – les systèmes de surveillance de masse mis en place par les États-Unis et ses plus proches alliés. Ces systèmes sont rendus possibles par l'extraordinaire rapidité de la révolution numérique (des serveurs de plus en plus grands, un débit internet de plus en plus élevé, des ordinateurs de plus en plus puissants) et par l'explosion quantitative des données disponibles (en raison du foisonnement d'internet, de la téléphonie mobile et des réseaux sociaux). Si les formes classiques de surveillance conservent leur importance, le nouveau terrain des services de renseignement est le monde des données, le « big data », les données de masse.

Dans ce numéro des Échos nous présentons un panorama des principaux outils actuels de la surveillance et nous exposons les menaces qu'ils présentent pour le respect de la vie privée et le risque qu'ils nous mènent à une société de suspicion généralisée.

LES PRINCIPAUX OUTILS DE LA SURVEILLANCE

En 1949, George Orwell, dans son roman *1984*, imaginait le « télécran » : un dispositif omniprésent s'apparentant à un téléviseur, capable de diffuser de la propagande politique et de surveiller les occupants de la pièce dans laquelle il était placé. Cet appareil était **fixe**, **ne pouvait pas être éteint** et permettait de **voir et d'entendre**.

Il faisait donc figure de pâle ancêtre des moyens de surveillance modernes. Le téléphone est maintenant **mobile**, lui non plus **ne peut pas être éteint** (sauf à lui retirer sa batterie). Piraté à distance, son micro permet d'**entendre**, son appareil photo de **voir**, son GPS de **localiser** à 5 mètres près. L'attaquant peut aussi déduire les **centres d'intérêt** et les **relations** du propriétaire en consultant son historique de navigation et son répertoire.

Cet objet n'est pas le seul à pouvoir être surveillé et nous ne pouvons donc que constater **l'étendue des possibilités de surveillance.** Nous allons en faire une courte présentation.

1 - Écoutes téléphoniques et interception des communications électroniques

Les communications téléphoniques et les connexions internet peuvent depuis des années être surveillées dans le cadre d'une procédure judiciaire. Sans cadre légal, les services de renseignement (par exemple : la Direction générale de la sécurité extérieure –DGSE-, la Direction générale de la sécurité intérieure –DGSI-, ou encore l'Unité de coordination de la lutte anti-terroriste –UCLAT-), pratiquaient également ce type de surveillance. Depuis la nouvelle loi du 24 juillet 2015 « relative au renseignement », les services de renseignement peuvent avoir accès aux données de connexion sans accord d'un juge, avec le simple aval du premier ministre en cas « d'urgence absolue ».

2 – Surveillance d'internet

L'ensemble des connexions seront dorénavant surveillées au moyen de boîtes noires pour alerter les services de renseignement sur toute connexion « suspecte ». Il s'agit d'ordinateurs qui, au moyen de processus automatisés (algorithmes), déterminent si l'usage qui est fait d'internet est suspect ou non. L'algorithme qui permet de déterminer si une connexion est suspecte n'est évidemment pas public et il est donc impossible d'avoir un contrôle démocratique sur cet outil de surveillance. Depuis le 15 mars 2015, l'État s'est doté de la capacité de bloquer des

connexions vers des sites « terroristes ». La mise en œuvre en est pour l'instant modérée, mais la plupart des pays dans lesquels ce type de blocage a été instauré ont répertorié à tort des sites comme terroristes, dont des sites d'opposants politiques.

3 - Écoutes de téléphonie et géolocalisation

Les téléphones mobiles sont surveillés de la même manière que les fixes. Mais il est aussi possible de localiser tout téléphone mobile, qu'il soit ou non équipé d'un GPS. Notons qu'il existe également des outils capables de récupérer le répertoire ou l'historique de navigation web d'un téléphone mobile, permettant alors de connaître les relations de son propriétaire ainsi que ses centres d'intérêts.

4 – Caméras de surveillance

Les caméras de surveillance sont soumises à autorisation préfectorale lorsqu'elles sont dirigées vers le domaine public et au contrôle de la CNIL (commission nationale informatique et libertés) sur les lieux privés. Elles continuent de s'étendre massivement sur tout le territoire (1 million en 2012) et se perfectionnent de jour en jour. Elles seront bientôt capables d'identifier formellement une personne d'après son image, de la suivre de caméra en caméra et de détecter « automatiquement » les activités potentiellement criminelles (projet européen INDECT).

5– IMSI catcher

Il s'agit de systèmes se présentant sous la forme de « valises » comportant un ordinateur portable. Celui-ci intercepte les communications de téléphonie mobile en imitant le comportement d'une antenne relais, de manière que les mobiles proches puissent s'y connecter. Les services de renseignement peuvent ainsi surveiller un mobile précis dans le cadre d'une filature ou établir une liste des participants à une manifestation. Selon la nouvelle loi, ces valises, jusque-là interdites, peuvent être utilisées par les services de renseignement avec l'aval du premier ministre, sans intervention d'un juge.

Ces moyens de surveillance sont quasiment tous aux mains de l'Etat. Il faudrait y ajouter les prélèvements ADN, la biométrie, les puces sans contact (RFID), la surveillance satellitaire et celle opérée sur les câbles sous-marins, le dispositif « voisins vigilants », les drones, les compteurs électriques intelligents (bientôt généralisés, par la loi du 17 août 2015), le Passenger Name Record, l'accord SWIFT, *etc.* Insistons sur la question des fichiers informatiques : il est interdit en France de croiser les données collectées au sein de fichiers différents, qu'ils soient publics ou privés. Néanmoins, les services de renseignement disposent de plusieurs fichiers sur lesquels la CNIL n'a aucun pouvoir de contrôle et dont l'existence ne s'appuie même pas sur une publication au Journal Officiel (le fichier CRISTINA par exemple, fichier de la Dgsi « pour la sécurité du territoire…). La surveillance est donc potentiellement globale.

Deux aspects sont préoccupants :

- **la surveillance lorsqu'elle est généralisée et concerne toute la population, y compris « ceux qui n'ont rien à se reprocher ». Elle met en cause dans ce cas plusieurs droits (d'expression, d'opinion, d'aller et venir) ;**
- **le manque de contrôles démocratiques efficaces.**

LA SURVEILLANCE ANTITERRORISTE : QUELS ENJEUX POUR NOS LIBERTÉS ?

Le terrorisme est un défi à la solidité de notre démocratie. Il nécessite une réponse efficace pour protéger notre société. **Les services de renseignement doivent disposer de moyens techniques et juridiques suffisants pour prévenir les actes criminels. Mais les mesures prises à ce titre ne doivent**

pas saper la démocratie, l'État de droit et les droits de l'Homme. Dans le domaine du renseignement, appliqué notamment à la lutte antiterroriste, la France adopte les mêmes méthodes que les États-Unis. Après la loi du 21 décembre 2012 « relative à la sécurité et à lutte contre le terrorisme », la loi de programmation militaire 2014 – 2019, la loi du 23 novembre 2014 « renforçant les dispositions relatives à la lutte contre le terrorisme », la loi sur le renseignement du 24 juillet 2015 entrée en vigueur le 3 octobre n'apporte pas les bonnes réponses.

1 – Les méthodes de surveillance utilisées menacent sérieusement **le droit au respect de la vie privée**, en particulier au secret des correspondances (par l'utilisation d'outils permettant d'intercepter des communications, dont les « boîtes noires » qui vont toucher la totalité des Français). Comme on l'a vu ci-dessus, ces dispositifs permettent de recueillir, de façon massive et très peu sélective, des données informatiques et téléphoniques constituant le quotidien de nos échanges.

> ***Article 12 – 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.*

Cela est d'autant plus grave que la loi permet des intrusions dans la vie privée des personnes suspectées mais aussi de celles travaillant dans les mêmes lieux, voire se trouvant à proximité.

Comment des recherches sur Google peuvent vous conduire à être assigné à résidence ?

Nacer vit à Septèmes-les-Vallons avec son épouse et ses quatre enfants. Il a travaillé pour Veolia dans une station d'épuration des eaux d'Aix-en-Provence de 2006 à 2009. Il est en conflit avec son ex-employeur. Quand il revient en août 2015 sur son ancien lieu de travail pour voir un collègue, Veolia signale sa présence au commissariat de police au motif qu'il pourrait préparer une attaque bactériologique !
Il est assigné à résidence le 15 novembre ; l'arrêté d'assignation explique que Nacer aurait effectué sur Google des recherches liées à la « chimie du traitement des eaux ». En réalité Nacer, qui a une incapacité permanente de travail de 25 %, avait simplement vérifié sur Google la liste des produits chimiques que Veolia lui avait communiquée en janvier 2015 pour qu'un médecin puisse établir un lien de causalité

entre son travail et la maladie contractée.
La ligne Internet de Nacer était-elle sous surveillance ? La nôtre pourrait donc l'être aussi ? Ou bien Google a-t-il transmis aux services de renseignement l'historique des recherches de Nacer ? Mais à la demande de qui et sous quel contrôle ?
L'arrêté a été annulé le 8 décembre, le ministère de l'Intérieur reconnaissant sa « méprise ».

2 – Ces mesures intrusives peuvent être mises en œuvre après autorisation du Premier ministre **sans un contrôle préalable indépendant**. La jouissance du droit fondamental au respect de la vie privée ne devrait pas être limitée sans que l'autorité judiciaire ne vérifie au préalable la légalité, la nécessité et la proportionnalité, c'est-à-dire le bienfondé, d'une mesure de surveillance. Certes la **Commission nationale de contrôle des techniques de renseignement** doit être consultée. Mais il s'agit d'une autorité administrative qui ne donne que des avis, la décision revenant au Premier ministre. Bien que l'autorité judiciaire soit considérée par la Constitution comme « gardienne des libertés individuelles », elle perd ici tout pouvoir au profit du seul Conseil d'État (qui n'est pas un organe de l'autorité judiciaire). Ainsi on a là une grave **atteinte à l'équilibre des pouvoirs**, qui est à la base de l'État de droit et de la jouissance effective des droits civils et politiques.

> ***Article 30 – Déclaration universelle des droits de l'homme***
> ***Aucune disposition*** *de la présente Déclaration* ***ne peut être interprétée comme impliquant*** *pour un État, un groupement ou un individu un droit quelconque de se livrer à une activité ou d'accomplir* ***un acte visant à la destruction des droits et libertés qui y sont énoncés***.

3 - La loi est-elle au moins claire et précise quant à la nature des activités reprochées ou soupçonnées des personnes devant être surveillées ? Ce n'est pas le cas, loin s'en faut ! En effet **le champ d'application de la loi est très large** : indépendance nationale, intégrité du territoire et de la défense nationale, intérêts majeurs de la politique étrangère et… prévention de toute forme d'ingérence étrangère ; mais aussi intérêts économiques, industriels et scientifiques majeurs…, prévention des violences collectives de nature à porter atteinte à la paix publique, de la criminalité et délinquance organisées… Autant **d'objectifs vastes et peu définis**. Qui vont bien au-delà de la lutte contre le terrorisme, et qui permettent de surveiller l'activité des syndicats, des ONG, des partis politiques, des cultes, de la société civile dans son ensemble.

Cette loi est extrêmement dangereuse. Elle autorise tous les excès, tous les débordements, toutes les « affaires » et toutes les atteintes aux libertés. Ce qui est en jeu, c'est bien sûr l'efficacité de la lutte contre le terrorisme, c'est aussi la société dans laquelle nous voulons vivre. **Il faut trouver le bon équilibre entre sécurité et respect des droits de l'Homme**. Comment le faire sans débat avec la société civile, les associations concernées, les citoyens ?

Le plus stupéfiant dans cette régression démocratique est que le pouvoir prétend défendre la société contre elle-même ; tous les acteurs sociaux – avocats, magistrats, journalistes spécialisés, autorités indépendantes (CNIL, CNIS, CNCDH), Défenseur des droits, associations de défense des DH, organisations syndicales…- ont fait part unanimement de leur refus d'une loi qu'ils considèrent comme liberticide *(voir par exemple le communiqué du 30 septembre 2015 de l'Observatoire des libertés et du numérique dont font partie notamment le syndicat de la magistrature, le syndicat des avocats de France, la quadrature du net et la LdH)*.

VERS UNE SOCIÉTÉ DE SUSPICION GÉNÉRALISÉE

Bien sûr, au vu des événements tragiques du mois de novembre et du contexte international, il peut sembler légitime de mettre en place de telles mesures de surveillance massive, de restreindre pour un temps nos droits et libertés en faveur d'une plus grande sécurité. Comme l'indique l'AEDH (association européenne des droits de l'Homme) dire cela sans nuance, c'est oublier que :

- Rien ne garantit que les droits et libertés que nous sacrifions aujourd'hui nous seront rendus demain. Au contraire, s'engager dans cette spirale c'est prendre le risque de s'enfoncer toujours plus loin dans les mesures liberticides, de rendre toujours plus difficile un retour en arrière.
- Les systèmes de surveillance mis en place ne sont pas utilisés uniquement dans le cadre de la lutte contre le terrorisme. En France, « *les intérêts économiques, industriels et scientifiques majeurs* » du pays (notamment) sont suffisants pour justifier une telle intrusion dans la vie privée de l'ensemble de la population.
- Rien ne permet d'affirmer que ces systèmes garantiront effectivement une sécurité accrue. L'expérience américaine des 15 dernières

années a montré que la surveillance de masse n'a jamais été la solution miraculeuse au terrorisme.

- Les systèmes de surveillance de masse sont pensés pour identifier plus facilement les individus présentant des risques. Or, l'actualité le montre, une grande majorité des personnes impliquées dans les attentats ou tentatives d'attentats étaient déjà connues des services de renseignement. Le problème est moins d'identifier tous les individus à risque que de surveiller efficacement par des moyens humains ceux pour lesquels il y a des indices convergents de dangerosité.

Voici ce que déclarait Amnesty International le 1er octobre 2015 : **« … La surveillance de masse incontrôlée fait du respect de la vie privée l'exception, ouvrant la porte à une société de** suspicion **généralisée ».**

Les mesures de surveillance de masse (qui peuvent permettre rapidement – du fait de l'évolution technique – un contrôle généralisé et sans limites de la population), mises entre les mains d'un pouvoir autoritaire ou totalitaire, pourraient ainsi conduire à un Etat policier avec ce que cela signifie d'arbitraire et d'atteintes aux libertés (par exemple qualifier ses opposants de terroristes). **Pour trouver un bon équilibre entre sécurité et respect des droits et des libertés**, nous proposons les trois principes suivants :

- Garantir l'**indépendance et l'efficacité de la Commission** de contrôle des techniques de renseignement : ses avis devraient être « conformes » c'est-à-dire obligatoirement suivis ;
- Mettre les décisions de surveillance sous le **contrôle du juge judiciaire** qui en vérifierait le bien-fondé ;
- Mettre cette importante question de société en **débat public** avec les professionnels (magistrats, journalistes…), les associations, les citoyens.

La LDH vous intéresse ? N'attendez pas, rejoignez la !

Ligue des Droits de l'Homme, section d'Aix-en-Provence Tél : 06 44 94 45 74
ldh.aix@laposte.net - www.ldh-aix.org - www.facebook.com/ldh.aix