Introduction

Surveiller : observer attentivement quelqu'un ou quelque chose pour le contrôler.

Dictionnaire *Larousse*.

L'idée d'un monde placé sous « surveillance totale » a longtemps paru un délire utopique ou paranoïaque, fruit de l'imagination plus ou moins hallucinée des obsessionnels du complot. Il faut pourtant se rendre à l'évidence : nous vivons, ici et maintenant, sous l'emprise d'une sorte d'Empire de la surveillance. À notre insu, nous sommes de plus en plus observés, épiés, surveillés, contrôlés, fichés. Chaque jour, des technologies nouvelles affinent le pistage de nos traces. Des firmes commerciales et des agences publicitaires fouillent notre vie. Au prétexte de lutter contre le terrorisme ou d'autres fléaux[1], des gouver-

1. Julian Assange affirme que les démocraties sont confrontées, en fait, aux « quatre cavaliers de l'Infocalypse » : le terrorisme, la pornographie enfantine, le blanchiment d'argent et les guerres contre la drogue et le narcotrafic. Chacun de ces fléaux, qui doivent être évidemment combattus, sert aussi de prétexte au renforcement

nements – y compris les plus démocratiques – s'érigent en *Big Brother*, n'hésitant plus à enfreindre leurs propres lois pour mieux nous espionner. En secret, les nouveaux États orwelliens, avec l'aide, souvent, des géants du Net, cherchent à établir des fichiers exhaustifs de nos contacts et de nos données personnelles[1] telles qu'elles figurent sur différents supports électroniques.

Après la vague d'attaques terroristes qui a frappé, depuis vingt ans, des villes comme New York, Washington, Paris, Toulouse, Bruxelles, Boston, Ottawa, Oslo, Londres, Madrid, Tunis, Marrakech, Casablanca, Ankara, etc., les autorités n'ont pas manqué d'utiliser le grand effroi de sociétés sous le choc pour intensifier la surveillance et réduire d'autant la protection de notre vie privée.

Entendons-nous bien, le problème n'est pas la surveillance en général, c'est la *surveillance de masse clandestine*. Il va de soi que, dans un État démocratique, les autorités ont toute légitimité, en s'appuyant sur la loi et avec

---

permanent des systèmes de surveillance globale des populations. *Cf.* Julian Assange, avec Jacob Appelbaum, Andy Müller-Maguhn et Jérémie Zimmermann, *Menace sur nos libertés. Comment Internet nous espionne. Comment résister,* tr. fr. A. Gerschenfeld et A. Muchnik, Paris, Robert Laffont, 2013.

1. Il s'agit essentiellement d'informations qui permettent de nous identifier soit directement, soit indirectement. À savoir : les nom, prénom, photo, date et lieu de naissance, statut matrimonial, adresse postale, numéro de sécurité sociale, numéro de téléphone, numéro de carte bancaire, plaque d'immatriculation du véhicule, e-mail, comptes des réseaux sociaux, adresse IP d'ordinateur, groupe sanguin, empreintes digitales, empreinte génétique, éléments d'identification biométrique, etc.

l'autorisation préalable d'un juge, de placer sous surveillance toute personne qu'elles estiment suspecte. Comme le dit Edward Snowden :

> Pas de problème s'il s'agit de mettre sur écoute Oussama Ben Laden. Aussi longtemps que les enquêteurs doivent avoir la permission d'un juge – un juge indépendant, un vrai juge, pas un juge secret –, et peuvent prouver qu'il y a une bonne raison de délivrer un mandat, alors ils peuvent faire ce travail. Et c'est comme cela que ça doit se faire. Le problème, c'est lorsqu'ils nous contrôlent tous, en masse, tout le temps, sans aucune justification précise pour nous intercepter, sans aucun indice juridique spécifique démontrant qu'il existe une raison plausible à cette violation de nos droits[1].

À l'aide d'algorithmes de plus en plus perfectionnés, des milliers de chercheurs, d'ingénieurs, de mathématiciens, de statisticiens, d'informaticiens traquent et criblent les informations que nous générons sur nous-mêmes. Des satellites et des drones au regard perçant nous suivent depuis l'espace. Dans les aérogares, des scanners biométriques analysent notre démarche, « lisent » notre iris et nos empreintes digitales. Des caméras infrarouges mesurent notre température corporelle. Les pupilles silencieuses des caméras vidéo nous scrutent sur les

1. Katrina van den Heuvel et Stephen F. Cohen, « Entretien avec Edward Snowden », New York, *The Nation*, 28 octobre 2014 ; tr. fr. M. Azzoug, *Mémoire des luttes*, 25 novembre 2014 (http://www.medelu.org/Les-revelations-sur-la).

trottoirs des villes ou dans les allées des hypermarchés[1]. Elles nous pistent aussi au bureau, dans les rues, dans l'autobus, à la banque, dans le métro, au stade, dans les parkings, les ascenseurs, les centres commerciaux, les routes, les gares, les aéroports.

De surcroît, avec le développement en cours de l'« Internet des objets », de nombreux éléments de notre foyer (réfrigérateur, armoire à pharmacie, cave à vins, etc.), voire même notre véhicule[2], vont aussi pouvoir fournir des informations précieuses sur nos pratiques de vie les plus personnelles.

Il faut dire que l'inimaginable révolution numérique que nous vivons, et qui bouleverse déjà tant d'activités et de professions, a chamboulé aussi totalement le champ du renseignement et de la surveillance. À l'heure d'Internet, celle-ci est devenue omniprésente et parfaitement immatérielle, imperceptible, indécelable, invisible. En plus, elle est désormais, techniquement, d'une excessive simplicité.

Logiciels espions

Finis les grossiers travaux de maçonnerie pour installer câbles et micros, comme dans le célèbre film

1. Comme l'a bien montré le film de Stéphane Brizé, *La Loi du marché*, 2015.
2. *Cf.* « La voiture, cette espionne », *Le Monde*, 2 octobre 2015.

Conversation secrète[1] où on voyait un groupe de « plombiers » présenter, dans un Salon consacré aux techniques de surveillance, des mouchards plus ou moins bricolés, équipés de boîtiers débordant de fils électriques qu'il fallait dissimuler dans les murs ou sous les planchers… Plusieurs scandales retentissants à l'époque – l'affaire du Watergate[2] aux États-Unis ; celle des « plombiers du *Canard*[3] » en France –, humiliants échecs pour les officines de renseignement, démontrèrent les limites de ces vieilles méthodes mécaniques, aisément détectables et repérables.

Aujourd'hui, mettre quelqu'un sur écoute est devenu d'une déconcertante facilité, à la portée du premier venu. Une personne ordinaire voulant espionner son entourage trouve en accès libre et dans le commerce un large choix d'options[4]. D'abord des manuels d'ins-

1. Francis Ford Coppola, *Conversation secrète (The Conversation)*, 1973.

2. Affaire d'espionnage politique aux multiples ramifications, le scandale du Watergate commence en 1972 avec l'arrestation de faux cambrioleurs venus poser des micros à l'intérieur de l'immeuble Watergate, à Washington, dans les bureaux du Parti démocrate, et aboutit, en 1974, à la démission de Richard Nixon, alors président des États-Unis.

3. Scandale politique sous la présidence de Georges Pompidou : en décembre 1973, à Paris, un système d'écoutes, posé par une dizaine d'agents de la Direction de la surveillance du territoire (DST) déguisés en plombiers, est découvert dans les locaux de l'hebdomadaire satirique *Le Canard enchaîné*.

4. Même si, en France, l'article 226-1 du Code pénal stipule qu'est « puni d'un an d'emprisonnement et de 45 000 euros

truction très didactiques « pour apprendre à pister et à espionner les gens[1] ». Et pas moins d'une demi-douzaine de logiciels espions (mSpy, GsmSpy, FlexiSpy, Spyera, EasySpy) qui « lisent » sans problème les contenus des téléphones portables[2] : SMS, e-mails, comptes Facebook, WhatsApp, Twitter, etc.

Avec l'essor de la consommation en ligne, la surveillance de type commercial s'est aussi grandement développée, et a donné naissance à un gigantesque marché de nos données personnelles, devenues des marchandises. Lors de chacune de nos connexions sur un site, des cookies[3] gardent en mémoire l'ensemble des recherches

---

d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui : en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ».

1. Lire, par exemple, Charles Cohle, *Je sais qui vous êtes. Le manuel d'espionnage sur Internet*, Nantes, Institut Pandore, 2014.

2. Il existe même des « comparateurs de logiciels de surveillance » que la publicité présente ainsi : « Un comparatif clair et complet des programmes mouchards pour mobile, vous permettant ainsi de faire votre choix et de prendre de cette façon une décision éclairée et économique avant d'acheter votre application de localisation ». *Cf.* http://www.smartsupervisors.com/

3. Le cookie est l'équivalent d'un petit fichier texte stocké sur le terminal de l'internaute. Il permet aux développeurs de sites Internet de conserver des données des utilisateurs afin de faciliter leur navigation. Les cookies ont toujours été controversés car ils contiennent des informations personnelles résiduelles pouvant potentiellement être exploitées par des tiers. (Source : Wikipédia.)

effectuées et permettent d'établir notre profil de consommateur. En moins de vingt millisecondes, l'éditeur du site visité vend aux annonceurs potentiels les informations nous concernant, collectées en particulier par les cookies. À peine quelques millisecondes plus tard, la publicité supposée avoir le plus d'impact sur nous surgit sur notre écran. Et nous voilà définitivement fichés[1].

Une alliance sans précédent

La surveillance s'est en quelque sorte « privatisée » et « démocratisée ». Ce n'est donc plus une affaire réservée aux seuls services étatiques de renseignement. Mais, en même temps, les capacités des États en matière d'espionnage de masse se sont accrues de façon exponentielle. Et cela en raison aussi des étroites complicités nouées avec les grandes firmes privées qui dominent les industries de l'informatique et des télécommunications. Dans l'entretien que nous publions dans la seconde partie de cet ouvrage, Julian Assange, fondateur de WikiLeaks[2], affirme :

> Les nouvelles sociétés, comme Google, Apple, Microsoft, Amazon et plus récemment Facebook ont établi des liens étroits avec l'appareil d'État à Washington, en

1. http://digital-society-forum.orange.com/fr/
2. À propos de WikiLeaks, lire I. Ramonet, *L'Explosion du journalisme*, Paris, Galilée, p. 81-106.

> particulier avec les responsables de la politique étrangère. Cette relation est devenue une évidence […]. Ils ont les mêmes idées politiques et partagent une vision du monde identique. Et, au bout du compte, les liens étroits et la vision du monde commune de Google et de l'Administration américaine sont au service des objectifs de la politique étrangère des États-Unis[1].

Cette alliance sans précédent – État + appareil militaire de sécurité + industries géantes du Web – a donc produit cet Empire de la surveillance dont l'objectif très concret et très clair est de mettre Internet, tout Internet, et tous les internautes, sur écoute.

À ce stade, il faut clairement garder à l'esprit deux idées bien précises :

1) Le cyberespace est devenu une sorte de cinquième élément. Le philosophe grec Empédocle soutenait que notre monde était constitué d'une combinaison de quatre éléments : terre, air, eau et feu. Mais la découverte d'Internet, avec son mystérieux interespace superposé au nôtre, formé de milliards d'échanges numériques de toute nature, de son *streaming* et de son *clouding*, a fait surgir un nouvel univers pour ainsi dire quantique, qui vient compléter, comme un authentique cinquième élément, la réalité de notre monde contemporain.

À cet égard, notons que chacun des quatre éléments traditionnels constitue, historiquement, un champ de bataille, un lieu de confrontation. Et que les États ont

1. *Cf. infra*, p. 138.