CYBERSURVEILLANCE MONDIALE DES TÉLÉCOMMUNICATIONS ET D'INTERNET

Patrick Le Guyader

CYBERSURVEILLANCE MONDIALE DES TÉLÉCOMMUNICATIONS ET D'INTERNET

ECHELON / PRISM / GAFAM / TECHNOLOGIE 5G /...

Autres ouvrages de l'auteur

- *Protection du patrimoine des entreprises et des institutions*
  Menaces – risques – parades
  Hermes Science *Lavoisier* 2006
- *Les systèmes électroniques et informatiques de surveillance*
  Contrôle de la vie privée des personnes et des biens
  Hermes Science *Lavoisier* 2008
- *Protection des données sur internet*
  Hermes Science *Lavoisier* 2013

Ce livre a été publié sur www.bookelis.com

ISBN : xxx-xx-xxx-xxxx-x

TABLE DES MATIÈRES

AVANT-PROPOS

En 1947, les États-Unis, associés à leurs partenaires anglo-saxons dans le cadre du pacte secret *UKUSA*, poursuivent leur collaboration sur les écoutes militaires afin d'être en mesure de déchiffrer les communications des pays étrangers ennemis.

Par décret en date du 4 novembre 1952, ils instituent une nouvelle Agence de sécurité nationale portant le nom de *NSA* (National Security Agency) destinée à poursuivre un programme appelé *Shamrock* visant à l'écoute et à l'enregistrement de toutes les communications téléphoniques et les télégrammes entrant et sortant des USA.

Au début des années 1970, un nouveau programme est mis en place, destiné à l'interception à grande échelle des communications transitant par les satellites commerciaux, de type INTELSAT et INMARSAT.

Ce vaste programme d'écoute des télécommunications satellitaires est appelé le réseau *ECHELON* (Code P415).

À la suite de la chute du mur de Berlin en 1989 et à l'éclatement de l'URSS en 1991, qui ont mis fin à la guerre froide, les États-Unis et ses partenaires ont élargi leur domaine de compétence à des surveillances plus orientées sur des secteurs politiques, économiques et commerciaux.

Depuis les attentats du 11 septembre 2001, l'insécurité étant devenue l'une des préoccupations premières des différents gouvernements et notamment des États-Unis, ces derniers exploitent cette situation pour mettre en place une vaste opération de réduction des libertés publiques au titre du terrorisme, en violant

le 4e amendement de la Constitution américaine qui garantit le droit à la vie privée de ses citoyens.

Le rédacteur avait déjà attiré l'attention des lecteurs dans son livre intitulé *Les Systèmes électroniques et informatiques de surveillance – Contrôle de la vie privée des personnes et des biens*, éditions Lavoisier, 2008.

Après avoir mis en place le *Patriot Act* en 2001 et le *FISA Amendments Act* en 2008, qui garantit l'impunité aux entreprises qui coopèrent avec les autorités en leur fournissant des renseignements, les gouvernements américains successifs ont privilégié les sources techniques utilisées par la NSA afin de soutenir leur économie et les entreprises américaines dans leurs exportations.

En 2013, le lanceur d'alerte Edward Snowden, ingénieur dans une société de sous-traitance de la NSA, implantée à Hawaï, a dénoncé le système de surveillance internet *PRISM*, effectué par la NSA, via les câbles sous-marins.

Dans un contexte international très tendu, les Américains n'hésitent plus, dans la recherche du renseignement privé, à continuer de se doter d'armes juridiques. Après le Patriot Act et la loi FISA, une nouvelle loi du 23 mars 2018 institue le *Cloud Act* (Clarifying Lawful Overseas Use of Data Act), destiné à permettre aux autorités judiciaires américaines d'accéder aux données électroniques stockées à l'étranger.

La NSA est aidée dans cette tâche de recherche de renseignement par les *GAFAM* (Google, Amazon, Facebook, Apple et Microsoft), qui sont tous implantés sur le territoire américain.

L'auteur s'efforce d'attirer l'attention du lecteur sur les relations étroites qui unissent la NSA et les GAFAM dans la recherche et le stockage des données privées des internautes. Ces géants de l'internet se dotant également de *câbles sous-marins*, dont la reconnaissance juridique reste à démontrer.

Il remarque que, dans un contexte commercial international tendu et incertain, l'administration américaine est passée maître dans l'art d'imposer une *extraterritorialité juridique* du droit américain.

Il se félicite de la mise en place du Règlement général sur la protection des données (RGPD) européen, applicable, sans transposition, depuis le 25 mai 2018 et visant les GAFAM mais également toutes les entreprises européennes, les prestataires de services et les sous-traitants.

L'auteur s'interroge sur l'absence de réaction des pays européens après les enquêtes parlementaires menées sur le réseau de surveillance Echelon.

Il sensibilise également les utilisateurs sur l'usage des moyens mobiles de communication face à l'émergence exponentielle des nouvelles technologies telles que le Web 3.0, les télécommunications de la nouvelle génération 5G ou l'intelligence artificielle.

Il constate la politique protectionniste menée par les États-Unis visant les nouvelles technologies internationales de l'information et de la communication, ainsi que les surveillances commerciales menées par la NSA (Echelon et Prism) vis-à-vis des entreprises étrangères et notamment françaises.

Il attire l'attention sur le fait que la Chine est actuellement le moteur de croissance des nouvelles technologies dans le monde, avec la société *Huawei*, qui maîtrise parfaitement les télécommunications 5G.

Il s'interroge également sur les ambitions chinoises de créer de nouvelles routes de la soie digitales (câbles sous-marins) entre le bassin méditerranéen et la Chine, via notamment un hub pakistanais, qui ne manqueront pas de soulever des interrogations politiques et sécuritaires sur le plan international.

George Orwell : *« La paix, c'est la guerre. »*

Chapitre I

PRÉSENTATION

À l'heure de la mondialisation où plus de la moitié des échanges se font par itinérance, il est impossible, tant pour les entreprises que pour les particuliers, de communiquer autrement que par les réseaux téléphoniques satellitaires et le réseau internet, via les câbles sous-marins.

Depuis une vingtaine d'années, nous avons assisté à la montée en puissance de l'informatique, d'internet et des réseaux de communication.

Nous sommes passés du *Web 2.0,* dit Web social, simple d'utilisation ne nécessitant pas des connaissances techniques et informatiques pour les utilisateurs, au *Web 3.0* comme l'internet des objets (IoT) puis au *Web 4.0* dit Web des robots.

Il en est de même pour l'évolution des télécommunications, de la 1G à la 4G et bientôt la 5G, qui permet d'atteindre des débits très importants autorisant des usages multimédias (vidéo, visioconférence) ou l'accès à internet haut débit.

Cette évolution globale de la *téléphonie mobile internet,* permettant l'utilisation des smartphones comme de véritables petits ordinateurs, est un facteur de danger quant à la protection des données personnelles et des informations des entreprises.

Ce document a pour but d'attirer l'attention sur les pratiques et les techniques utilisées par les services de renseignement anglo-saxons pour dérober, en grandes quantités et de façon transparente, les informations numériques tant sur les moyens fixes que sur les périphériques mobiles lors de déplacements professionnels ou privés, notamment à l'étranger.

Plus globalement, il a pour but de sensibiliser sur la *cybersurveillance* et le *cyberespionnage,* qu'ils soient politiques ou économiques, issus des pratiques de la guerre froide.

Ce livre a pour objectif de :

- Sensibiliser le lecteur sur l'ensemble des technologies de l'information et de la communication et les supports de transmission utilisés faisant l'objet d'une écoute systématique par les services de renseignement gouvernementaux, notamment anglo-saxons, dans le cadre du pacte UKUSA avec la NSA.
- Fournir des éléments concrets sur les différents moyens utilisés (satellites, stations terrestres, satellites espions, câbles sous-marins, stations d'atterrage, etc.) pour récupérer les informations personnelles, politiques, commerciales, etc.
- Approfondir l'organisation autour des réseaux ECHELON et PRISM.
- Développer le rôle joué par les GAFAM en tant que support dans la transmission des informations auprès de la NSA.
- Aborder l'émergence des nouvelles technologies liées au Web 3.0, les télécommunications 5G et l'intelligence artificielle.
- Dénoncer l'espionnage politique, industriel et commercial qui en découle.

Nous aborderons les thèmes suivants :

- Les origines du pacte UKUSA (chapitre 2)
- Les réseaux de la NSA (chapitre 3)
- Les moyens utilisés pour la surveillance (chapitre 4)
- Le rôle des GAFAM (chapitre 5)
- Les menaces pesant sur les technologies (chapitre 6)
- La technologie 5G (chapitre 7)
- Les autres moyens de surveillance (chapitre 8)
- Les protections sur les moyens mobiles (chapitre 9)
- Le renseignement économique, politique et commercial (chapitre 10)