(Source : Hashtable)

Si l'année a changé, les mauvaises habitudes, elles, sont bien restées les mêmes. Pour tenter d'y mettre fin, l'individu lambda se lancera donc dans de bonnes résolutions. Certaines tiendront, beaucoup seront oubliées dans quelques jours. Pour les politiciens en revanche et en particulier ceux qui sont au pouvoir, nulle prise de conscience : les mauvaises habitudes sont bien trop confortables pour qu'on les abandonne ainsi.

Et dans ces mauvaises habitudes, on retrouve en peloton de tête celle qui consiste à espionner tout le monde, ses adversaires et le peuple en premier. La fin d'année, déjà propice à faire passer les informations les plus scandaleuses sans que personne ne réagisse, aura aussi avantageusement été employée à camoufler dans les vapeurs éthyliques les décrets et les lois les plus scélérats.

Alors que 2014 agonisait, c'est ainsi qu'on découvrait par le détail les capacités réelles de la NSA, l'agence d'espionnage américaine, à casser les chiffrements employés par divers procédés. Pour les habitués de ces colonnes et pour les citoyens vigilants de leurs libertés, découvrir que la NSA peut casser assez facilement certains protocoles sécurisés, Skype ou les échanges par Facebook n'est pas une grosse surprise.

Il n'en reste pas moins que ces éléments viennent confirmer que les logiciels comme TOR, GnuPG ou OTR représentent de réelles solutions pour garantir une assez bonne

confidentialité de vos échanges d'information, puisque l'agence américaine avoue avoir de bonnes difficultés à casser la cryptographie employée par ces logiciels.

Commentaire :

Admettons pour un instant que ces logiciels soient *réellement* une façon de communiquer de façon confidentielle (ce dont je doute très fort), n'est-ce pas là la plus belle façon d'attirer inutilement les soupçons? Qui plus est, ne serait-ce pas une belle attrape que de créer des logiciels à fortecryptographie afin de cibler qui a quelque chose à cacher?

En ces temps où, très clairement, l'emprise de Big Brother s'étend un peu partout et surtout bien au-delà d'où on souhaiterait le cantonner, ces éléments vont devenir rapidement des figures imposées.

Et pendant que beaucoup (pour ne pas dire « tous ou à peu près ») se focalisaient sur les débordements de plus en plus inquiétants de la NSA, le gouvernement français, d'autant plus en catimini que le sujet est sensible et la période propice aux petits coups de pendards, en profitait pour recréer les Renseignements Généraux, pourtant disparus depuis quelques années.

En effet, au détour de l'un de ces énièmes rapports que le citoyen ne peut pas lire tant ils

sont nombreux, copieux et amphigouriques, on apprend que vient commodément de voir le jour un Service central de renseignement territorial (SCRT) équipé de tous les attributs habituels d'un outil de renseignement à l'usage du pouvoir en place : des fonctionnaires de police, des gendarmes, des autorisations d'écoutes téléphoniques, et des missions franchement proches des précédents **Renseignements généraux, comme la recherche d'informations concernant *« tous les domaines de la vie institutionnelle, économique et sociale susceptibles d'entraîner des mouvements revendicatifs ou protestataires »*…**

À ces missions évidemment classiques s'ajoute celle de l'étude et du renseignement lié à la cyber-criminalité, **cette dernière étant suffisamment vague et mal définie pour y inclure, en définitive, tous les types d'informations échangées sur Internet qui pourraient intéresser le pouvoir**. Bref : si les Américains ont, à l'évidence, mis le paquet pour espionner la planète entière, l'État français n'est pas en reste pour tenter de faire pareil, à son échelle, et au moins sur la population sous sa responsabilité. On le savait déjà, mais le très sobre retour des Renseignements généraux permet de brosser un tableau de plus en plus précis de ce qui se met en place dans le pays, alors que les élections présidentielles de 2017 s'approchent doucement.

D'autant qu'à cette réintroduction furtive, il faut adjoindre, toujours en tapinois, la publication du décret d'application de l'article 20 de la Loi de Programmation Militaire, dont j'ai déjà parlé dans ces colonnes en 2013 et en 2014. **Pour rappel, ce texte prévoit un accès très vaste (trop, en fait) des services de l'État aux télécommunications (téléphone, SMS, Internet) et à toutes les informations qui transitent par les réseaux nationaux, et comme d'habitude, ce sont les prétextes de lutte anti-terroriste qui ont servi pour élaborer un véritable open-bar de la mise sur écoute de tous les Français.**

Ce décret permet de donner quelques informations sur la façon dont ces écoutes seront mises en place. En substance, un service spécialisé du Premier ministre en sera chargé en centralisant les demandes des agents et les transmettra aux opérateurs de téléphonie ou internet, en les épurant de toute information sensible. Car si, sur le papier tout du moins, les

services de l'État devront justifier leurs requêtes auprès du Premier ministre (via une *« personnalité qualifiée »*), **ces justifications ne seront pas disponibles aux opérateurs et les fournisseurs d'accès ne sauront même pas de quel service ou ministère émane une demande, ni à quelle date elle a été formulée.**

Quant à la formulation de ce qui pourra être demandé et « intercepté » (*« informations ou documents traités ou conservés par les réseaux ou services de communications électroniques, y compris 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, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications »*), **elle est si vaste qu'elle laisse toute la place nécessaire à toutes les dérives possibles et imaginables.** Et comme l'histoire nous l'a prouvé, si la dérive est

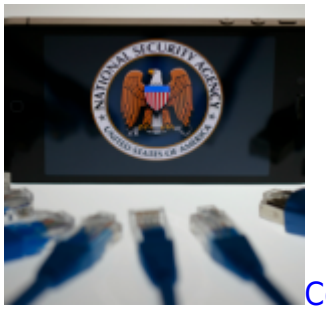
possible, elle aura très probablement lieu.

D'ailleurs, vu les contre-mesures timidement mises en place (la Commission nationale de contrôle des interceptions de sécurité, sans aucun pouvoir de sanction réel), et le flou qui règne sur la régulation qui devrait pourtant entourer d'aussi *libérales* facilités offertes à l'État pour espionner ses petits citoyens, **ces dérives seront non seulement possibles, mais elles seront inévitables**.

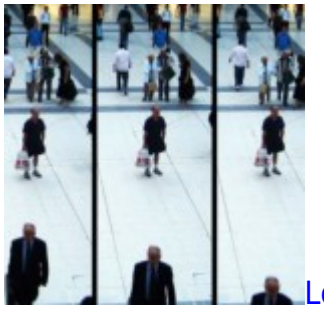
Non, vraiment, cette période de fêtes de fin d'année fut particulièrement riche pour l'État Big Brother. **Dans le silence assourdissant des grands médias, les politiciens qui nous dirigent se sont généreusement octroyés de belles parts de notre liberté, et notamment la plus fondamentale d'entre elles : celle de pouvoir conserver son intimité.**

À ce titre, l'année 2015 commence sur les chapeaux de roues !

À lire également :



Comment la NSA utilise les données des téléphones pour relier les personnes entre elles



Logiciels mouchards, métadonnées, réseaux sociaux et profilage : comment la France surveille ses citoyens

La NSA aspire des millions de carnets d’adresses dans le monde

Grande Bretagne : 8 millions d’enfants fichés en secret