Révélations sur le Big Brother français

Jacques Follorou, Franck Johannès

Le Monde, 14 juillet 2013

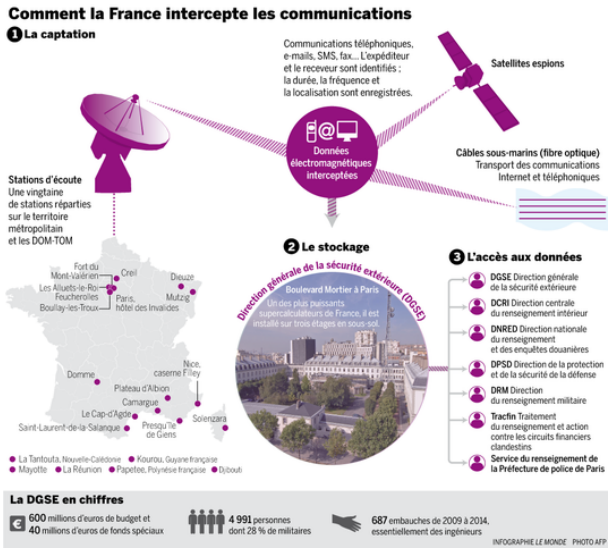

FIGURE 1 –

Si les révélations sur le programme d'espionnage américain Prism ont provoqué un concert d'indignation en Europe, la France, elle, n'a que faiblement protesté. Pour deux excellentes raisons : Paris était déjà au courant. Et fait la même chose.

Le Monde est en mesure de révéler que la Direction générale de la sécurité extérieure (DGSE, les services spéciaux) collecte systématiquement les signaux électromagnétiques émis par les ordinateurs ou les téléphones en France, tout comme les flux entre les Français et l'étranger : la totalité de nos communications sont espionnées. L'ensemble des mails, des SMS, des relevés d'appels téléphoniques, des accès à Facebook, Twitter, sont ensuite stockés pendant des années.

Si cette immense base de données n'était utilisée que par la DGSE qui n'officie que hors des frontières françaises, l'affaire serait déjà illégale. Mais les six autres services de renseignement, dont la Direction centrale du renseignement intérieur (DCRI), les douanes ou Tracfin, le service de lutte contre le blanchiment, y puisent quotidiennement les données qui les intéressent. En toute discrétion, en marge de la légalité et hors de tout contrôle sérieux. Les politiques le savent parfaitement, mais le secret est la règle.

Un dispositif clandestin

Ce Big Brother français, petit frère des services américains, est clandestin. Pourtant, son existence figure discrètement dans des documents parlementaires. Les huit députés et sénateurs de la délégation parlementaire au renseignement rappellent, dans leur rapport du 30 avril, 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 renseignement".

Les parlementaires proposent même d'aller plus loin, de « *renforcer les capacités exploitées par la DGSE* » et de « *consolider l'accès des autres services aux capacités mutualisées de la DGSE* ».

La cible : les « métadonnées »

Les services de renseignement cherchent non pas le contenu des messages, mais leur contenant. Il est plus intéressant de savoir qui parle et à qui que d'enregistrer ce que disent les gens. Plus que les écoutes,

ce sont ces données techniques, les « *métadonnées* », qu'il s'agit d'éplucher.

La DGSE collecte ainsi les relevés téléphoniques de millions d'abonnés – l'identifiant des appelants et des appelés, le lieu, la date, la durée, le poids du message. Même chose pour les mails (avec possibilité de lire l'objet du courrier), les SMS, les fax... Et toute l'activité Internet, qui passe par Google, Facebook, Microsoft, Apple, Yahoo !... C'est ce que la délégation parlementaire au renseignement appelle très justement « *le renseignement d'origine électromagnétique* » (ROE M), traduction du Sigint (signal intelligence) de la NSA.

Ces métadonnées permettent de dessiner d'immenses graphes de liaisons entre personnes à partir de leur activité numérique, et ce depuis des années. De dessiner une sorte de journal intime de l'activité de chacun, tant sur son téléphone que sur son ordinateur. A charge ensuite pour les services de renseignement, lorsqu'un groupe intéressant a été identifié, d'utiliser des techniques plus intrusives, comme les écoutes ou les filatures.

Un supercalculateur boulevard Mortier

Le dispositif est évidemment précieux pour lutter contre le terrorisme. Mais il permet d'espionner n'importe qui, n'importe quand. La DGSE collecte ainsi des milliards de milliards de données, compressées et stockées, à Paris, sur trois niveaux, boulevard Mortier, dans les sous-sols du siège de la DGSE.

Le directeur technique de la DGSE depuis 2006, Bernard Barbier, a évoqué le dispositif en public à deux reprises, en 2010, lors du Symposium sur la sécurité des technologies de l'information et des communications, puis devant l'Association des réservistes du chiffre et de la sécurité de l'information, des propos rapportés sur de rares sites spécialisés, dont Bug Brother, le blog de Jean-Marc Manach hébergé par Le Monde.

Bernard Barbier a alors parlé du « *développement d'un calculateur à base de FPGA* » (des circuits logiques programmables), qui est « *probablement le plus gros centre informatique d'Europe après les Anglais* », capable de gérer des dizaines de pétaoctets de données, – c'est-à-dire des dizaines de millions de gigaoctets. La chaleur dégagée par les ordinateurs suffit à chauffer les bâtiments de la DGSE...

La France est dans le top 5 en matière de capacité informatique, derrière les Etats-Unis, la Grande-Bretagne, Israël et la Chine. M. Barbier estimait à 4 milliards le nombre d'objets connectés en 2013, avec un débit de l'ordre de 1 milliard de communications simultanées. "Aujourd'hui, nos cibles sont les réseaux du grand public, indiquait le directeur, parce qu'utilisés par les terroristes."

La DGSE, à la tête de "la plus forte équipe de crypto-mathématiciens" de France, pénètre les systèmes informatiques – et collecte évidemment des millions de données personnelles.

Un renseignement « mutualisé »

Les autres services de renseignement français ont accès en toute discrétion à cette gigantesque base de données, sobrement baptisée "infrastructure de mutualisation". Il s'agit de la direction du renseignement militaire (DRM), la direction de la protection et de la sécurité de la défense (DPSD), la direction centrale de la sécurité intérieure (DCRI), la Direction nationale du renseignement et des enquêtes douanières (DNRED), de Tracfin et même du petit service de renseignement de la préfecture de police de Paris.

Selon le Sénat, 80 % des moyens de la direction technique de la DGSE sont utilisés par ces autres services. Chacun donne le nom de la cible visée à son interlocuteur de la DGSE, qui répond « *hit* » (touché) ou « *no hit* » selon qu'elle figure ou non dans la base de données. Puis les services de la DGSE rendent intelligibles les métadonnées, en y ajoutant du renseignement classique.

Les demandes de consultations sont loin de se limiter au seul terrorisme ou à la défense du patrimoine économique. Le libellé très flou de la protection de la sécurité nationale permet notamment d'identifier les entourages de personnalités au plus haut niveau de l'Etat, quelles que soient leur qualité et la nature des liens espionnés.

Absence de contrôle

Le dispositif est parfaitement illégal – « *a-légal* », corrige l'un des patrons d'une des agences de renseignement. « *Le régime juridique des interceptions de sécurité interdit la mise en œuvre par les services de renseignement, d'une procédure telle que Prism, assure la Commission nationale de l'informatique et des libertés (CNIL). Chaque demande de réquisition de données ou d'interception est ciblée et ne peut pas être réalisée de manière massive, aussi quantitativement que temporellement. De telles pratiques ne seraient donc pas fondées légalement.* » La CNIL ne peut infirmer ou confirmer l'existence du système français – elle n'a d'ailleurs pas accès aux fichiers de la DGSE ou de la DCRI.

La loi encadre certes strictement les interceptions de sécurité, autorisées par le premier ministre, sur avis de la Commission nationale consultative des interceptions de sécurité (CNCIS), mais n'a en rien prévu un stockage massif de données techniques par les services secrets. « *Voilà des années que nous sommes dans l'autorisation virtuelle, confie l'un des anciens patrons des services. Et chaque agence se satisfait bien de cette liberté permise grâce au flou juridique qui existe autour de la métadonnée.* »

Un parlementaire confirme « *qu'une grande part des connexions électroniques en France est effectivement interceptée et stockée par la DGSE* ». Mais officiellement, « *l'infrastructure de mutualisation* » n'existe pas.