La faille juridique qui permet à la DGSE de singer la NSA

Protégés par un obscur article de loi, nos espions captent et enregistrent des milliards de données personnelles.

LA transparence attendra. Le projet de loi de programmation militaire, qui doit être voté cet automne, était censé renforcer le contrôle du Parlement sur les services secrets. Il n'en sera rien : le texte adopté lors du Conseil des ministres du 2 août n'aligne que des belles phrases qui n'engagent pas à grand-chose. Au désespoir de la Délégation parlementaire au renseignement, qui n'aura pas les moyens de savoir si les barbouzes de la DGSE espionnent – comme la NSA américaine – les simples citoyens.

Après les déclarations de Hollande, qui avait promis, le 10 juin, d'*« élargir ses prérogatives »*, la Délégation, présidée par le PS Jean-Pierre Sueur, avait cru qu'elle disposerait de vrais pouvoirs d'investigation. En particulier du droit d'auditionner n'importe quel agent des services et non plus, comme aujourd'hui, seulement les *« directeurs en fonction »* de la DGSE, de la DCRI ou de la DRM (Direction du renseignement militaire).

Espoir vite douché : l'article 5 du projet de loi accorde à la Délégation la possibilité de rencontrer uniquement les *« directeurs d'administration centrale ayant à connaître des activités des services »*. De plus, ces auditions ne pourront avoir lieu qu'avec l'*« accord préalable des ministres concernés »*.

Les autres demandes de la Délégation ont été retoquées. A commencer par la proposition du député PS Jean-Jacques Urvoas. Ce doux rêveur suggérait la création d'une autorité indépendante, dotée de moyens suffisants pour contrôler réellement les services secrets.

La botte secrète des barbouzes

Cette victoire par KO devrait permettre aux agents de la DGSE de continuer de suivre de près les communications électroniques de leurs concitoyens. Sans trop se soucier de la loi de 1991 qui institue un strict contrôle des écoutes administratives par la Commission nationale de contrôle des interceptions de sécurité (CNCIS).

Cette dernière estime que la DGSE respecte la législation quand il s'agit d'écoutes en bonne et due forme, effectuées sur le territoire national. Un contrôleur de la Commission visite d'ailleurs régulièrement son QG du boulevard Mortier. Mais la DGSE utilise d'autres filières…

D'abord, les barbouzes ne sont pas soumises à la loi française quand elles opèrent de l'étranger. Ensuite, une disposition méconnue leur permet de capter en douce une masse énorme d'informations sans en référer à quiconque. L'article 20 de la loi de 1991 prévoit que la CNCIS n'a pas à se mêler *« des mesures prises par les pouvoirs publics pour assurer, aux seules fins de défense des intérêts nationaux, la surveillance et le contrôle des transmissions empruntant la voie hertzienne »*.

Lors du vote de ce texte, le gouvernement Rocard avait expliqué qu'il ne s'agissait que d'un simple *« balayage aléatoire »*. En clair : les services secrets peuvent pêcher au petit bonheur la chance sur les ondes, à condition de ne pas viser quelqu'un en particulier. Une partie des échanges Internet passent par les satellites ou par les faisceaux hertziens. Pour le reste, il y a fort à parier que la DGSE traite le gros du trafic transitant par câble et fibre optique comme le hertzien. Qui vérifiera ?

Stock de balayures

« L'article 20, c'est la zone grise, confie Jean-Jacques Urvoas au "Canard". *On touche là à l'incapacité du gouvernement de contrôler les méthodes des services. »* Car la loi de 1991 n'avait pas prévu la formidable extension des mémoires d'ordinateurs. Or la DGSE ne se contente pas de balayer : après avoir capté des données plus ou moins au hasard (les professionnels disent « sniffer »), elle conserve – sans aucune limite de temps – tout ce que ramassent ses balayettes électroniques. Comme l'a souligné « Le Monde » (23/8), il s'agit de « métadonnées » qui permettent de savoir qui a communiqué (par téléphone, courriel, SMS, Internet…) avec qui, à quel moment et, parfois, de quel endroit.

Les mots de passe utilisés par tout un chacun subissent le même traitement : *« Nous stockons bien évidemment tous les mots de passe. Nous avons des dictionnaires de millions de mots de passe »*, avait imprudemment avoué, en juin 2010, Bernard Barbier, le directeur technique de la DGSE, au cours d'une rencontre avec des professionnels de la sécurité informatique. Le même avait alors ajouté : *« Toutes ces métadonnées, on les stocke sur des années, et, quand on s'intéresse à une adresse IP* (connexion à Internet) *ou à un numéro de téléphone, on va chercher dans nos bases de données, on retrouve la liste de ses correspondants pendant des années et on arrive à reconstituer tout son réseau. »*

Cette formidable bibliothèque est également mise à la disposition des services de police – et plus particulièrement de la DCRI. Et cela en dehors de tout contrôle, puisque la CNCIS n'a pas le droit de se mêler de ces histoires de *« balayage hertzien »*. Elle est tout juste bonne à passer la serpillière…

Hervé Liffran

C'est ma première "cryptoparty"

FURIEUSEMENT tendance, la « cryptoparty » ! Cette réunion d'un nouveau genre, bière dans le sac et ordi sous le bras, fait un triomphe chez nos voisins teutons. C'est la riposte qu'ont trouvée les citoyens allemands à l'insatiable curiosité de la NSA américaine, ses grandes oreilles et son mépris absolu de la vie privée.

Vaccinés par le nazisme, avec, en prime, les piqûres de rappel de la Stasi pour ceux de l'Est, ils ont décidé de s'organiser. Le principe est simple : un ou plusieurs spécialistes de la Toile, souvent des hackers, expliquent à plusieurs douzaines d'utilisateurs comment protéger leurs courriels et leurs conversations. *« Il y a peu,* écrit la "Berliner Zeitung" (16/7), *les gens qui verrouillaient leurs e-mails ou leur PC étaient moqués comme autant de conspirationnistes. Depuis les révélations d'Edward Snowden, les utilisateurs lambda, eux aussi, se demandent comment naviguer sans être observés. »*

Lors de ces soirées, l'internaute se voit proposer des solutions pour se protéger. D'abord, apprendre à élaborer un mot de passe redoutable. Puis, penché sur le clavier, se familiariser avec DuckDuckGO, un moteur de recherche qui ne vend pas les mots-clés utilisés par ses clients. Ou avec TOR (en anglais, l'acronyme de « Onion Router »), élu meilleur logiciel libre de l'année en 2011. Ce réseau mondial construit par couches successives (d'où son nom) permet de se balader incognito sur le Net. Sans oublier le système « https everywhere ». Né d'une collaboration entre TOR et l'Electronic Frontier Foundation, qui souhaite promouvoir le respect de la vie privée, il permet le cryptage automatique des données personnelles échangées sur toute une série de sites Web.

La clé USB du bonheur ?

B. R.

Les terroristes de papier

S'IL subsistait le moindre doute sur la gravité des violations du droit et des libertés publiques commises par la NSA et l'administration américaine, les réactions fiévreuses et désordonnées des gouvernements concernés suffiraient à le dissiper. L'enjeu est tel qu'une vieille démocratie comme la Grande-Bretagne s'assied soudain sur la liberté de la presse, soucieuse avant tout de voler au secours de l'allié américain et de cacher son éventuelle complicité. La France se tait, après avoir montré sa complaisance en bloquant l'avion du président bolivien, Evo Morales, dans lequel aurait pu se trouver Snowden, le lanceur d'alerte par qui le scandale est arrivé. Seule l'Allemagne proteste. Et, devant ce spectacle, la Russie de Poutine se marre.

En première ligne depuis qu'il a révélé l'affaire, le « Guardian », respectable quotidien anglais, est sous pression. David Cameron, le Premier ministre conservateur, lui a d'abord envoyé un émissaire pour le convaincre de lui remettre les disques durs sur lesquels figuraient les documents de Snowden : *« Vous vous êtes bien amusés, maintenant vous n'avez plus besoin d'écrire là-dessus. »*

L'insécurité de l'Etat

Le 20 juillet, le « Guardian » cède sous la menace d'une procédure judiciaire qui peut l'empêcher de travailler. Les disques durs sont détruits dans les sous-sols du journal devant deux experts de l'agence de renseignement électronique britannique. Même les Américains ont trouvé le coup plutôt raide : *« Il est difficile d'imaginer que des représentants des forces de l'ordre détruisent, aux Etats-Unis, des documents de journalistes »*, a dû convenir le porte-parole d'Obama à la Maison-Blanche.

L'ère numérique rend ridicule cette destruction puisque des copies ont été réalisées. Mais le gouvernement britannique ne s'est pas contenté de cet autodafé numérique. Le 18 août, David Miranda, le compagnon du journaliste qui avait recueilli les confidences de Snowden, a été retenu pendant neuf heures dans la zone de transit de l'aéroport de Heathrow. Son agenda, ses téléphones, ses ordinateurs, sa console de jeux vidéo, ses clés USB, son appareil photo ont été saisis. Sous quel prétexte ? Celui de la loi antiterrorisme. Raccourci saisissant : la défense des libertés publiques est ainsi assimilée à un attentat à la bombe. Et le journaliste à une menace pour la sécurité de l'Etat.

Mais, au-delà de la presse, ce sont bien les libertés individuelles de tous dont il s'agit, puisque n'importe quel internaute peut être suivi à la trace par un gouvernement. Les autorités de contrôle européennes (équivalant à la Cnil française) bataillaient depuis des années contre Google et les réseaux sociaux pour garantir à chaque citoyen un droit de regard sur l'utilisation de ses données personnelles. Aujourd'hui, ce sont les Etats qu'elles trouvent sur leur chemin. Rude tâche, alors qu'elles n'ont aucun moyen de coercition. Une nouvelle charte Informatique et Libertés s'impose, au moins à l'échelle européenne, mais l'affaire est loin d'être entendue car rien n'indique que les gouvernements, pourtant très à l'écoute, voudront bien y prêter une oreille attentive.

Jean-Michel Thénard