Surveillance des télécommunications : fin de partie

Tony BUNYAN

Tout au long de ces quatre dernières années, l'Union européenne a été le champ d'une bataille invisible et jamais rapportée entre d'une part, les exigences des agences de sécurité (agences de sécurité intérieure et extérieure, police, gendarmerie, douanes, services de contrôle de l'immigration…) et d'autre part, les fonctionnaires de l'Union européenne chargés de la protection des données (et soutenus par la Commission européenne) [1].

Au centre de ce conflit, se trouve la tentative d'assaut lancée par les agences de sécurité sur les lois de l'Union européenne relatives à la protection des données et de la vie privée au motif qu'elles feraient obstacle à leur besoin d'avoir accès à toutes les données échangées par des moyens de télécommunication. Selon les agences de sécurité, ces données devraient être conservées par les prestataires de service pendant une période s'étalant de un à sept ans et ces mêmes agences devraient pouvoir y avoir accès.

Les Directives européennes de 1995 et 1997 stipulent que de telles données ne peuvent être enregistrées que pour un seul motif : la vérification par le client de la liste détaillée de ses appels, après quoi ces données doivent être effacées ou rendues anonymes. Ces deux directives constituent le cœur même du droit à la vie privée au sein de l'UE et si celui-ci devait être remis en cause (garder une trace des données pour des raisons policières), cela le détruirait fatalement. L'histoire commence en 1993.

Les origines

Du temps de la guerre froide, d'énormes sommes ont été affectées par les Etats-Unis au NSA, et par le Royaume-Uni au *Government Communications Headquarters*(GCHQ) afin de mettre en place un système global de surveillance au profit des institutions militaires et de renseignement. Ce programme a débuté avec l'Accord dit UKUSA de 1948. Plus tard, au début des années 1980, ces mêmes institutions ont étendu leur réseau de surveillance grâce au système *Echelon*, afin de couvrir de façon encore plus étroite le renseignement politique et économique.

Les agences de sécurité n'ont pas eu accès à ce système de renseignement, si ce n'est de façon tout à fait exceptionnelle, lorsque

leur aide était jugée nécessaire. Les pouvoirs des agences de sécurité étaient alors définis par les différentes législations nationales, autorisant les interceptions des télécommunications et des postes sous réserve d'obtenir un mandat ou un ordre des juges et concernant un individu, une entreprise, une organisation ou un bâtiment précis. Bien entendu, les écoutes téléphoniques illégales se sont multipliées et dans la plupart des pays, les chiffres relatifs aux écoutes téléphoniques opérées par les agences de sécurité intérieure ont rarement été publiés.

Toutefois, au début des années 1990, il devint évident que l'on entrait dans une nouvelle ère des télécommunications avec l'apparition du téléphone mobile. Apparition qui présentait non seulement un nouveau défi pour les agences de sécurité mais surtout une nouvelle opportunité. Avec la chute du Mur de Berlin en 1989 et la disparition de la menace du communisme soviétique, de nouvelles menaces sont apparues. Plus précisément, des menaces déjà existantes ont été re-qualifiées en nouvelles menaces telles que le « crime organisé » ou « l'immigration illégale ». La fin de la menace soviétique a de plus atténué l'adhésion des gouvernements occidentaux au respect des normes démocratiques et des libertés civiles dans leur propre pays (à l'étranger, d'autres valeurs avaient cours comme par exemple le soutien de l'Occident aux régimes autoritaires à la condition qu'ils fussent anti-communistes).

Sur le front intérieur, « la loi et l'ordre » (et non les droits et les libertés civiles) devinrent une question politique (et électorale) dominante. Les nouvelles « menaces » et la politique de « la loi et l'ordre » surgirent pour se poser contre les normes démocratiques et libérales qui avaient pourtant été mises en place à la fin des années 90 (les directives européennes étaient entrées en vigueur en 1995 et 1997).

A l'été 1993, le FBI a réuni plusieurs Etats membres de l'UE pour débattre de la question émergeante, non pas seulement de savoir comment surveiller les nouveaux moyens de télécommunication, mais comment les utiliser pour qu'ils soient profitables aux agences de sécurité concentrant le renseignement (en y incluant le « trawling »). Aussi bien les hauts fonctionnaires, que la police et les représentants des agences de sécurité intérieure ont dû faire face à deux problèmes. Le premier a été de savoir comment inciter les industries de la télécommunication à fabriquer de nouveaux matériels et logiciels qui permettent l'interception (dont l'interception en « temps réel » de plusieurs séries de communications se tenant entre deux pays ou

plus). Le second problème a été de s'assurer qu'ils disposaient bien du pouvoir juridique de procéder à des interceptions sans restriction (et pas uniquement avec des mandats individuels ou grâce à des autorisations judiciaires).

La rencontre de 1993 au Quartier général du FBI à Quantico fut appelée « Séminaire sur l'application du droit international des télécommunications » (ILETS) et se tient depuis lors tous les ans. En octobre 1994, le Congrès des Etats-Unis adopta un projet de loi inspiré par le FBI exposant les « exigences nécessaires pour les utilisateurs internationaux » (IURs ou *Requirements*) pour pouvoir procéder à des interceptions de télécommunications. On supposait par là que ces textes façonneraient les normes internationales applicables à la nouvelle génération de matériels et de logiciels. Devant le danger de se retrouver à la traîne des Etats-Unis, l'UE a adopté un texte le 17 janvier 1995, sans d'ailleurs consulter un seul Parlement (qu'il soit européen ou national), et sous la forme de ce que l'on appelle la « procédure écrite » (le texte, au lieu d'être formellement adopté par le Conseil des ministres, a simplement été mis en circulation et approuvé). Cette action de l'UE n'a été rendue publique qu'en novembre 1996 lorsqu'un *Memorandum of Understanding* a été soumis à la signature des pays hors Etats-Unis et Union européenne. Les adresses auxquelles les signatures devaient parvenir étaient soit le Conseil de l'Union européenne à Bruxelles, soit le FBI aux Etats-Unis, d'où le nom donné à l'initiative : « le système UE-FBI de surveillance des télécommunications ».

ENFOPOL 98

En septembre 1998, le groupe de travail sur la Coopération policière au sein de l'UE a débattu puis approuvé une nouvelle volée de *Requirements* afin de couvrir les communications satellites et Internet. Les résultats prirent le nom d'ENFOPOL 98 et furent connus du grand public grâce à des fuites largement diffusées sur Internet. La couverture médiatique qui suivit la découverte contraignit les autorités à mettre cette initiative au placard jusqu'en 2001. Lors du Conseil de l'Union européenne du mois de mai consacré à la Justice et aux Affaires intérieures, les ministres approuvèrent un rapport expliquant bien clairement les conséquences des *Requirements* au sein de l'UE ; car en effet, ce qui est à présent connu sous le nom d'ENFOPOL 29 de 2001 a en fait incorporé toute la substance de l'ENFOPOL 98 de 1998. Bien qu'il mette en place des mesures encadrant les interceptions (dont la surveillance en temps réel), ENFOPOL 29 est toujours limité

par la nécessité d'obtenir un ordre spécifique autorisant l'écoute sur un sujet précis.

Les fonctionnaires de la Commission en charge de la protection des données se prononcent contre les demandes

Les fonctionnaires de la Commission en charge de la protection des données étaient tout à fait conscients des exigences des agences de sécurité, formulées lors de forums internationaux comme dans le sous-groupe du G8 consacré au crime High-Tech afin que les données soient automatiquement conservées et que les agences de sécurité puissent les consulter pendant des mois, si ce n'est des années. Les exigences des agences de sécurité de l'UE sont présentées en détail dans un rapport envoyé par le NCIS (Service britannique du renseignement criminel) au Ministère de l'Intérieur en août 1999, détaillant les mesures envisagées dont, si nécessaire, la création d'un « site d'archivage de données ».

L'opposition formulée par les fonctionnaires de la Commission en charge de la protection des données à l'encontre des demandes des agences de sécurité de l'UE est soutenue par le groupe de travail de l'UE sur la protection des données et par la Commission européenne. Aussi, la seule route encore praticable pour les agences de sécurité était de passer par le Conseil de l'Union européenne.

La résistance des agences de sécurité

Le mouvement vers le Conseil a été amorcé par une proposition de la Commission européenne sur « le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques » (COM(2000)385 final, 12.7.2000). La proposition a pour intention de mettre à jour le droit communautaire par la directive 97/55/EC mais elle n'a pas « *l'intention d'apporter des changements substantiels à la directive existante* », mais plutôt vocation à « *mettre à jour les dispositions existantes* ». La proposition se construit ainsi à partir des principes de la directive de 1997 et de son fondement qui se trouve dans la directive européenne de 1995 sur la protection des données inscrite dans le droit communautaire.

La proposition a été soumise au Parlement européen au cours de l'été 2000, car elle doit selon le principe de codécision, obtenir l'accord non seulement du Conseil et de la Commission, mais aussi du Parlement. Les rapporteurs parlementaires ignoraient jusqu'en avril 2001 que le Conseil entendait non seulement adopter ENFOPOL 98 (aujourd'hui

ENFOPOL 29), mais débattait aussi d'un ensemble de projets de « Conclusions » appelant la Commission à amender la proposition ainsi que toutes les directives de l'UE existantes afin de satisfaire aux exigences des agences de sécurité de l'UE. De plus, il était entendu d'adopter un projet de « position commune » sur cette nouvelle proposition avant que cette dernière ne passe en première lecture devant le Parlement européen (appelées « lignes de conduite », elles ont été adoptées au Conseil sur les Télécommunications le 27 juin 2001).

Le changement proposé par le Conseil et apporté à l'initiative de la Commission semble mineur, mais il conférerait aux gouvernements de l'Union européenne et à leurs agences de sécurité tous les pouvoirs dont ils auraient besoin pour adopter des lois de mémorisation des données au niveau national (le dixième alinéa autoriserait « la conservation des échanges de données et de localisation de celles-ci pour une période limitée »).

Avant tout cela, c'est le 7 juin 2001 que le Président du Groupe de travail sur la protection des données s'était adressé aux trois institutions européennes, leur disant entre autres choses :

« *une conservation systématique et préventive des communications ou de tout autre moyen de transfert de données des citoyens de l'Union européenne minerait les droits fondamentaux à la vie privée, à la protection des données, à la liberté d'expression, à la liberté et à la présomption d'innocence. La société de l'information pourrait-elle encore se réclamer société démocratique en de telles circonstances ?* ».

Le 11 juillet 2001, le Comité des Droits et Libertés des Citoyens a adopté son rapport sur ladite proposition par 22 voix contre 12 (la plupart des Eurodéputés socialistes – PSE – votant contre). Ce rapport propose que l'alinéa 10 soit modifié afin de limiter la conservation de données à des cas individuels spécifiques (comme à présent) et déclare : « *la surveillance électronique à grande échelle, exploratoire ou générale, est prohibée* ». Ce rapport devait être soumis au Parlement européen lors de sa séance plénière au début du mois de septembre. Si ce rapport devait être adopté sans amendement (et nous n'en avons aucune garantie), alors le Conseil se trouverait en porte-à-faux avec le Parlement européen et la Commission européenne.

Fin de partie

La résolution de ce problème marquera profondément non seulement les lois de l'UE sur la protection des données et les pouvoirs des agences de sécurité, mais ce sera aussi un important moment pour la démocratie au sein de l'UE. Soit la seule et unique raison pour conserver des données se maintiendra, soit elle tombera, mais sur cette question il ne saurait y avoir de « dérobade » ou de « compromis » bruxellois.

Cette fin de partie présente un autre tour inattendu. Le rapport du NCIS envoyé au Ministère britannique de l'Intérieur en 1999, ne l'a pas seulement été au nom des agences de sécurité mais aussi des agences de renseignement comme le MI5, MI6 et GCHQ. Il se pourrait bien aussi que ces agences souhaitent bénéficier des nouvelles formes d'interception qui permettraient d'avoir un accès direct à la source et à la suite de cela à la surveillance de type *trawling.*Ainsi, certains commentateurs débattent, que le moment venu, Echelon puisse être supplanté par de nouvelles technologies de surveillance qui émergeront si les gouvernements de l'Union européenne (et les Etats-Unis) poursuivent leur chemin.

Dans le processus de globalisation, les exigences des lobbies surfant sur la vague « la loi et l'ordre », quand mises en balance avec les droits et la vie privée des citoyens, sont proches de l'emporter. Seule une forte résistance démocratique peut contrecarrer de telles perspectives mais ceci, en Europe, est rien moins que certain.

---

[1] . Traduction : Nicolas Wuest-Famôse. Tous les documents cités en référence et bien d'autres encore sont disponibles sur le site Internet Statewatch Observatory on Surveillance in Europe (S.O.S) : www.statewatch.org/soseurope.htm