Fred Giuliani

Big Brother is watching you

« Celui qui cède sa liberté pour gagner en sécurité, n'a droit ni à la liberté ni à la sécurité. »
Benjamin Franklin

Le 21 février 2006, le Conseil des ministres de l'Union européenne a donné son accord pour une nouvelle directive «sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication». Derrière ce titre barbare ne se cache rien d'autre qu'une surveillance générale des moyens de télécommunications des 450 millions de citoyens de l'Union européenne.

En effet, cette directive oblige les pays membres de l'Union européenne à éditer des lois forçant les fournisseurs de services de télécommunications (téléphone et Internet) à sauvegarder et à stocker les données de communication électroniques de tous leurs clients pendant une durée minimale de 12 mois, et ce sans soupçon concret.

Quelles données faut-il stocker?

Sans entrer dans le détail des données à stocker, la directive prévoit le stockage des données personnelles de l'expéditeur et du destinataire, la date exacte de la communication, la durée de la communication, la localisation géographique de l'expéditeur et du destinataire en cas d'appel par téléphone mobile et, bien sûr, les adresses IP utilisées (adresse unique que chaque ordinateur reçoit lors d'une connexion à Internet) en cas d'une communication par Internet. Le contenu des courriels ou des appels téléphoniques est exclu.

On peut se demander comment nous avons pu arriver à une surveillance étendue des moyens de communication modernes. La directive élucide cela. En effet, la lutte contre le terrorisme semble justifier ces mesures de surveillance. Le point 10 nous renseigne que «le Conseil a réaffirmé dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation des données concernant les télécommunications».

La législation luxembourgeoise dépasse le simple cadre du combat contre le terrorisme et autorise l'accès aux données de télécommunication dans des conditions bien moins restrictives.

L'histoire de la directive

Sur le plan européen, le stockage préventif des données de communication a été envisagé la première fois en 2002 par la présidence danoise. Cette dernière avait émis une proposition en la matière, sans cependant convaincre une majorité des ministres européens.

Après les attaques terroristes de Madrid du 11 mars 2004, le Conseil européen charge le Conseil des ministres de vérifier s'il y a un besoin en matière de surveillance des télécommunications au sens large.

Cette initiative est reprise par la France, l'Irlande, la Suède et le Royaume-Uni qui ont soumis une première proposition en avril 2004. Celle-ci prévoyait le stockage des données de communication pendant une période de 12 mois et autorisait un accès à ces informations aussi bien de manière préventive que pour la résolution d'un délit commis. Elle ne limitait plus le recours à ces informations pour des activités terroristes, mais prévoyait aussi l'accès à ces informations dans le cadre de délits mineurs, tels que l'échange illégal de chansons par Internet.

C'est à ce moment-là que le Parlement européen se mêle de l'affaire. Le bras de fer entre ces deux institutions est lancé. A deux reprises, le Parlement européen, sous l'égide de l'Allemand Alexander Alvaro, rejette les tentatives du Conseil des ministres.

A un certain moment, il semble que la directive soit retirée de la table, mais les attentats de Londres du 7 juillet 2005 et la présidence anglaise font resurgir ce dossier épineux. Le commissaire européen de la Justice, Franco Frattini, reprend le dossier et le soumet sous forme d'une proposition de directive au

Parlement européen. Cette proposition prévoit le stockage des données relatives à l'usage d'Internet pendant six mois et celles relatives aux communications téléphoniques pendant 12 mois. Chaque pays peut cependant opter pour l'allongement de ces durées de rétention. De nouveau, la proposition ne se limite pas à donner accès aux données enregistrées dans le cas d'actes terroristes ou de crimes graves.

Tel que prévu par les procédures européennes, le dossier est transmis pour première lecture au Parlement européen. Ce dernier établit sous l'égide de M. Alvaro environ 200 changements par rapport à la proposition de la Commission. Parmi les plus importants figurent ceux qui comptent notamment restreindre l'accès aux informations de télécommunication dans des cas de crime grave ainsi que la réduction des types de données à stocker.

A ce moment-là, la proposition de la Commission risque d'être rejetée lors de la première lecture au Parlement européen. Au secours de la directive vient alors le ministre de l'Intérieur anglais, Charles Clarke, qui négocie en secret avec les chefs des fractions du Parlement européen et réussit à les convaincre de la nécessité de cette directive pour combattre le terrorisme et soumet une nouvelle proposition qualifiée de compromis. Un autre allié inattendu se rallie à la cause des politiques, l'industrie du divertissement. Celle-ci avait fortement soutenu la directive par intérêt économique. Cette directive dite «anti-terroriste» pourrait aussi facilement servir à poursuivre le téléchargement illégal de musique par le biais d'Internet ou de bourses d'échange. Un accès illégal à la musique qui fait perdre des centaines de millions d'euros par an. Ainsi, le groupe de pression CMBA (Creative and Media Business Alliance), composé de sociétés telles que Sony, Disney, IFPI, MPA et Universal Music, s'était adressé aux parlementaires européens afin de les motiver à soutenir la directive et de l'étendre pour en faire un moyen de combat efficace contre la piraterie et la contrefaçon.

Le 14 décembre, le Parlement européen accepte à la majorité des voix la proposition de compromis. Cette même proposition est approuvée le 21 février 2006 par le Conseil des ministres. Les pays membres disposent jusqu'au 15 septembre 2007 pour traduire cette directive dans leurs lois nationales, mais cependant jusqu'au 15 mars 2009 pour les services liés à Internet (accès à Internet, courriel et téléphonie à travers Internet)[1].

La situation au Luxembourg

En tant que bon élève, le Luxembourg était précurseur en matière de surveillance et de traçage des télécommunications. En effet, la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques impose au fournisseur de service:

• de conserver les données relatives au trafic pendant une période de 12 mois,

• de conserver les données de localisation autres que les données relatives au trafic pendant une période de 12 mois,

et ce pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales. Ainsi, l'accès aux données n'est pas retreint aux crimes particulièrement graves tels que le terrorisme, mais s'applique à tous les cas où la loi prévoit une peine d'emprisonnement. La législation luxembourgeoise dépasse donc le simple cadre du combat contre le terrorisme et autorise l'accès aux données de télécommunication dans des conditions bien moins restrictives. Les conséquences d'une telle législation se sont fait sentir lors des perquisitions auprès de BCE (Broadcasting Center Europe), à savoir le fournisseur informatique de RTL dans le cadre de l'affaire Hotmail[2].

© ann.deveria

Le volet protection

Il faut replacer cette directive dans son contexte politique. En effet, elle prévoit une surveillance des moyens de télécommunication et des accès à Internet de tous les citoyens de l'Union européenne et ce sans soupçon précis, le tout au nom de la lutte contre le terrorisme.

Il faut donc se poser la question de savoir si cette directive pourra prévenir des attentats terroristes? En effet, au vu des moyens techniques existants et de la disposition des terroristes, il semble peu probable que cette directive puisse prévenir des attentats terroristes dans l'Union européenne. Les moyens de contournement sont faciles à mettre en œuvre et bien documentés sur Internet.

En ce qui concerne le téléphone, plusieurs moyens permettent à l'initiateur de l'appel et au destinataire de l'appel de rester anonyme. On n'a même pas besoin d'avoir recours à des technologies de pointe. Il suffit d'utiliser une cabine téléphonique publique, comme il en existe encore par milliers à travers le monde, pour échapper au retraçage des appels. Un autre «outil» sont les cartes prépayées. Dans de nombreux pays européens, l'acquisition d'une carte prépayée, comme la plupart des adolescents en utilisent, peut se faire sans identification de l'acheteur. Nouveaux sont les services de téléphonie par Internet, tel Skype, qui sont souvent anonymes dans la mesure où l'identité n'est pas vérifiée lors de l'ouverture d'un compte auprès du fournisseur.

Les possibilités de contournement de la directive en matière d'envoi et de réception de mails sont aussi multiples. L'expéditeur et le destinataire peuvent facilement ouvrir sous une fausse identité des boîtes e-mails gratuites comme Yahoo, GMail et Hotmail. Les fournisseurs qui ne sont pas dans l'Union européenne ne sont pas soumis à l'obligation de stockage, ce qui ne permet pas de retracer l'utilisateur d'un compte e-mail. Plus sophistiqués, mais à la portée de chaque utilisateur d'Internet, sont des systèmes qui servent à rendre anonyme l'expéditeur d'un mail (système de *remailer* ou recours à des *open relay server*). Toute personne qui le souhaite peut aussi crypter ses communications sur Internet par des programmes (Virtual Private Network).

En effet, au vu des moyens techniques existants et de la disposition des terroristes, il semble peu probable que cette directive [de l'UE] puisse prévenir des attentats terroristes dans l'Union européenne.

Pour l'accès à Internet, il existe des solutions gratuites et commerciales de systèmes d'anonymisation de l'utilisateur. Ces solutions permettent d'accéder à des sites web avec une adresse IP qui n'est pas la leur. De même, on peut utiliser des bornes Internet publiques disponibles dans des cafés Internet ou des institutions publiques comme le Biergerzentrum.

Les moyens techniques évoqués ci-dessus sont légaux et décrits en détail sur Internet (voir le site du Chaos Computer Club). Ils montrent que chaque utilisateur Internet bien informé, et certainement chaque terroriste qui le souhaite, peut facilement contourner l'efficacité des mécanismes de traçage imposés par la directive. Le doute est donc permis quant à la possibilité de prévention d'un quelconque attentat par la directive.

Heinz Kiefer, président de la European Confederation of Police, souligne dans ce contexte que «… it remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. The result would be a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them».

Cette directive engendre des coûts non négligeables. Le système de stockage des données de connexions téléphoniques, courriels et Internet engendrent des coûts énormes chez les fournisseurs de services de télécommunication. En effet, ce traçage nécessite l'adaptation des infrastructures existantes et l'acquisition de capacités de stockage gigantesques. Selon diverses estimations, le coût par abonné pourrait atteindre entre 2 et 8 euros par an. Les fournisseurs de services doivent évidemment répercuter ces coûts sur leurs abonnés. Par ailleurs, les instances policières devront exploiter ces données de manière intelligible, ce qui nécessite davantage de personnel et d'infrastructures techniques. Ces coûts pourraient être acceptables si on avait la conviction que le traçage des télécommunications était un moyen efficace pour lutter contre le terrorisme. Mais la directive ne permet pas de prévenir de manière efficace un attentat.

Alors pourquoi les gouvernements veulent-ils mettre en place un système de surveillance des moyens de télécommunication qui engendre des coûts non négligeables pour les citoyens de l'Union européenne?

Les raisons politiques derrière cette directive

Tous les attentats depuis le 11 septembre 2001 ont entraîné des législations dites «anti-terroristes» qui étaient, à peu d'exceptions prêt, inappropriées et inefficaces. Le dernier exemple est la base de données dite «anti-terroriste» que le gouvernement allemand voudrait mettre en place suite à la tentative d'attentat à la bombe sur des trains allemands en 2006. Ce que l'on dissimule cependant à la population, c'est qu'aucun des deux présumés terroristes n'aurait figuré dans cette base de données d'après les critères établis par le ministère de l'Intérieur. Chaque attentat engendre une phase d'attention accrue dans la population pour des sujets de sécurité. Comme dans le cas de la directive européenne sur le retraçage des communications électroniques, elle sert aux dirigeants politiques à montrer leur détermination dans la lutte contre le terrorisme. La question de savoir si ces mesures sont jugées efficaces paraît être secondaire.

Le volet économique

Parmi les gagnants d'une politique de retraçage des communications électroniques se trouve d'abord toute l'industrie de la sécurité. En effet, les fournisseurs de services de télécommunication doivent se procurer des solutions performantes de stockage et de traçage des données de communication. AOL Angleterre estime l'investissement initial à 45 millions d'euros et prévoit encore un même montant en matière de coût opérationnel. Le volume de données stockées au niveau européen équivaut à 1 000 CD par jour, soit 365 000 CD par an. A ceci s'ajoutent les coûts d'exploitation d'une telle masse de données.

On l'a déjà soulevé, un gagnant inattendu mais très puissant du retraçage des communications électroniques est l'industrie de la musique. En effet, les bourses d'échange sur Internet servent souvent à échanger de manière illégale des chansons et des films. Afin de pouvoir poursuivre en justice ces «criminels», il faut savoir identifier les utilisateurs sur Internet. Or ces données n'étaient souvent pas disponibles. La nouvelle directive oblige les fournisseurs à stocker l'adresse IP des abonnés et donc l'identification du «criminel» devient beaucoup plus facile. Ainsi, l'association IFPI (International Federation of the Phonographic Industry) a déjà fait entendre de vouloir disposer d'un accès aux données stockées par les fournisseurs de services Internet en cas de présomption d'une copie illégale d'une chanson sur Internet. De même, la Creative and Media Business Alliance (CMBA) réclame le droit d'utiliser ces informations pour les poursuites de violation des droits d'auteur.

Le traçage de tous les moyens de télécommunication modernes constitue une menace fondamentale pour la liberté démocratique.

Les impacts de la directive sur la démocratie

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales précise dans l'article 8 que «toute personne a droit au respect de sa vie privée et familiale, de son domicile et de **sa correspondance**». Il est douteux que le stockage à titre préventif et sans soupçon concret soit en accord avec l'esprit de cette convention.

Une étude européenne menée en 2003 sur la protection des données relève que 33% des Européens jugent que la surveillance des communications téléphoniques est inacceptable et menace les droits fondamentaux et les libertés individuelles. En plus, 40% des Européens jugent que seules les communications des individus soupçonnés de terrorisme devraient être surveillées. Ainsi, 73% des Européens s'expriment contre une surveillance générale des communications téléphoniques.

Même le contrôleur européen de la protection des données exprime ses critiques par rapport à la directive en mettant la Commission en garde contre les effets de cette directive sur les droits fondamentaux des citoyens.

Le traçage de tous les moyens de télécommunication modernes constitue une menace fondamentale pour la liberté démocratique. En effet, ce traçage permet une surveillance des milieux politiques et est proche des moyens mis à disposition des polices politiques dans les anciens régimes totalitaires communistes. On entend souvent des slogans du genre: celui qui n'a rien fait d'illégal n'a rien à craindre de cette surveillance. Or chacun a ses petits secrets qu'il ne souhaite pas partager, même s'il ne s'agit pas d'affaires illégales.

Il appartient à chacun d'évaluer s'il est prêt à céder une partie de sa liberté pour une sécurité perçue comme plus poussée. Il faut cependant se poser la question si le traçage préventif des moyens de télécommunication de tous les citoyens européens n'est pas complètement démesuré par rapport aux gains escomptés? Il est plus que douteux que les mesures énoncées dans cette directive puissent empêcher un quelconque attentat terroriste. En effet, le traçage peut être facilement contourné et semble être un outil peu approprié pour prévenir un quelconque attentat. A la limite, le traçage permettrait de reconstituer *a posteriori* le déroulement de l'attentat et d'identifier les coupables. Si on étend le champ d'application de la directive à la criminalité en général, il reste à démontrer qu'une surveillance accrue entraîne automatiquement plus de sécurité réelle. En effet, dans les pays totalitaires, le niveau de surveillance est très élevé, mais en général, le niveau de criminalité et de corruption aussi.

[1] Notons encore que l'Irlande a porté plainte contre cette directive devant la Cour de justice européenne. Un jugement est attendu pour le milieu de l'année 2008.

[2] Voir l'article de Lex Folscheid "Pressefreiheit (Made in Luxembourg)" dans forum *n° 254.*