PAGE RÉALISÉE AVEC ALAIN BENSOUSSAN, AVOCAT

La conservation des données de connexion

ANTITERRORISME. Opérateurs télécoms, fournisseurs d'accès et hébergeurs doivent pouvoir remettre aux autorités de police les données techniques de connexion concernant leurs abonnés. A charge pour eux, donc, de les conserver.

Une obligation légale. Le Conseil constitutionnel ayant validé le projet de loi relatif à la lutte contre le terrorisme[1], ce texte est en vigueur depuis le 23 janvier 2006[2]. Afin de *« prévenir »* les actes de terrorisme, la loi contraint les opérateurs de télécommunications à conserver les données de connexion de leurs abonnés, et à tenir celles-ci à la disposition des services de police ou de la gendarmerie nationale.

Ces dispositions ne concernent pas le contenu des conversations ou des courriels échangés. Par données de connexion, il faut comprendre uniquement les informations aidant à déterminer l'heure d'un appel ou l'envoi d'un message, à localiser un terminal, son émetteur et son destinataire, et à prendre connaissance de la durée des communications. Les services de police ou de gendarmerie sont susceptibles de les réclamer pour prévenir un attentat, agir le plus en amont possible et, au besoin, écarter d'éventuels soupçons.

Un décret d'application doit préciser la procédure de suivi des demandes d'accès, ainsi que les conditions et la durée de conservation des données transmises.

Les opérateurs télécoms et tous les fournisseurs d'accès sont concernés. La loi définit à cette occasion, la notion d'*« opérateur de communications électroniques »*, entendu comme toute *« entreprise offrant au public à titre professionnel une connexion permettant une communication en ligne »* par l'intermédiaire d'un accès au réseau, *« y compris à titre gratuit »*. Les fournisseurs d'accès à internet (FAI) sont ainsi assimilés explicitement aux opérateurs. De même que les cybercafés et les lieux publics qui offrent des connexions via des bornes d'accès sans fil (Wi-Fi) ou des postes en accès libre : hôtels, restaurants, aéroports, universités, mairies…

Un dispositif limité à la prévention du terrorisme. La nouvelle forme de réquisition judiciaire instituée par la loi du 23 janvier 2006 est strictement limitée à la prévention du terrorisme. Les réquisitions de données autorisées par les nouvelles dispositions ne peuvent avoir d'autre finalité que de préserver l'ordre public et prévenir les infractions, et non de les réprimer. Le Conseil constitutionnel a rappelé le principe de séparation des pouvoirs administratif et judiciaire en ce domaine. ●

[1] *Décision n° 2005-532 DC du 19 janvier 2006.*
[2] *Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme, JO du 24 janvier 2006.*

LES FAITS SAILLANTS

Les données techniques sont les seules visées

- Les dispositions de la nouvelle loi visent à faciliter la collecte et la vérification rapide de renseignements opérationnels par l'exploitation des données engendrées par les communications électroniques.
Le dispositif de réquisition des données s'inspire de celui applicable en matière d'interceptions de sécurité d'origine administrative (écoutes téléphoniques).

LA TENDANCE

La durée de conservation, un enjeu dans l'Union

- Les attentats survenus à Madrid et à Londres ont relancé le débat sur la durée de rétention des données techniques de connexion au sein de l'Union européenne. La France s'est s'engagée, au côté de la Suède, de l'Irlande et du Royaume-Uni, en faveur d'une durée de conservation de trois années, en dépit du coût de l'application de cette mesure (estimé à 175 millions d'euros), et de ses incidences incontestables sur la vie privée.

À RETENIR

- En attendant un décret d'application, c'est la loi pour la sécurité quotidienne (LSQ) du 15 novembre 2001 qui fixe, à un an au maximum, la durée de conservation des données. Au-delà, opérateurs télécoms et FAI sont tenus de les effacer ou de les rendre anonymes.
- La loi du 23 janvier 2006 prévoit que les *« surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs »* pour répondre à ces demandes feront l'objet d'une compensation financière.
- Difficile à déterminer pour les grands opérateurs, le surcoût découlant de l'application de la loi (s'il existe) risque de l'être encore plus pour des structures aussi petites qu'un cybercafé, par exemple, car le stockage des données techniques de trafic ne correspond pas directement à leur activité de fournisseur de services. Celles-ci doivent prévoir d'installer un système ad hoc, qui permettrait également de chiffrer les frais de traitement des données techniques de connexion.