PAGE RÉALISÉE AVEC ALAIN BENSOUSSAN, AVOCAT

Données de connexion : un an de sauvegarde

DÉCRET. Depuis le 26 mars, la loi impose aux opérateurs télécoms, fournisseurs d'accès à internet et professionnels assimilés de garder un an durant les données techniques des communications de leurs clients. Une lourde obligation.

Quelles sont les données concernées ? Attendu depuis quatre ans, le décret sur les données de connexion est paru au Journal Officiel du 26 mars 2006. Le 2006-358 fixe la nature et la durée de conservation des données de connexion selon l'activité des opérateurs et le type de communication. Objectif : répondre aux *« besoins de la recherche, de la constatation et de la poursuite des infractions »*.

Les opérateurs de communications électroniques devront conserver les informations autorisant l'identification de l'utilisateur; les données relatives aux terminaux de communication utilisés; les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication; les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs; et, enfin, les données aidant à l'identification du ou des destinataires de la communication.

Pour les activités de téléphonie, s'ajoutent à ces données celles susceptibles de déterminer l'origine et la localisation d'une communication. Ce sont, par exemple, les informations favorisant la localisation du possesseur d'un téléphone portable allumé. Pour les communications internet, l'obligation concerne les seules données de trafic (« logs de connexion ») qui fournissent l'heure et la durée d'une connexion au web, ainsi que le numéro de protocole internet utilisé (adresse IP). Les données portant sur le contenu des communications ne sont donc pas visées, notamment le contenu des courriers électroniques et les données de navigation (adresses des pages internet visitées).

Combien de temps ces données doivent-elles être conservées ? Les opérateurs de communications électroniques doivent les garder pendant un an à compter du jour de leur enregistrement. Cette durée vaut pour toutes les données, indépendamment de l'activité des opérateurs et de la nature des communications.

Qui paiera le coût de cette obligation ? Le principe est que les dépenses permettant les interceptions justifiées par les nécessités de la sécurité publique ne sauraient incomber directement aux opérateurs privés. Mais seuls sont compensés les *« surcoûts identifiables et spécifiques »* supportés par les opérateurs requis par les autorités judiciaires pour la fourniture de données relevant des catégories mentionnées au décret. La compensation financière s'effectuera selon les modalités définies par le pouvoir réglementaire, à savoir par un arrêté ministériel. ●

LES FAITS SAILLANTS

Une application immédiate

- Etendue par la loi du 23 janvier 2006 sur le cyberterrorisme à tous les fournisseurs d'accès et d'hébergement à internet, aux cybercafés et lieux publics proposant des liaisons via des bornes d'accès sans fil (Wi-Fi) ou des postes en accès libre (hôtels, universités, mairies...), la conservation des données est une obligation. Et elle s'applique sans période transitoire.

LA TENDANCE

Un texte contesté

- L'Association des fournisseurs d'accès et de services internet a annoncé un recours devant le Conseil d'Etat. Le décret ne tiendrait pas compte des réserves des commissions consultatives [*], serait contraire en certains points à la loi qu'il précise, et ne permettrait pas une *« juste rémunération »* du coût de l'obligation, principe reconnu par le Conseil constitutionnel.

(*) La Cnil, la CCRSCE (Commission consultative des réseaux et services de communications électroniques et la CSSPPCE (Commission supérieure du service public des postes et communications électroniques).

À RETENIR

- Les opérateurs de téléphonie et fournisseurs d'accès internet conservaient déjà de leur propre initiative certaines données. Ils pouvaient donc les transmettre, le cas échéant, à la justice. En revanche, les cybercafés et autres prestataires assimilés devront mettre en place des systèmes spécifiques.
- L'obligation de conservation cause peu de souci dans un système d'abonnement, le titulaire étant aisément identifiable. Quand l'utilisateur n'est pas identifié (bornes Wi-Fi, cybercafés...), la mise en œuvre risque de rencontrer des difficultés. Certaines catégories de données (en-tête de courriel, données de serveur proxy...) pourraient aussi poser problème.
- Le système à mettre en place doit collecter des données aujourd'hui non conservées, les stocker dans des conditions de sécurité et d'accessibilité adéquates, les traiter dans des délais compatibles avec les enquêtes judiciaires, et comptabiliser leurs frais de traitement.