



Par
Anne-Catherine
LORRAIN

Doctorante au CERDI
(Centre d'Études et de
Recherche en Droit de
l'Immatériel)

Université Paris XI



Par Garance
MATHIAS

Avocat à la Cour

Données de connexion : la publication du premier décret ou la première pierre d'un édifice encore inachevé

Au sein du dispositif législatif existant, la conservation des données relatives à une communication électronique est l'exception. L'effacement ou l'anonymisation des données de connexion (1) demeure le principe, auquel il ne peut être dérogé que sous certaines conditions.

La loi française a récemment intégré de nouvelles dispositions quant à l'exercice de ces conditions dans le décret n° 2006-358 adopté le 24 mars 2006.

RLDI 501

D. n° 2006-358, 24 mars 2006, JO 26 mars, p. 4609

Comme nous avons déjà eu l'occasion de l'écrire (2), les textes législatifs concernant la conservation des données de connexion sont nombreux. Depuis quelques mois, l'édifice législatif s'est vu rehaussé de quelques pierres supplémentaires – et non des moindres – tant au niveau européen que national.

Au niveau national. – La loi relative à la lutte contre le terrorisme a été définitivement adoptée (3), et surtout, le décret d'application de l'article L. 34-1 du Code des postes et communications électroniques (C. P et CE) (4), a enfin été adopté le 24 mars 2006 (5). En effet, l'obligation des opérateurs de communications électroniques de conserver certaines données de trafic de leurs abonnés – obligation posée à l'article L. 34-1 du Code des P et CE, initialement prévue par la loi sur la Sécurité Quotidienne du 15 novembre 2001 (6) dont le dispositif a été pérennisé par la loi du 18 mars 2003 sur la sécurité intérieure (7) – nécessitait des précisions quant aux catégories de données soumises à conservation ainsi qu'à leur durée de conservation.

Au niveau européen. – Sous l'impulsion du Conseil extraordinaire Justice et Affaires Intérieures et dans le cadre de la politique dite du « troisième pilier » (coopération policière et judiciaire en matière pénale), de nombreux travaux ont été effectués concer-

nant la rétention des données de connexion. C'est dans ce contexte que le projet de décision-cadre sur la rétention des données de trafic, présenté par le Conseil européen en 2004 (8) a été adopté par le Conseil JAI en octobre dernier. Le Contrôleur Européen de la Protection des Données (CEPD) (9) également donné ses observations sur cette décision-cadre afin d'assurer un renforcement mutuel entre le fonctionnement des services répressifs et l'adéquation protection des données personnelles. Les préconisations du CEPD sont les suivantes :

- les données de la police et du système judiciaire doivent être soumises aux règles de protection des données tant dans le cadre des échanges entre États membres qu'au sein de chaque État membre ;
- les données sur les différentes catégories de personnes (victimes, témoins, suspects, ...) doivent être traitées différemment et accompagnées de garanties ;
- préalablement au traitement des données, la qualité des données reçues d'un pays tiers doit être évaluées « *scrupuleusement en tenant compte du respect des droits de l'homme et des normes en matière de protection des données* ».

L'impulsion du Conseil Justice et Affaires Intérieures a été déterminante pour parvenir à l'adoption, dans les meilleurs délais, de la directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications >

(1) Les expressions « données relatives à une communication électronique », « données de trafic » ou « données de connexion » sont utilisées en tant que synonymes. (2) Données de connexion : état des lieux ou première tentative de démantèlement de la toile législative, RLDI 2005/12, n° 334, p. 48. (3) Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JO 24 janv., p. 1129. (4) Article L. 34-1 II du Code des Postes et des communications électroniques : « Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le V, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs ». (5) Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques, JO 26 mars, p. 4609. (6) Loi n° 2001-1062 du 15 novembre 2001 sur la sécurité quotidienne, JO 16 nov. (7) Loi n° 2003-23 du 18 mars 2003 sur la sécurité intérieure, JO 19 mars, p. 4761. (8) Projet de décision-cadre du Conseil sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme (Doc. CE n° 8958/04, 28 avr. 2004). (9) Voir le communiqué de presse du CEPD n° EDPS/05/8 du 19 décembre 2005 (<<http://europa.eu.int/rapid/pressReleasesAction.do?reference=EDPS/05/8&format=HTML&aged=0&language=FR&guiLanguage=en>>).

électroniques (10). Cette directive (11) dite du « premier pilier » (12) a pour principal objectif d'« harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public et aux réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite des infractions graves telles qu'elles sont définies par chaque État membre en droit interne » (13).

Quant au champ d'application de la directive, celui-ci exclut le contenu des communications électroniques mais couvre toutes « données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré » (14).

Les États membres ont jusqu'au 15 septembre 2007 pour transposer en droit interne la directive relative à la conservation des données de trafic. Chaque État membre peut néanmoins différer cette transposition jusqu'au 15 mars 2009. La France ne s'est pas manifestée pour le report de l'application de la directive (15).

Et pour cause : la France dispose déjà d'un dispositif législatif national relatif à la rétention des données de connexion, dont la publication du décret du 24 mars 2006 manifeste le développement continu.

Est-ce toutefois une raison suffisante pour affirmer que le dispositif législatif national est en parfaite conformité avec le texte de la directive ? La question mérite d'être soulevée.

Le décret du 24 mars 2006 est une pièce essentielle de l'édifice législatif français relatif à la conservation des données de connexion. Ce texte réglementaire apporte des précisions concernant les catégories de données pouvant être conservées et la durée de leur conservation (I). Le décret donne enfin substance au principe avancé par la loi de la compensation financière des opérateurs dans le cadre de telles procédures de conservation (II). Cependant, quelques questions restent dans l'ombre...

I. – PREMIÈRE RÉPONSE À LA QUESTION : « QUELLES DONNÉES CONSERVER ET POUR COMBIEN DE TEMPS ? »

Rappelons que la loi (C. P et CE, art. L. 34-1) prévoit la possibilité de déroger au principe général d'effacement des données relatives à une communication électronique dans trois hypothèses :

- les données utiles dans le cadre de la facturation et du paiement des prestations de communications électroniques ;
- les données utiles dans le cadre de la recherche ou de la poursuite d'une infraction ;

- les données utiles dans le cadre de la protection des systèmes d'information de l'opérateur de communication électronique.

La loi relative à la lutte contre le terrorisme (précitée) ajoute au Code des P et CE un nouvel article L. 34-1-1 qui octroie à des enquêteurs anti-terroristes individuellement désignés de la police et de la gendarmerie le droit d'obtenir, afin de prévenir les actes de terrorisme, et ce hors de toute procédure judiciaire, la transmission par les opérateurs de communications électroniques des données qu'ils conservent en application de l'article L. 34-1 du Code des P et CE.

L'article L. 34-1 du Code des P et CE laissant au pouvoir réglementaire le soin de déterminer la nature des données pouvant faire l'objet d'une procédure de rétention ainsi que la durée de leur conservation, le décret d'application était donc attendu avec impatience (16).

En revanche, la conservation des données de connexion par les fournisseurs d'hébergement attend ces mêmes précisions dans un décret ministériel qui n'a pas été adopté à ce jour, en application de la loi pour la confiance dans l'économie numérique (17).

A. – Les catégories de données pouvant être conservées

Le décret du 24 mars 2006 définit les données dites « de trafic » comme « les informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi ». Par l'utilisation du terme de « finalités », le législateur se plie au « principe de finalité », selon lequel la conservation des données doit demeurer l'exception au principe de protection des données, et qui doit ainsi être justifiée, proportionnée et limitée au but poursuivi. Quant à la « pertinence » des données

conservées, elle n'est précisée par le législateur qu'au travers une liste de catégories de données pouvant faire l'objet d'une procédure de conservation.

Les données pouvant être conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions sont :

- « les informations permettant d'identifier l'utilisateur » (nom, prénom, adresse, etc.) ;
- « les données relatives aux équipements terminaux de communication utilisés » (ceux des opérateurs de téléphonie et des fournisseurs d'accès) ;
- « les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication » (adresse IP, date et heure de connexion et de déconnexion) ;
- « les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs » ;

Les États membres ont jusqu'au 15 septembre 2007 pour transposer en droit interne la directive relative à la conservation des données de trafic.

(10) Directive n° 2006/24/CE du 15 mars 2006 du Parlement européen sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive n° 2002/58/CE, JOUE 13 avr., n° L 105, p. 54. La directive a été adoptée par le Conseil JAI le 21 février 2006. (11) Sur la distinction entre la décision-cadre et la directive relative à la rétention des données de trafic, voir notre précédent article, précité, p. 49. (12) En vertu du premier pilier, ou pilier « Communauté », la majorité des textes sont proposés par la Commission et adoptés par le Conseil et le Parlement européen. Les procédures intergouvernementales concernent notamment le troisième pilier. (13) Directive précitée, art. 1.1. (14) Directive précitée, art. 1.2. (15) À ce jour, plusieurs États membres ont fait une déclaration leur réservant le droit de différer l'application de la directive relative à la conservation de données de trafic : Pays-Bas, Autriche, Royaume-Uni, Estonie, Chypre, Grèce, Luxembourg, Slovaquie, Suède, Lituanie, Lettonie, République tchèque, Belgique, Pologne, Finlande, Allemagne (<<http://www.europarl.europa.eu/oeil/file.jsp?id=5275032¬iceType=null&language=fr>>). (16) Le décret du 24 mars 2006 (précité) introduit les articles R.10-12 à R10-14 au sein de la partie réglementaire du Code des P et CE. (17) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO, 22 juin, p. 11168, article 6, II.

– « les données permettant d'identifier le ou les destinataires de la communication ». Il s'agit, par exemple, de l'adresse IP du destinataire d'un courrier électronique. Toutefois, il est permis de s'interroger sur la possibilité de conservation des adresses URL des sites visités, ce que le décret ne précise pas...

Cette liste correspond aux données envisagées par la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (18). Les catégories de données énumérées par le décret forment toutefois une liste assez sommaire. Sous couvert de l'exception au principe de protection des données, et d'une liste de conditions de dérogation au principe devant être limitative et exhaustive, le caractère ouvert d'une telle liste risque de réduire le principe à peau de chagrin...

Le décret est d'ailleurs moins prolixe que la directive du 15 mars 2006, qui décrit de façon plus détaillée les catégories de données pouvant faire l'objet d'une mesure de conservation (19), tant concernant la téléphonie fixe et mobile que l'Internet (accès, courrier, téléphonie). Ces données doivent être utiles pour :

- retrouver ou identifier la source d'une communication ;
- identifier la destination d'une communication ;
- déterminer la date, l'heure et la durée d'une communication ;
- déterminer le type de communication ;
- identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ;
- localiser le matériel de communication mobile.

Dans le doute, les fournisseurs d'accès français pourront toujours se référer au texte communautaire... à moins qu'ils ne préfèrent de toute façon viser large, et conserver toutes les données permettant de répondre aux objectifs cités par le décret.

Par ailleurs, pour la sécurité des réseaux et des installations, les opérateurs ne peuvent conserver que les données suivantes :

- « les données permettant d'identifier l'origine de la communication » ;
- « les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication » ;
- « les données à caractère technique permettant d'identifier le ou les destinataires de la communication » ;
- « les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ».

B. – La durée de conservation des données

Le décret a opté pour la durée de conservation maximale d'un an à compter du jour de l'enregistrement des données (20). Ce délai concerne les données conservées pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ainsi que les données nécessaires au paiement et à la facturation des services rendus.

Toutefois, par exception, les données conservées pour la sécurité des réseaux et des installations peuvent être conser-

vées pour une durée n'excédant pas trois mois. Cette dichotomie dans les durées, nullement préconisée par la directive européenne du 15 mars 2006 (précitée), risque cependant de créer un certain imbroglio pour les professionnels des communications électroniques.

La durée de conservation d'un an s'inscrit dans les limites posées par la directive du 15 mars 2006, qui prévoit une durée de conservation minimale de six mois et maximale de deux ans à compter de la date de la communication des données (21). La directive préconise en effet une conservation

pendant deux ans des données en matière de terrorisme et de crime organisé (22).

Faut-il déduire de ce texte que les opérateurs français devront stocker les données de trafic pendant deux ans, faute de pouvoir déterminer *a priori* si les données collectées se rapportent au terrorisme ou à une enquête pénale « classique » ?

La menace terroriste étant de plus en plus citée à l'appui des initiatives des législateurs national et communautaire – comme l'illustre la loi relative à la lutte contre le terrorisme (précitée) et la directive du 15 mars 2006 (précitée) –, faut-il prévoir une augmentation du nombre des enquêtes « anti-terroristes » ?

Dans l'affirmative, faut-il présager de l'augmentation du nombre des procédures d'enquête et de conservation des données exorbitant du droit commun ?

Ne sera-t-il pas plus « simple » et pragmatique pour les enquêteurs de se référer au droit européen plutôt qu'à la loi française, et d'exiger ainsi une durée de conservation des données de deux ans ?

La liste des catégories de données soumises à conservation et la durée de leur conservation ne risquent-elles pas ainsi de s'allonger, au péril de la sauvegarde du principe de la protection des données à caractère personnel... et à quels frais pour les opérateurs zélés ou soumis aux contraintes des enquêteurs ?

II. – PREMIÈRE RÉPONSE À LA QUESTION : « COMMENT ASSURER CONCRÈTEMENT LA COMPENSATION FINANCIÈRE DES OPÉRATEURS ? »

Le décret du 24 mars 2006 détermine les modalités de compensation financière des opérateurs, en application de l'article L. 34-1 du Code des P et CE.

La tarification applicable selon les catégories de données et les prestations requises seront déterminées par arrêté du ministre de l'Économie, des Finances et de l'Industrie et du Garde des sceaux. En pratique, certains opérateurs adressent d'ores et déjà des factures détaillant le coût de la recherche et de la conservation des données sollicitées dans le cadre d'une procédure pénale (instruction, enquête).

Le décret ne fait que préciser que ce futur arrêté distinguera les tarifs applicables « en tenant compte, le cas échéant, des surcoûts identifiables et spécifiques supportés par les opérateurs » ➤

*Le décret a opté pour
la durée de conservation
maximale d'un an
à compter du jour
de l'enregistrement
des données.*

(18) Article 1 d). (19) Dir. n° 2006/24/CE, 15 mars 2006, art. 5. (20) C. P et CE, art. L. 34-1. (21) Dir. 15 mars 2006, précitée, art. 7. (22) Dir. 15 mars 2006, précitée, considérant (9) : « (...) Étant donné que la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive. L'adoption d'un instrument relatif à la conservation des données constitue dès lors une mesure nécessaire au regard des exigences de l'article 8 de la CEDH ». Sur la question de la compatibilité de la conservation des données et le respect de l'article 8 de la Convention européenne des droits de l'homme, voir notre article précité, p. 51 et s.

requis par les autorités judiciaires pour la fourniture de ces données » (article 3 du décret, modifiant l'article R. 213-1 du Code de procédure pénale).

Les opérateurs ont leur mot à dire sur la mise en place d'une telle tarification, eux-seuls étant en mesure d'estimer les coûts réellement engendrés par une procédure de conservation de données (23). Le Gouvernement ne saurait ignorer la demande de participation des opérateurs à l'élaboration du prochain arrêté ministériel sur cette question de leur compensation financière.

Pour résumer la teneur du dispositif législatif, l'exception tend à devenir le principe !

Le décret du 24 mars 2006, s'il apporte des précisions essentielles à la mise en œuvre des procédures de conservation des données de connexion, demeure toutefois assez flou, ce qui ne sert malheureusement pas la nécessité d'encadrement de toute exception au principe de protection des données à caractère personnel.

Face à la montée des arguments dits « *sécuritaires* » du législateur, le décret du 24 mars 2006 n'est qu'une première étape d'un dispositif qui doit garantir le respect de la vie privée et les principes fondamentaux de la protection des données. ♦

(23) D'après l'AFA (Association des Fournisseurs d'Accès), l'indemnisation prévue par le gouvernement devrait s'élever à 20 euros pour chaque demande de fourniture de données techniques et à 3,80 euros pour les informations contractuelles. L'AFA estime que cette tarification est inacceptable et envisage une action devant le Conseil d'État si ces chiffres devaient être confirmés dans le futur arrêté.