

Pour les autorités judiciaires, l'exploitation des données de communications téléphoniques et de connexions au réseau internet est fondamentale afin de lutter contre le terrorisme et la grande criminalité.

Ces informations existent et ont été constituées, notamment par les opérateurs de télécommunications pour leurs propres besoins, tant commerciaux que financiers.

Alors que le projet de loi relatif à la lutte contre le terrorisme vient d'être adopté par l'Assemblée nationale (1), l'enjeu du contrôle des communications, notamment électroniques, et plus particulièrement des données de connexion, est au cœur de l'actualité. Le débat est donc ouvert.

Données de connexion : un état des lieux ou une première tentative de démêlage de la toile législative



Par Garance
MATHIAS
Avocate à la Cour



Par Anne-Catherine
LORRAIN
Doctorante
au Centre d'Études
et de Recherche du Droit
de l'Immatériel (CERDI)
Université Paris XI

Les questions posées sont les suivantes. Face à la menace terroriste et aux impératifs étatiques de sécurité, doit-on sacrifier le respect de la vie privée (2) ? Comment adapter au secteur des communications électroniques l'équilibre posé par la loi du 6 janvier 1978 (3) et la directive de 1995 (4) entre le principe de protection des données à caractère personnel et la légitimité de leur traitement à des fins de sécurité ou de poursuite judiciaire ?

Quelles sont les données de connexion ? Peuvent-elles être utilisées à des fins radicalement différentes de celles pour lesquelles elles sont collectées initialement (à titre commercial ou financier), si légitimes soient-elles ? À quelles conditions ? Pendant quelle durée ? À quel coût ?

Quelle est la position de l'Union européenne sur la question du traitement des données de connexion ? Existe-t-il une possible harmonisation entre les États membres ?

Tentons tout d'abord de définir la notion hétérogène de données de connexion, dont il n'existe pas de définition juridique précise.

Les données de connexion, de manière générale, sont les informations produites ou nécessitées par l'utilisation des réseaux de communications électroniques, qu'il s'agisse des communications téléphoniques ou des connexions au réseau internet (données de trafic, de localisation, de facturation, etc.).

Les opérateurs (5) disposent ainsi de deux catégories de données se rapportant aux utilisateurs de leurs réseaux : celles, administratives, relatives à leurs clients qu'ils traitent dans le cadre général de leur relation commerciale (les nom, prénom, adresse, mode de paiement de l'abonnement, etc.) et celles, techniques, relatives aux communications émises par leurs clients sur leurs réseaux (numéros de téléphone appelant et appelé, date et durée de l'appel ou de la connexion, identifiant de l'appareil utilisé par leurs clients, etc.).

Dans cette logique, le projet de loi relatif (6) à la lutte contre le terrorisme définit son champ d'application par une formule qui se veut précise et exhaustive : « les données (...) sont limitées aux données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques

relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date de la communication ».

De son côté, le droit communautaire offre une définition extensive des données de connexion. En effet, la directive dite « vie privée et communications électroniques » du 12 juillet 2002 (7) parle de « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » (8).

Face à la diversité des législations nationales relatives au traitement des données de connexion, dont les textes se sont multipliés pour les besoins de la lutte contre le terrorisme, une harmonisation s'impose entre les États membres de l'Union européenne.

C'est dans cette logique que la Commission européenne a récemment présenté une proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques (9).

Des considérations d'ordre économique sous-tendent également cette proposition de directive. L'insécurité juridique causée par les disparités législatives des États membres fait supporter aux opérateurs un coût financier et une certaine insécurité économique, ce qui est de mauvais augure au sein d'un marché qui se veut « unique » et où doit prospérer la libre circulation des services. Par ce texte, l'Union européenne manifeste ainsi l'intention de remédier à cette situation.

Avant d'aborder les enjeux juridico-économiques liés au traitement des données de connexion, un bref historique des législations nationale et européenne s'impose.

ÉTAT DES LIEUX DU CADRE LÉGISLATIF EUROPÉEN ET NATIONAL

Le cadre législatif communautaire

L'Union européenne a appréhendé les données de connexion dans le cadre de plusieurs textes, et ce préalablement à la récente proposition de directive (10).

Ainsi, le Conseil européen a présenté un projet de décision-cadre sur la rétention des données de trafic le 28 avril 2004 (11). Cette décision-cadre a été adoptée par le Conseil extraordinaire Justice et Affaires Intérieures (JAI) en octobre dernier, en dépit de son rejet par le Parlement européen en juin 2004 et d'un avis défavorable du Groupe « Article 29 » en novembre 2004 (12). La décision-cadre a également provoqué quelques réserves en France, notamment par le Sénat (13), particulièrement en ce qui concerne la durée de conservation des données.

Alors que cette décision-cadre vient d'être adoptée, la proposition de directive traduit explicitement la volonté de l'Union de faire passer la question de la rétention des données de connexion au sein des compétences du premier pilier, et non plus au sein de celles du troisième pilier (14). Précisions que l'organisation au sein du troisième pilier ne permet qu'une prise de décision par les membres du Conseil européen dans les domaines de justice et de police, alors que le premier pilier concerne les directives et la co-décision, impliquant tous les organes décisionnels communautaires.

En d'autres termes, la question de la conservation des données est estimée – à juste titre – suffisamment importante pour que les autorités européennes, et notamment le Parlement, aient un droit de regard accru.

L'objectif de la proposition de directive n'est pas de redéfinir les principes de protection des données à caractère personnel dans le cadre des communications électroniques, qui sont déjà posés par la directive du 12 juillet 2002 (15) et que la proposition ne fait que rappeler. L'objectif est d'encadrer les conditions d'exercice de l'obligation de traitement des données à caractère personnel imposée aux opérateurs, tout particulièrement dans le cadre des poursuites judiciaires.

La Commission résume l'esprit du texte en ces termes : la proposition de direc-

tive a pour but d'harmoniser les obligations, pour les opérateurs de services de communications électroniques, de conserver certaines données relatives au trafic, de sorte qu'elles puissent être transmises aux autorités compétentes des États membres en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions graves, comme les actes terroristes et la criminalité organisée (16). La proposition vise à garantir que les données relatives au trafic seront conservées à travers l'Union européenne et pourront être mises à la disposition des autorités compétentes dans les mêmes conditions, tout en recherchant à faciliter la standardisation des technologies pour les opérateurs.

Au regard de ces textes européens, les données de connexion sont assimilées à des données à caractère personnel, ainsi soumises au régime de protection issu

La question de la conservation des données est estimée – à juste titre – suffisamment importante pour que les autorités européennes, et notamment le Parlement, aient un droit de regard accru.

de la directive de 1995 (17). La directive « *vie privée et communications électroniques* » (18) qui adapte ce régime aux communications électroniques, distingue arbitrairement deux types de données, à savoir :

- les données relatives au trafic (19), définies comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* » ;
- les données de localisation (20), définies comme « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

Cette distinction est purement théorique. Par ailleurs, la directive « *vie privée et communications électroniques* » dispose que les utilisateurs doivent garder la possibilité d'interdire « *temporairement, par un moyen simple et gratuit* », le traitement de leurs données de localisation « *pour chaque connexion au réseau ou*

pour chaque transmission de communication » (21). Or nul ne peut envisager comment prendre en compte en pratique, sans un coût financier et technique conséquent, cette possibilité laissée aux usagers d'interdire le traitement de ces données.

Compte tenu des impératifs renforcés de sécurité liés aux menaces terroristes, la proposition de directive possède un champ d'application élargi visant indistinctement « *les communications qui génèrent des données relatives au trafic, les données de localisation ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur* » (22).

La proposition de directive liste dans son article 4 les catégories de données à conserver par les opérateurs. Celles-ci comprennent les données les données nécessaires pour :

- retrouver et identifier la source d'une communication ;
- retrouver et identifier la destination d'une communication ;
- déterminer la date, l'heure et la durée d'une communication ;
- déterminer le type de communication ;
- déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication ;
- localiser le matériel de communication mobile.

Les types de données à conserver pour chacune des catégories de données susmentionnées sont précisés en annexe, comme notamment dans le cadre du courrier électronique, l'adresse IP (Internet Protocol), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès internet, le code d'identification personnel de la source de communication, etc.

La vocation sous-jacente de la proposition de directive est de tenter de rassurer les opérateurs au regard de leurs préoccupations économiques. L'obligation donnée aux États membres de rembourser aux opérateurs les surcoûts qu'ils justifient avoir supportés en est une illustration (23). Cependant, comme nous le verrons plus loin, les modalités d'exercice de l'obligation de conservation des données ne laissent pas présager de sinécure pour les opérateurs...

La proposition de directive se fait l'écho d'une tendance sécuritaire liée aux menaces terroristes, qui s'est généralisée pour tous les États membres. Elle en est même l'aboutissement, dans la mesure où pour la première fois, le législateur communautaire parle très clairement d'« *obligation* » de conservation des données (24).

>

La France s'inscrit, à l'instar de ses voisins européens, dans cette tendance de sécurité nationale. Cependant, avant de prendre en compte les besoins spécifiques de la lutte contre le terrorisme, le système de conservation des données du législateur français a emprunté un chemin éclairé par le droit communautaire.

Le cadre législatif national

Le projet de loi relatif à la lutte contre le terrorisme (25) fait suite à de nombreux textes législatifs traitant de la question de la rétention des données de connexion. La loi sur la sécurité quotidienne du 15 novembre 2001 (26) a soumis les opérateurs à l'obligation de conserver les données de leurs abonnés (article 29, devenu article L. 34-1 du Code des postes et communications électroniques après modification par loi du 9 juillet 2004 sur les communications électroniques) (27). Ce dispositif de conservation des données n'ayant été adopté que pour une durée limitée (jusqu'au 31 décembre 2003), il a été pérennisé par la loi du 18 mars 2003 sur la sécurité intérieure (28).

Un décret devait être pris en application de l'article L. 34-1 du Code des postes et communications électroniques afin de préciser les catégories de données soumises à conservation ainsi que leur durée de conservation. Malgré l'élaboration d'un projet de décret soumis à l'avis de la Commission nationale informatique et libertés (CNIL) (29), aucun décret n'a vu le jour, son adoption faisant l'objet d'un fort lobbying de la part des opérateurs. Ce dispositif de conservation a été prévu dès 2001 par le projet de loi sur la société de l'information, qui n'a cependant jamais été examiné par le Parlement mais sur lequel la CNIL a été consultée (30). Cet avis a été l'occasion pour la CNIL de souligner « *le caractère inédit* » du dispositif retenu, dérogeant au principe de finalité du traitement des données. Le dispositif donne en effet l'obligation aux opérateurs de communications électroniques de conserver, aux fins exclusives de faciliter le travail des autorités policières et judiciaires, des données qui se rapportent à l'ensemble des personnes utilisant leurs services et dont la conservation ne présente aucune utilité pour eux.

Le dispositif de la loi sur la sécurité quotidienne a donné suite à d'autres textes législatifs dont l'objet était de préciser ses conditions d'application. Ainsi, un rapport annexé à la loi d'orientation et de programmation de la sécurité intérieure de 2002 (LOPSI) (31) incite à l'élaboration d'un texte permettant aux autorités judiciaires d'accéder directement et à dis-

tance aux données de connexion conservées. Également en 2002, la loi de finances rectificative pour 2001 a autorisé les agents fiscaux, douaniers et enquêteurs de la Commission des opérations de bourse (COB) à collecter les données de connexion conservées par les opérateurs de télécommunications, les fournisseurs d'accès et les hébergeurs (32).

Les données de connexion concentrent toutes les interrogations autour de la question cruciale de leur conservation.

L'activité législative française ne s'est pourtant pas arrêtée là. La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, dite loi « *Perben II* » (33), prévoit notamment un droit pour les officiers de police judiciaire de se faire communiquer des documents dans le cadre d'une enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives (34).

Par la suite, la loi du 9 juillet 2004 relative aux communications électroniques (35) (modifiant les articles L. 34-1 et suivants du Code des postes et des communications électroniques) et la loi du 6 août 2004 (36) ont opéré la transposition de la directive de « *vie privée et communications électroniques* » (37), parachevant ainsi le dispositif législatif de conservation des données de connexion. Selon le nouvel article L. 34-1, les opérateurs de communications électroniques et fournisseurs d'accès internet doivent effacer ou rendre anonyme toute donnée relative au trafic. Mais par exception, dans des circonstances relevant notamment d'une action pénale, il peut être différé aux opérations tendant à effacer ou à rendre anonymes ces données techniques.

Alors que l'article L. 34-1 du Code des postes et des communications électroniques met l'obligation de conservation des données à la charge des opérateurs de communications électroniques, la loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN) instaure la même obligation aux hébergeurs internet (38). Cette distinction n'est pas neutre dans la mesure où ces dispositions légales doivent, pour chacune d'entre elles, être précisées par un décret en Conseil d'État précisant notamment la nature et la durée de conserva-

tion des données devant être conservées, qui peuvent donc être différentes.

Ainsi, malgré l'existence d'un cadre législatif, aucune règle d'application n'est posée sur les catégories de données concernées, sur la durée de leur conservation, sur la nature des communications à surveiller, ni sur les modalités d'action des opérateurs, y compris financière (surcoûts, modalités de compensation, etc.) (39).

Ce « *patchwork* » législatif, tant au niveau européen que national, a pour principal inconvénient de ne pas offrir de sécurité juridique suffisante. Les garanties offertes ne sont satisfaisantes ni pour les citoyens, dont le respect de la vie privée souffre des exceptions aux contours incertains, ni aux opérateurs, qui supportent une obligation leur faisant courir des risques supplémentaires, notamment financiers.

C'est l'équilibre entre tous ces intérêts qui doit être recherché par la loi. Cet équilibre peut-il être atteint ? Une fois la dérogation au principe de protection des données acceptée, dans un contexte légitime de sécurité (I), la pérennité du système réside dans les modalités d'encadrement de cette dérogation, tolérables par toutes les personnes concernées, internautes et opérateurs (II).

I. – L'OBLIGATION DE CONSERVATION DES DONNÉES DE CONNEXION

Les données de connexion concentrent toutes les interrogations autour de la question cruciale de leur conservation. Préalablement à l'étude de l'étendue du champ d'application de cette conservation (B), il convient d'en exposer les principes (A).

A. – Un régime dérogatoire au droit commun sur la protection des données à caractère personnel

Comment s'assurer que la conservation des données ne s'inscrit pas dans ce que certains qualifient de « *dérive sécuritaire* » (40) ? Les textes de loi, qui prennent en compte la possibilité d'exceptions au principe de la protection des données à caractère personnel, fournissent une première réponse à cette interrogation.

1. De la possibilité à l'obligation de déroger au principe de non-conservation des données à caractère personnel

La directive de 1995 (41) pose les principes directeurs de la protection des données à caractère personnel. Parmi ces

principes, celui de la confidentialité (effacement et anonymisation) des données est repris par tous les textes ultérieurs, dont ceux régissant les communications électroniques [notamment par la directive « *vie privée et communications électroniques* » (42), transposée en droit français par la loi du 9 juillet 2004 (43)].

De façon plus générale, l'article 8 de la Convention européenne des droits de l'Homme affirme le respect de la correspondance et de la vie privée de chaque personne (44). Ce principe trouve son écho dans l'article 9 du Code civil français, qui établit également le principe du respect de la vie privée.

Ainsi, la loi du 10 juillet 1991 (45) qui garantit le secret des correspondances privées émises par voie de télécommunications, s'applique au courrier électronique selon une jurisprudence constante (46). La loi de 1991 n'autorise l'interception des correspondances privées émises par voie de télécommunications que sous le contrôle du juge. Les autorités judiciaires ont sollicité ces mesures en rappelant leur besoin d'outils pour lutter non seulement contre la cybercriminalité, mais aussi contre la criminalité traditionnelle utilisant l'internet comme un simple moyen de communication.

La directive « *vie privée et communications électroniques* » et l'article L 34-1 du Code des postes et des communications électroniques posent un principe d'effacement ou d'anonymisation des données relatives à une communication électronique. Il existe trois possibilités de dérogation au principe général d'effacement, qui sont strictement encadrées :

- les opérateurs peuvent utiliser, conserver et le cas échéant transmettre à des tiers concernés les données relatives au trafic pour les besoins de la facturation et du paiement des prestations de communications électroniques, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement soit au maximum ;
- les opérateurs peuvent conserver certaines données en vue d'assurer la sécurité de leurs réseaux ;
- l'effacement des données relatives au trafic peut être différé pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et seulement afin de mettre ces données à disposition de l'autorité judiciaire.

Toutefois, les fins de facturation et de poursuite judiciaire n'ont pas les mêmes implications pour les opérateurs. En effet, les premières mettent en œuvre des don-

nées administratives, conservées par les opérateurs dans le cadre de leur activité professionnelle et incluses dans les contrats conclus avec les abonnés à leur service, tandis que les secondes ne sont d'aucune utilité pour les opérateurs.

Les autorités compétentes peuvent solliciter les opérateurs à tout moment afin d'obtenir les données nécessaires à la recherche d'infractions pénales. Dans l'éventualité d'une telle demande, les opérateurs se voient donc contraints de conserver des données que leur activité n'aurait pas amené à traiter. Ainsi, la loi ne se contente plus d'exposer les exceptions possibles au principe de protection des données, mais instaure une véritable exception obligatoire à ce principe. Si la loi ne le dit pas expressément, la proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques (47) saute le pas, en parlant bel et bien d'« *obligation de conservation des données* » (48).

La responsabilité ainsi attribuée aux opérateurs les amène à jouer le rôle d'auxiliaire de justice (49). Dans le cadre d'une procédure judiciaire, les données de connexion sont en effet un élément de preuve important concourant à la manifestation de la vérité. Or, il convient de ne pas perdre de vue que les opérateurs, acteurs de l'économie, ne font pas l'objet de procédure d'agrément judiciaire ni de formation spécifique liées à la recherche, à la constatation et à la poursuite d'infractions pénales.

**Dans le cadre
d'une procédure
judiciaire, les données
de connexion sont
un élément de preuve
important concourant
à la manifestation
de la vérité.**

Faire supporter aux opérateurs l'obligation de fournir des preuves informatiques aux autorités judiciaires est une responsabilité lourde de conséquences dans le cadre de l'aboutissement d'une procédure pénale. Ceci mérite la plus grande attention du législateur.

Par ailleurs, la collecte et le stockage des données de connexion font supporter aux opérateurs, en plus des contraintes techniques, un coût économique qui n'est pas pris en compte par les autorités à ce jour.

2. La conservation des données de connexion à des fins de poursuite des infractions pénales : l'exemple de la contrefaçon

Dans sa version originelle datant de 1978, la loi « *Informatique et libertés* » (50) ne permettait le traitement des données personnelles relatives aux infractions, condamnations et mesures de sûreté que par :

« 1° *Les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;*
2° *Les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ; (...)* ».

Les échanges de contenus protégés par le droit de la propriété intellectuelle s'étant particulièrement développés sur internet, les sociétés de perception et de répartition des droits d'auteur et droits voisins ont été tentées d'adapter leurs moyens de lutte contre la contrefaçon par la mise en place d'outils logiciels permettant de détecter les actes de contrefaçon en ligne, notamment sur les réseaux « *peer to peer* ». Malgré un premier revers subi en 2001 par la SACEM et la SDRM, qui se sont vu interdire par la CNIL l'utilisation d'un tel outil logiciel (dénommé « *Webcontrol24* ») (51), la préoccupation des défenseurs des droits d'auteur et droits voisins a été entendue.

En effet, la loi du 6 août 2004 (52) ajoute au texte de 1978 une nouvelle catégorie de personnes habilitées au traitement des données relatives aux infractions : « *Les personnes morales mentionnées aux articles L. 321-1 et L. 331-1 du Code de la propriété intellectuelle, agissant au titre des droits dont elles assurent la gestion ou pour le compte des victimes d'atteintes aux droits prévus aux livres I^{er}, II et III du même Code aux fins d'assurer la défense de ces droits* » (article 9 4°) (53). La loi vise ici les sociétés de perception et de répartition des droits d'auteur et droits voisins ainsi que les organismes professionnels défendant ces droits.

Le Conseil constitutionnel a validé la constitutionnalité de cette disposition (54), sous réserve que les données collectées ne puissent acquérir un caractère nominatif que dans le cadre d'une procédure judiciaire et qu'un tel traitement de données concernant les infractions soit subordonné à un régime d'autorisation de la CNIL.

C'est sur cette disposition de la loi du 6 août 2004 que le Syndicat des Éditeurs de Logiciels de Loisirs (SELL) a mis en place un système consistant à envoyer des messages d'avertissement (indiquant la protection par le droit d'auteur des logiciels concernés et les sanctions encourues en cas de leur violation) aux personnes

mettant à disposition ou téléchargeant illégalement sur internet des logiciels appartenant au catalogue du SELL. Le système, qui donnait également la possibilité de dresser des procès-verbaux à l'encontre des prétendus contrefacteurs, a été autorisé par la CNIL le 11 avril 2005 (55).

Plus récemment, la Société des Auteurs, Compositeurs et Éditeurs de Musique (SACEM), la Société pour l'administration du Droit de Reproduction Mécanique (SDRM), la Société Civile des Producteurs Phonographiques (SCPP) et la Société civile des Producteurs de Phonogrammes en France (SPPF) ont souhaité mettre en œuvre un procédé de repérage et d'avertissement des internautes soupçonnés d'échanger illégalement des fichiers musicaux sur internet. La CNIL a refusé d'autoriser un tel mécanisme dans une décision du 18 octobre dernier (56).

Contrairement au procédé proposé par le SELL, la Commission a estimé que les garanties offertes par le système de traitement n'étaient pas suffisantes. La transmission des messages d'avertissement avait pour particularité de passer par l'intermédiaire des fournisseurs d'accès internet, qui étaient chargés d'envoyer les messages à leurs abonnés après les avoir identifiés par corrélation avec les adresses IP collectées par les sociétés de gestion. Par ces deux décisions, la CNIL dégage certains principes gouvernant la validité des outils logiciels de repérage des contrefacteurs. Concernant tout d'abord l'envoi de messages pédagogiques aux internautes soupçonnés d'actes de contrefaçon :

- l'autorisation donnée aux fournisseurs d'accès de traiter les données de connexion de leurs abonnés est limitée aux cas prévus par la loi. L'envoi de messages pédagogiques pour le compte de tiers ne fait pas partie de ces cas ;

- selon le principe énoncé par le Conseil constitutionnel dans sa décision du 29 juillet 2004 (57), les données collectées à l'occasion des traitements portant sur des infractions aux droits d'auteur et droits voisins ne peuvent acquérir de caractère nominatif que sous le contrôle de l'autorité judiciaire. La possibilité d'identification des internautes par les fournisseurs d'accès (ceux-ci envoyant les messages pédagogiques à leurs abonnés selon le procédé proposé par la SACEM, la SDRM, la SCPP et la SPPF) entre en contradiction avec ce principe.

Concernant ensuite la recherche et la constatation d'actes de contrefaçon :

- la phase judiciaire de la collecte des données de connexion doit être stric-

tement encadrée. Ainsi, les procès-verbaux permettant de lancer des poursuites ne peuvent être dressés que par des personnes dûment habilitées (dans le cas du SELL, par un agent assermenté désigné par le Syndicat et agréé par le ministère de la Culture) ;

- le traitement des données personnelles doit être proportionné et limité au but poursuivi. Les dispositifs logiciels doivent avoir pour objet de réaliser des actions ponctuelles et ne peuvent aboutir à une collecte massive de données ou à une surveillance continue du réseau « *peer to peer* » ;

- les internautes soupçonnés d'effectuer des actes de contrefaçon ne peuvent faire l'objet d'une collecte de données que dans des conditions objectives. Est considérée comme objective la sélection d'internautes faisant référence au degré de gravité de l'infraction supposément commise. À l'inverse, n'est pas considérée comme objective la sélection des internautes suivant des critères dépendant de la volonté des personnes utilisant l'outil logiciel (dans le cas SACEM/SDRM/SCCP/SPPF, des seuils correspondant au nombre de fichiers échangés étaient susceptibles d'être modifiés à tout moment par les sociétés de gestion).

La collecte de données à des fins de poursuite d'actes de contrefaçon est également envisagée par le droit communautaire (58). La directive relative au respect des droits de propriété intellectuelle (59) prévoit un « *droit d'information* » permettant aux autorités judiciaires d'ordonner la communication d'« *informa-*

Le droit national et communautaire offre à la lutte contre la contrefaçon les moyens de légitimer le traitement des données de connexion des internautes, dans des conditions qui se préciseront davantage au fil de la jurisprudence.

tions sur l'origine et les réseaux de distribution des marchandises ou des services qui portent atteinte à un droit de propriété intellectuelle » (60). Les informations visées par la directive sont les nom et adresse des personnes impliquées dans une activité illicite. La communication de ces informations peut être ordonnée au contrevenant ou à toute autre personne qui, notamment, « *a été trou-*

vée en train de fournir, à l'échelle commerciale, des services utilisés dans des activités litigieuses » ou « *a été signalée (...) comme intervenant dans la production, la fabrication ou la distribution des marchandises ou la fourniture de services* ». Ces dispositions permettent au juge d'obliger les opérateurs internet à révéler l'identité de leurs abonnés.

Le droit national et communautaire offre ainsi à la lutte contre la contrefaçon les moyens de légitimer le traitement des données de connexion des internautes, dans des conditions qui se préciseront davantage au fil de la jurisprudence.

B. – Le champ d'application de l'obligation de conservation des données de connexion

Si la conservation des données de connexion est imposée aux opérateurs, le champ d'application de cette obligation est cependant encadré par une délimitation des catégories de données à conserver (1) et des personnes habilitées au traitement des données (2).

1. Les données concernées par l'obligation de conservation

a) Des données qui ne doivent pas concerner le contenu des communications

L'article 34-1 V° du Code des postes et des communications électroniques énonce que « *les données conservées et traitées dans les conditions définies aux II et III portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* ».

Dans une recommandation datant de 2001, le Forum des droits sur l'internet (61) a attiré l'attention des pouvoirs publics sur la nécessité pour le décret d'application de la loi sur la sécurité quotidienne (62) d'exclure les données indirectes de contenu (par exemple, l'URL de sites visités, l'adresse IP du serveur consulté ou l'intitulé d'un courrier électronique) ou de comportement (par exemple, l'adresse du destinataire d'un courrier électronique). En revanche, le Forum admet que l'adresse IP est bien une donnée nécessaire à l'établissement de la communication électronique, qui n'indique d'ailleurs rien quant au contenu des informations consultées ou au comportement de l'internaute.

À titre d'illustration, les données relatives aux en-têtes de message des courriers électroniques comportent le risque de dévoiler une partie du contenu des communications électroniques, car leur conservation implique le traitement du nom de domaine du serveur de l'ensemble des messages électroniques qu'une personne aura écrits (par exemple, de nombreux messages adressés à des personnes titulaires d'une adresse électronique du type nom.prenom@entreprise.fr). Les données relatives à l'adresse IP du terminal de l'utilisateur comportent également un risque similaire. La conservation de ces données doit interdire aux opérateurs qui utiliseraient des serveurs « proxies » de traiter les informations relatives aux pages internet consultées par leurs clients. Les fournisseurs d'accès se verraient alors contraints de scinder les données éventuellement enregistrées dans leurs serveurs « proxies » afin de ne conserver que les données relatives aux adresses IP de leurs clients, à l'exclusion de toute autre donnée qui pourrait en être issue (63).

b) Des données qui permettent l'identification des personnes

La loi du 6 août 2004 (64) traite des données à caractère personnel, notion plus large que celle de données nominatives : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». Une personne est ainsi identifiable au regard de l'ensemble des moyens à disposition du responsable du traitement, dont les données de connexion font partie.

L'article 34-1 V° du Code des postes et des communications électroniques étend le champ d'application de la conservation des données aux « données portant exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux ». L'identification des personnes est ainsi permise par le traitement des données de connexion. L'article 43-9 de la loi du 30 septembre 1986 telle que révisée par la loi du 1^{er} août 2000 (65) dispose que les fournisseurs d'accès et d'hébergement « sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont ils sont prestataires ». La communication de ces données peut être requise par les autorités judiciaires (66).

L'exactitude des données permettant l'identification des personnes ayant contribué à la création d'un contenu n'est pas

L'un des risques, tant pour les internautes que pour les opérateurs, réside dans une notion élargie de l'« opérateur » soumis à l'obligation de conservation des données de connexion.

exigée par la loi (67). Cependant, dans l'hypothèse où les données communiquées par l'opérateur ne permettent pas d'identifier l'auteur du contenu litigieux, la jurisprudence prend en compte le préjudice subi par le demandeur (68).

L'absence de décret précisant la nature des données à conserver ainsi que leur durée de conservation laisse le juge français dans l'incertitude, ce qui explique en grande partie les atermoiements judiciaires sur la question...

2. Les personnes soumises à l'obligation de conservation des données de connexion

L'un des risques, tant pour les internautes que pour les opérateurs, réside dans une notion élargie de l'« opérateur » soumis à l'obligation de conservation des données de connexion. Or il semble qu'une telle notion élargie trouve les faveurs du législateur et du juge.

En effet, malgré une notion d'opérateur communément liée à l'activité professionnelle de fourniture d'accès à un réseau de télécommunications (opérateur de télécommunications et fournisseurs d'accès et d'hébergement internet), les opérateurs ayant une activité accessoire de fourniture d'accès au réseau sont également soumis à l'obligation de conservation des données.

L'article 43-7 de la loi du 1^{er} août 2000 (69) définit l'opérateur en tenant compte tant de celui dont l'activité principale est la fourniture d'accès, que de celui qui, dans le cadre de ses fonctions, permet matériellement l'accès au réseau de façon accessoire. Ce dernier type d'opérateur est parfaitement illustré par le chef d'entreprise. Dans le cadre de l'exercice de leurs fonctions, les salariés disposent d'un accès au réseau internet. Par voie de conséquence, l'entreprise peut être considérée comme un fournisseur d'accès et est soumise à ce titre à

l'obligation de conservation des données de connexion, qu'elle doit communiquer le cas échéant aux autorités judiciaires. C'est la solution adoptée par la Cour d'appel de Paris dans une affaire opposant les sociétés World Press Online et BNP Paris Bas (70).

Cependant, l'obligation d'identifier l'auteur des contenus n'a pas été directement mise à la charge de l'entreprise. L'arrêt BNP reconnaît certes le statut d'opérateur à une entreprise n'exerçant pas l'activité de fourniture d'accès au réseau à titre principal, mais le juge a choisi de ne pas exiger l'identification des titulaires des adresses IP, bien que la loi l'y autorise.

Compte tenu du caractère accessoire et gratuit de l'activité fourniture d'accès au réseau, plusieurs interrogations peuvent être soulevées : le principe étant celui de l'effacement et de l'anonymisation des données, comment les archiver ? Sous quel format ? Dans quelles conditions d'accès et de sécurité physique et informatique ? Faudra-t-il habiliter un salarié spécifiquement désigné au sein de l'entreprise afin d'accéder aux données de connexion ou faudra-t-il prévoir une extension des compétences du nouveau correspondant à la protection des données (« correspondant CNIL ») institué par la loi du 6 août 2004 ? (71)

Le projet de loi sur le terrorisme (72) assimile aux opérateurs de communications électroniques les personnes physiques ou morales dont l'activité professionnelle directe ou indirecte est d'offrir une connexion internet à destination du public par l'intermédiaire d'un accès au réseau, à titre gratuit ou payant (73). Comme le précise expressément l'exposé des motifs du projet de loi, les cybercafés sont ainsi assimilés aux opérateurs de communications électroniques.

Dans son avis sur le projet de loi, la CNIL (74) estime que le projet de loi n'est pas suffisamment précis sur la question de l'identification des opérateurs habilités à conserver les données de connexion. L'inquiétude de la CNIL est tout à fait justifiée, dans la mesure où la notion de gratuité de l'accès au réseau élargit de façon exponentielle la définition d'opérateur. Ainsi, toute personne physique ou morale pouvant matériellement faire accéder des tiers au réseau, même à titre gratuit, devrait être considérée comme un opérateur, dont la notion perd ainsi tout caractère de métier, de savoir-faire spécifique. Un tel élargissement de la notion d'opérateur contribue à étendre l'obligation de conservation des données de connexion aux non-professionnels de la fourniture d'accès aux communications électro-

>

niques, ce qui risque fortement d'alourdir la facture, tant en termes financiers pour les opérateurs de tous ordres qu'en termes de garanties juridiques pour les internautes.

II. – L'ENCADREMENT DE L'OBLIGATION DE CONSERVATION DES DONNÉES

Afin de limiter la conservation des données à caractère personnel, exception au principe, il ne suffit pas d'en définir le champ d'application. Le principe de protection des données ne peut être suffisamment garanti que par un dispositif législatif affirmant clairement sa primauté (A). En outre, le dispositif n'est viable à long terme que si l'équilibre avec les intérêts des opérateurs soumis à l'obligation de traitement des données est recherché, notamment en reconnaissant à ceux-ci le droit d'obtenir une compensation financière (B).

A. – La nécessaire protection des droits et libertés individuelles

L'obligation de conservation des données à caractère personnel est encadrée par le principe de finalité (1) ainsi que par l'instauration d'une durée limitée de rétention (2). Le contrôle de la mise en œuvre de la conservation des données est également un autre moyen de garantie (3).

1. Le principe de finalité

La conservation de données à caractère personnel est une exception au principe de confidentialité et d'anonymisation des données. À ce titre, le traitement des données personnelles mérite une justification indiscutable et doit être proportionné et limité au but poursuivi.

En ce qui concerne les données conservées par les opérateurs à des fins qui ne sont pas liées à leur activité (contrairement aux données conservées pour la facturation de leurs clients et la sécurité de leurs réseaux), mais aux fins de les communiquer à des tiers, la finalité de la conservation prend une dimension tout à fait spécifique. La rétention de données pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales nécessite un cadre législatif particulièrement strict.

Le principe de finalité oblige à ce que les catégories de données collectées et traitées ainsi que leur durée de conservation soient déterminées par la finalité du traitement. En d'autres termes, le traitement et la conservation d'une donnée ne peuvent se justifier qu'au regard de la finalité qui préside à sa collecte. Afin

de faciliter le travail des autorités judiciaires, les législations de protection des données à caractère personnel leur ont reconnu, dans le strict cadre défini par la procédure pénale, la possibilité d'accéder aux données relatives aux infractions pénales.

La limitation dans le temps de la rétention des données est l'une des meilleures garanties pour restreindre la portée de l'exception au principe de protection des données.

Au regard de l'article 8 de la Convention européenne des droits de l'homme (75), la Cour européenne des droits de l'homme a posé le principe de l'équilibre entre les nécessités étatiques liées à la sécurité et le principe de protection de la vie privée des personnes (76). Selon cette jurisprudence, toutes les mesures de conservation des données (celles-ci correspondant dans les affaires concernées à des écoutes téléphoniques) ne peuvent donner lieu à des mesures générales de surveillance et de contrôle.

La directive de juillet 2002 (77) précise dans son article 15-1 que « *les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques (...)* ».

Cependant, la récente proposition de directive (78) limite la portée de ces garanties en insérant un nouvel article 15-1 bis (79). Cette disposition est la seule modification apportée par la proposition de directive au texte de 2002 : « *Le paragraphe 1 [de l'article 15 de la directive de juillet 2002] n'est pas applicable aux obligations en matière de conservation de données pour la prévention, la recherche, la détection et la poursuite d'infractions pénales graves, comme les actes terroristes et la criminalité organisée (...)* ».

Ainsi, selon le nouveau texte communautaire, la conservation de données pour la prévention, la recherche, la détection et la poursuite d'infractions pénales graves ne nécessiterait plus d'être une mesure nécessaire, appropriée et proportionnée. Cette disposition vide quelque peu le principe de finalité de sa substance. Pourra-t-elle survivre à l'autorité des textes protecteurs des libertés individuelles et à la jurisprudence protectrice de la Cour européenne des droits de l'homme (80) ? On peut en douter...

Dans un récent avis, le Groupe de travail de l'article 29 (81) déplore l'insuffisance des garanties offertes par la proposition de directive et souligne le caractère indéterminé de son domaine d'application. Selon le Groupe, l'obligation de conservation des données devrait viser les seuls crimes organisés et les actes de terrorisme, et non les simples « *infractions pénales graves* ». Même si la proposition de directive garantit qu'aucun accès ne sera accordé aux données conservées à des finalités autres que répressives, c'est-à-dire que les fournisseurs de services de communications électroniques ne pourront y avoir accès, le texte a suscité quelques réserves de la part du Groupe de travail.

Dans le projet de loi relatif à la lutte contre le terrorisme (82), l'obligation de conservation des données de connexion n'a pas pour seul but de réprimer les actes de terrorisme et de faciliter la constatation des infractions et l'identification de leurs auteurs, mais aussi de prévenir de tels actes (83). La mise en œuvre de cette politique de prévention nécessite une vigilance particulière de la part de la CNIL, qui relève à ce propos (84) le caractère imprécis de l'objectif de « *prévention* » des actes de terrorisme.

2. Une durée de conservation limitée

La limitation dans le temps de la rétention des données est l'une des meilleures garanties pour restreindre la portée de l'exception au principe de protection des données.

L'article L. 34-1 du Code des postes et des communications électroniques dispose qu'il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes ces données techniques. Faute de décret pris en application de ces dispositions, la durée exacte de conservation des données n'est pas davantage précisée à ce jour. Cette précision serait d'autant plus utile que les délais de conservation diffèrent suivant la nature des données concernées. En effet, pour les données conservées pour les besoins de la recherche, de

la constatation et de la poursuite des infractions pénales, une durée maximale d'un an (à compter de leur enregistrement) semble communément admise. Cette durée convient également à la rétention des données collectées aux fins de facturation. Pour les données nécessaires à la sécurité des réseaux des opérateurs, une durée de trois mois serait *a priori* suffisante.

Dans son avis relatif à la loi sur la société de l'information de 2001, la CNIL (85) a estimé qu'une période de conservation de trois mois pour les données traitées aux fins de recherche, de constatation et de poursuite des infractions pénales serait proportionnée. La recommandation de la CNIL a été dépassée depuis par le législateur... Dans son examen de la loi sur la sécurité intérieure du 18 mars 2003, la CNIL (86) a reconnu que l'augmentation du délai de conservation des données pouvait être justifiée par l'évolution de la criminalité sur les réseaux informatiques. Cependant, la CNIL a refusé une durée supérieure à trois mois qui, selon la Commission, est seule à pouvoir justifier une telle dérogation au principe de protection des données personnelles. La CNIL rappelle que le but légitime poursuivi par les autorités judiciaires peut toujours être garanti par d'autres moyens juridiques, notamment par la préservation de certaines données dans le cadre de procédures judiciaires. C'est notamment suite aux difficultés issues de la diversité des délais de conservation parmi les législations des États membres de l'Union européenne (87) que l'élaboration de la proposition de directive sur la conservation des données (88) s'est avérée nécessaire.

Toutefois, cette proposition de directive ne facilite pas pour autant la tâche aux opérateurs, qui se voient imposer une double durée de conservation suivant le mode de communication des données : en principe, un an à compter de la date de la communication, à l'exception des données relatives à des communications utilisant uniquement ou principalement le protocole internet pour lesquelles le délai est de six mois (89).

Le principe demeure celui d'une conservation des données d'un an. Afin d'alléger leur obligation de conservation, les opérateurs ne chercheront-ils pas à réduire la durée de rétention des données à six mois en démontrant que les communications concernées utilisent « *uniquement ou principalement* » le protocole internet ? Il convient de s'interroger sur l'interprétation des termes « *uniquement ou principalement* ». Comment distinguer techniquement les communi-

cations utilisant « *principalement* » internet des autres communications électroniques ? Faudra-t-il que les opérateurs mettent en place deux systèmes de conservation ? Comment va s'opérer la restitution des données au sein d'une telle dualité de fonctionnement ?

La durée prescrite par la loi doit-elle être interprétée comme étant minimale ou maximale ? La loi française est claire à ce sujet en parlant de durée maximale (90). Cependant, si une durée maximale s'avère plus protectrice des libertés individuelles (et plus pratique pour les opérateurs), les textes ont parfois fait preuve d'hésitation (91).

Le Groupe « Article 29 » (92) attire l'attention sur l'importance de l'interprétation de la durée de conservation comme étant maximale, les États membres restant libres de prévoir des durées de conservation plus courtes. Comme le rappelle le Groupe de travail, une durée minimale laisserait en effet la porte ouverte à des délais de conservation supérieurs, dépassant ainsi les conditions légales de ce qui doit demeurer une exception au principe de non-conservation.

3. Le contrôle de la communication des données de connexion conservées

Afin d'échapper aux critiques d'ingérence et de non-respect des libertés fondamentales, le projet de loi relatif à la lutte contre le terrorisme (93) a posé pour garantie que les demandes d'accès aux données conservées par les opérateurs devront être motivées, centralisées et soumises à la décision d'une personne qualifiée nommée par le ministre de l'Inté-

La France a opté pour un cadre réglementaire qui fera certainement l'objet de nombreuses concertations impliquant les opérateurs.

rieur après avis de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) (94). En outre, les demandes d'accès aux données doivent faire l'objet d'un enregistrement communicable à tout moment à la CNCIS. Le projet de loi précise qu'un rapport d'activité annuel doit être établi par cette personnalité qualifiée et adressé au ministre de l'Intérieur et à la CNCIS. Un décret en Conseil d'État pris après avis de

la CNCIS et de la CNIL devra préciser notamment la procédure de suivi des demandes et les conditions et durée de conservation des données transmises. La loi est cependant lacunaire sur la formation de cette personnalité qualifiée, sur les délais de sa réponse ou encore sur la possibilité d'effectuer un recours hiérarchique contre une décision de refus de sa part. En revanche, la constatation d'un manquement ou d'une violation des libertés par cette personnalité qualifiée oblige celle-ci à saisir le ministre de l'Intérieur.

À défaut de précision du projet de loi, on peut espérer pour la sauvegarde des libertés que les recommandations et avis rendus en application de ces dispositions soient publics.

Néanmoins, on peut regretter que la constatation des violations des libertés individuelles soit confiée à cette seule personnalité qualifiée, sans que les opérateurs – acteurs majeurs du dispositif – ne puissent la saisir ou exercer un recours. Dans son avis relatif au projet de loi sur le terrorisme, la CNIL (95) estime que les garanties procédurales doivent être complétées.

La Commission déplore également l'absence de procédures d'évaluation dans le projet de loi français, à l'instar de la proposition de directive (96) qui prévoit une évaluation au plus tard tous les trois ans de l'application de la directive afin d'estimer la nécessité d'une éventuelle révision. La proposition prend également en compte des études d'impact de la rétention des données sur les acteurs du marché des communications électroniques, considérées pertinentes par la CNIL.

B. – La nécessaire compensation financière des opérateurs ?

Alors que l'objectif de protection des libertés individuelles est indiscutable, les opérateurs ne peuvent-ils pas réclamer une quelconque prise en compte de leurs intérêts ? L'obligation de conservation qui leur est imposée ne mérite-t-elle pas une compensation ?

Le projet de loi relatif à la lutte contre le terrorisme prévoit l'adoption de deux décrets d'application :

- un décret après avis de CNCIS (précitée) concernant les modalités d'application de la communication des données de connexion, notamment la procédure de suivi des demandes pour les agents de police ou de gendarmerie et les conditions et durée de conservation des données transmises ;
- un décret concernant la compensation financière.

La France a donc opté pour un cadre réglementaire qui fera certainement l'objet de nombreuses concertations impliquant les opérateurs. Cependant, un décret aurait dû être adopté concernant la compensation financière des opérateurs, en application de l'article L. 34-1 du Code des postes et communications électroniques (97).

Que doit-on entendre par compensation financière ? Doit-il s'agir d'un simple remboursement des frais ou d'une rémunération, voire les deux ? Il serait logique qu'indépendamment d'un remboursement par réquisition, inclus dans les frais de justice, une juste rémunération soit mise en place.

En effet, l'opérateur est soumis à une obligation de conservation des données dans des conditions encore indéterminées, faute de décret d'application, mais que l'on peut supposer particulièrement lourdes (support, accès limité, sécurité, etc.) au regard de la nécessité de protection des données traitées.

Le coût économique engendré par l'obligation de conservation des données de connexion est conséquent. Il implique en effet à la fois :

- un coût économique concernant spécifiquement le stockage de données que l'opérateur n'aurait pas à conser-

ver dans le strict cadre de son activité, et ce pendant une durée pouvant aller jusqu'à un an ;

- un coût salarial correspondant au recrutement et à la formation d'un personnel qualifié, consacré à la gestion des demandes de communication des données de connexion.

La prise en compte de la charge financière supportée par les opérateurs s'inscrit d'ailleurs dans une logique législative plus large. Ainsi, dans le cadre général des interceptions de sécurité portant sur le contenu des communications, une rémunération des opérateurs est requise par la loi (98).

Cette rémunération des opérateurs est impérative pour le Conseil Constitutionnel qui, dans sa décision du 28 décembre 2000 (99), rappelle que l'assistance fournie aux autorités judiciaires par les opérateurs ne correspond pas à leur activité principale de fourniture de service. Le Conseil constitutionnel se fonde sur le principe fondamental de l'égalité devant les charges publiques (100).

Au-delà du niveau national, la question de la rémunération des opérateurs a une incidence économique non négligeable. La compensation ne doit pas se contenter d'être symbolique afin d'éviter toute distorsion de concurrence entre les opé-

rateurs des États membres de l'Union européenne. Les opérateurs des divers États membres se regroupant au sein de structures économiques (filiales ou accords de partenariats), il serait souhaitable qu'une harmonisation européenne limite le risque d'un traitement inégalitaire entre les opérateurs des États membres.

En conclusion, notre modeste tentative de démêler les fils du « patchwork » législatif relatif aux données de connexion dévoile un vaste chantier juridique qui est encore loin d'être achevé, même si ce domaine est prioritaire tant au niveau national qu'euro-péen. Il semble que les intérêts des internautes et les intérêts des opérateurs ne soient pas si éloignés dans la problématique de la conservation des données de connexion. Aucun d'eux n'a en effet intérêt à une conservation des données de longue durée. Seul l'avenir dira si internautes et opérateurs feront cause commune face à la multiplication des mesures sécuritaires de l'État...

À la lecture de la loi française et de la loi communautaire, force est de constater que les garanties relatives au respect du principe de protection des données personnelles s'amenuisent face aux besoins croissants de sécurité publique. Il reste à espérer que la démocratie n'en pâtira pas davantage... u

(1) Projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, n° 2615, déposé à l'Assemblée nationale le 26 octobre 2005 et adopté en première lecture le 29 novembre 2005 après déclaration d'urgence.

(2) La question de la conciliation entre la lutte contre le terrorisme et le principe de protection des données à caractère personnel est débattue au sein de l'Union européenne. À titre d'illustration, le « programme de La Haye », lancé en mars 2004, a pour objectif de faciliter les échanges d'informations entre États membres tout en respectant la protection des données à caractère personnel.

(3) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(4) Directive n° 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE 23 nov. 1996, n° L 281, p. 31.

(5) L'article L. 32 15° du Code des postes et des communications électroniques définit l'opérateur comme étant « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ».

(6) Précité.

(7) Directive n° 2002/58/CE du Parlement et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »), JOCE 31 juill., n° L 201, p. 37, adaptant la directive 95/46/CE (précitée) au secteur des communications électroniques.

(8) Article 2 (b) de la directive. Le considérant (15) précise qu'« une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau ».

(9) Proposition de directive du Parlement et du Conseil sur la conservation des données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive n° 2002/58/CE (COM(2005)438 final, 21 sept. 2005). Voir le communiqué de presse de la Commission européenne à l'adresse <www.europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/1166&format=HTML&aged=0&language=FR&guiLanguage=fr>. Le texte intégral de la proposition est accessible à l'adresse <www.droit-technologie.org/1_2.asp?actu_id=1116>.

(10) Précitée.

(11) 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. Cons. CE n° 8958/04, 28 avr. 2004). Le projet a été présenté par la France, l'Irlande, la Suède et la Grande-Bretagne.

(12) Avis n° 9/2004 en date du 9 novembre 2004. Le Groupe de travail de l'article 29 est un groupe de travail institué par l'article 29 de la directive n° 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JOCE 23 nov. 1996, n° L 281, p. 31). Le Groupe « Article 29 » a un caractère consultatif et indépendant. Il est composé d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

(13) Rapport Portelli fait au nom de la commission des lois du Sénat, à propos de la proposition de résolution présentée par Alex Türk au nom de la délégation pour l'Union européenne sur le projet de décision-cadre sur la rétention de données traitées et stockées en rapport avec la fourniture des services de communications électroniques, 16 févr. 2005.

(14) Cf. Wery E., <www.droit-technologie.org>, 19 oct. 2005.

- (15) La directive du 12 juillet 2002 (précitée) est une directive-cadre dans le domaine du traitement des données à caractère personnel applicable aux communications électroniques. Rappelons que cette directive fait partie de l'ensemble des directives intégrées au « *paquet télécoms* ». Voir notamment Costes L., Lamy droit de l'informatique et des réseaux, Bull. actualité, sept. 2002, n° 150, p. 1 ; Decocq G., Comm. com. électr., oct. 2002, p. 37 et Verbiest Th. et Dervaux J., <www.droit-technologie.org>, 22 avr. 2002.
- (16) Cf. exposé des motifs (p. 6) et article 1^{er} de la proposition de directive.
- (17) Précitée.
- (18) Précitée.
- (19) Article 2 (b) de la directive du 12 juillet 2002.
- (20) Article 2 (c) de la directive du 12 juillet 2002.
- (21) Article 9.2 de la directive du 12 juillet 2002.
- (22) Article 2 (a) de la proposition de directive.
- (23) Voir *infra*, II, B.
- (24) Cf. l'intitulé de l'article 3 de la proposition de directive : « *l'obligation de conservation de données* ».
- (25) Précitée.
- (26) Loi n° 2001-1062, 15 nov. 2001 (LSQ), JO 16 nov. 2001. Sur la LSQ, voir notamment Costes L., Lamy droit de l'informatique et des réseaux, Bull. d'actualité, nov. 2002, n° 141, p. 1.
- (27) Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, JO 10 juill. 2004, p. 12483.
- (28) Loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure, JO 19 mars, p. 4761.
- (29) CNIL, Dél. n° 03-056, 9 déc. 2003.
- (30) CNIL, Dél. n° 01-018, 3 mai 2001.
- (31) Loi n° 2002-1094, 29 août 2002, JO 30 août, p. 14398. Voir plus particulièrement en annexe 1, le Rapport sur les orientations de la politique de sécurité intérieure.
- (32) Loi n° 2001-1276 du 28 décembre 2001, JO 29 déc., p. 21133. Le Conseil constitutionnel a d'ailleurs validé ce texte, en estimant qu'il n'y avait aucune atteinte à la protection des libertés publiques (Déc. n° 2001-457 DC, 27 déc. 2001).
- (33) Loi n° 2004-204, 9 mars 2004, JO 10 mars, p. 4567.
- (34) Article 706-95 du Nouveau Code de procédure pénale.
- (35) Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle, JO 10 juill., p. 12483.
- (36) Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO 7 août, p. 14063. Pour une étude approfondie de la loi, cf. Dossier spécial La loi « *Informatique et libertés* » et l'entreprise, RLDI 2005/9, nos 267 à 270 ; spéc. Frayssinet J., La loi relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ?, p. 49 et s. ; Türk A., Comm. com. électr., févr. 2005, p. 12 ; Caprioli E., Comm. com. électr., févr. 2005, p. 24 ; Leclercq P., Comm. com. électr., févr. 2005, p. 29 ; Lepage A., Comm. com. électr., févr. 2005, p. 33.
- (37) Précitée.
- (38) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO 22 juin 2004, p. 11168, art. 6 II.
- (39) Cf. Reynaud P., <www.droit-technologie.org>, 9 sept. 2004.
- (40) Cf. Verbiest T. et Wery E., Terrorisme et internet : vers une dérive sécuritaire ?, <www.droit-technologie.org>, 25 mars 2002.
- (41) Précitée.
- (42) Précitée.
- (43) Précitée.
- (44) Convention européenne des droits de l'homme, article 8 – Droit au respect de la vie privée et familiale : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».
- (45) Loi n° 91-646 du 10 juillet 1991, JO 13 juill. 1991, p. 9167 modifiant l'article 100 du Code de procédure pénale et l'article L 226-15 du Code pénal.
- (46) Voir notamment la jurisprudence « *Nikon* » : Cass. soc., 2 oct. 2001, n° 99-42.942, SA Nikon France c/ Frédéric O.
- (47) Précitée.
- (48) Article 3 de directive précitée.
- (49) Cf. Verbiest T. et Wery E., précités.
- (50) Précitée, article 30.
- (51) Des extraits de cette décision de la CNIL, en date du 7 février 2001, sont cités au sein d'une étude réalisée par le collectif EUCD à l'occasion d'une audition devant la Commission spécialisée du CSPLA sur la propriété littéraire et artistique et les libertés individuelles, le 7 février 2003. Sur cette décision, voir également le Rapport du Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA) sur la propriété littéraire et artistique et les libertés individuelles dans l'environnement numérique, juin 2003 (spéc. p. 11).
- (52) Précitée.
- (53) Voir Frayssinet J., L'accouplement du droit de la protection des données personnelles avec le droit d'auteur, Légipresse, nov. 2004, n° 216, p. 119.
- (54) Cons. const., déc. n° 2004-499 DC, 29 juill. 2004.
- (55) Sur cette décision, voir Frayssinet J., Attention, en cas d'abus le SELL peut être dangereux pour la contrefaçon de logiciels de jeux !, Légipresse, mai 2005, n° 221, I, p. 75.
- (56) Voir le compte-rendu de la décision sur le site internet de la CNIL : <www.cnil.fr>, Échos des séances, 24 octobre 2005. Voir aussi Wery E., <www.droit-technologie.org>, 25 oct. 2005.
- (57) Précitée.
- (58) La question des données personnelles et de la protection des droits de propriété intellectuelle a été étudiée par le Groupe de travail de l'« *Article 29* » (précité) dans un document de travail du 18 janvier 2005 (WP 104). Sur ce document, voir Munoz R., Comm. com. électr., mai 2005, p. 4 (n° 150).
- (59) Directive n° 2004/48/CE du 29 avril 2004 relative au respect des droits de propriété intellectuelle, JOCE 30 avr. 2004, n° L 157, p. 45.
- (60) Article 8 de la directive du 29 avril 2004.
- (61) Recommandation du Forum des droits de l'internet concernant la conservation des données relatives à une communication électronique en date du 18 décembre 2001 (accessible sur le site du Forum : <www.foruminternet.org>).
- (62) Précitée.
- (63) Ce point a été soulevé par la CNIL dans son avis du 9 décembre 2003 (précité).
- (64) Précitée.
- (65) Loi n° 2000-719 du 1^{er} août 2000, JO 2 août, p. 11903.
- (66) Article 43-9 alinéa 2.
- (67) La première version du projet de loi pour la confiance dans l'économie numérique (précitée) prévoyait pourtant une obligation de vérification des données conservées par les hébergeurs et fournisseurs d'accès, mais cette obligation a disparu après le passage du texte en première lecture devant le Sénat et n'a pas été reprise par la suite par les députés.
- (68) Ainsi, dans l'hypothèse où l'hébergeur avait rempli son obligation de communication des données de connexion, le juge lui a refusé le bénéfice de l'article 700 du Nouveau Code de procédure pénale sur le fondement de l'équité du procès (cf. TGI Paris, réf., 1^{er} déc. 2003, Ouvaton c/ Metrobus), aux motifs que l'hébergeur devait « *assumer la contrepartie d'une responsabilité limitée* » (TGI Paris, réf., 26 mai 2003, J'Accuse et UEJF c/ OVH et a.). Si les données déclarées ne sont pas de nature à permettre l'identification de l'auteur du site litigieux, le juge peut considérer que

l'hébergeur a ainsi manqué à l'obligation légale imposée par la loi du 30 septembre 1986 modifiée, et a donc commis une négligence au sens de l'article 1383 du Code civil (TGI Paris, 16 févr. 2005, Sté Dargaud Lombard c/ Tiscali Média).

- (69) Précitée.
- (70) CA Paris, 4 févr. 2005, S.A. BNP Paribas c/ Sté World Press Online. Cf. RLDI 2005/4, p. 37 et Verbiest T. et Reynaud P., <www.droit-technologie.org>, 9 mars 2005.
- (71) Loi précitée. Sur le correspondant à la protection des données, voir notamment Vercken G., Van Ossel G. et Serpagli C., RLDI 2005/9, n° 269, p. 58 et s.
- (72) Précité.
- (73) Article 4 du projet de loi.
- (74) Avis en date du 10 octobre 2005.
- (75) Précité.
- (76) CEDH, 6 sept. 1978, 5029/71, Klass et a. c/ Rep. Fed. d'Allemagne, et CEDH, 2 août 1984, 8691/79, Malone c/ Royaume-Uni.
- (77) Précitée.
- (78) Précitée.
- (79) Article 11 de la proposition de directive.
- (80) Aff. Klass et Malone, précitées.
- (81) Groupe de travail de l'article 29 (précité), Avis n° 113/2005, 21 oct. 2005.
- (82) Précité.
- (83) L'objectif de prévention des actes de terrorisme apparaît expressément tout au long de l'exposé des motifs de la loi.
- (84) Avis de la CNIL sur le projet de loi relatif à la lutte contre le terrorisme, précité.
- (85) Avis du 3 mai 2001 (précité).
- (86) Loi et avis précités.
- (87) Pour un comparatif des législations des États membres de l'Union européenne, voir le tableau en annexe du Rapport Portelli (précité).
- (88) Précitée.
- (89) Considérant (12) et article 7 de la proposition de directive. Le Groupe « Article 29 » a émis ses réserves quant à cette double durée de conservation (avis en date du 21 octobre 2005, précité).
- (90) Cf. article 34-1 du Code des postes et des communications électroniques (précité).
- (91) La décision-cadre du Conseil sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques (précitée) prévoit ainsi une durée minimale d'un an et une durée maximale de trois ans (article 4).
- (92) Groupe de travail de l'article 29 (précité), avis de nov. 1999 et oct. 2005, précités.
- (93) Article 5 du projet de loi précité.
- (94) La CNCIS est une autorité administrative indépendante régie par la loi du 10 juillet 1991 (précitée).
- (95) Avis précité.
- (96) Précitée.
- (97) Article L 34-1 II du Code des postes et des communications électroniques : « *Un décret en Conseil d'État, 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'État, par les opérateurs* ».
- (98) L'article L 35-6 du Code des postes et des communications électroniques dispose que « *les prescriptions exigées par la défense et la sécurité publique et les garanties d'une juste rémunération des prestations assurées à ce titre, à la demande de l'État, par les opérateurs, sont déterminées par décret* ».
- (99) Déc. Cons. cons. n° 2000-441 D, 28 déc. 2000, relative à la loi de finances rectificatives pour 2000.
- (100) Principe énoncé à l'article 13 de la Déclaration des droits de l'homme et du citoyen : « *Pour l'entretien de la force publique et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens en raison de leur faculté* ».