



Par  
Anne-Catherine  
LORRAIN

CERDI  
Université Paris Sud  
Paris XI



Par Garance  
MATHIAS

Avocat à la Cour

# Conservation des données de connexion : un projet de décret resserre la toile... ou comment l'ombre de « *Big Brother* » menace la « *confiance dans l'économie numérique* »

(À propos du projet de décret portant application de l'article 6 II de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique)

Un récent projet de décret portant application de l'article 6-II de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (1) (LCEN) vient préciser les modalités de conservation par les fournisseurs d'accès et les hébergeurs des données relatives à une communication électronique (2) permettant d'identifier les créateurs des contenus sur internet.

RLDI 919

**C**e décret (3), qui devrait être adopté avant la fin de l'année, a d'ores et déjà suscité une vague de critiques de la part des professionnels de l'économie numérique, qui voient en ce texte une menace pour l'internet « *made in France* » (4).

Même si l'obligation légale de conservation des données de connexion par les hébergeurs n'est pas nouvelle, ce projet de décret tend à rehausser d'une nouvelle pierre l'édifice législatif relatif à la conservation des données de connexion. La construction de cet édifice semble maintenir le législateur dans une activité constante, ce qui ne doit pas empêcher les observateurs de s'arrêter sur la rédaction des textes proposés (I), et surtout de les critiquer (II). À l'appui de cet exercice, le risque supporté par certains droits fondamentaux oriente la lecture du texte vers une conclusion assez pessimiste.

## I. – CONTEXTE ET DESCRIPTION DU PROJET DE DÉCRET

L'activité continue du législateur sur la question de la rétention des données vient de s'illustrer à nouveau par la publication de ce projet de décret d'application de la LCEN, touchant cette fois-ci à l'identification des créateurs de contenus. Le contexte législatif relatif à la conservation des données de

connexion est particulièrement fourni, tant au niveau européen que national (5). La France a légiféré sur la question dès l'adoption des premiers textes fondateurs en la matière, dont la Convention du Conseil de l'Europe sur la cybercriminalité de 2001 (6), et avant même que l'Union européenne n'adopte définitivement sa directive en mars 2006 (7).

### A. – Contexte

La loi ne permet la conservation des données relatives à une communication électronique que sous certaines conditions, leur effacement ou leur anonymisation demeurant le principe (8). Le législateur a d'abord précisé les conditions aménageant la conservation « *exceptionnelle* » (9) des données de connexion dans un décret du 24 mars 2006 (10), en application de l'article 34-1 du Code des P et CE (11), permettant la rétention des données utiles :

- dans le cadre de la facturation et du paiement des prestations de communications électroniques ;
- dans le cadre de la recherche ou de la poursuite d'une infraction ;
- dans le cadre de la protection des systèmes d'information de l'opérateur de communication électronique.

Ce décret soumet à l'obligation de conserver les données (et de les communiquer aux autorités compétentes en ayant fait la demande) les « *opérateurs de communications électroniques* », à savoir, selon les >

(1) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (JO 22 juin 2004, p. 11168). (2) Les expressions « *données relatives à une communication électronique* » et « *données de connexion* » sont utilisées, ci-après en tant que synonymes. (3) Le projet de décret a été publié en avril 2007. (4) M. Philippe Jannet, président du Groupement des éditeurs de sites en ligne (Geste), « L'État veut-il tuer Internet en France ? », Le Monde, 20 avril 2007. (5) Voir RLDI 2005/12, n° 334 et RLDI 2006/17, n° 501. (6) Le premier texte de loi français concernant la question de la conservation des données relatives à une communication électronique est la loi sur la sécurité quotidienne du 15 novembre 2001 (JO 16 nov. 2001), adoptée quelques jours avant la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001. (7) Directive 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 (JOCE 13 avr. 2006, n° L 105/54, p. 0054). (8) En droit national, le principe est posé par la loi n° 2004-801 du 6 août 2004 (JO 7 août 2004) adaptant la loi n° 78-17 du 6 janvier 1978 « *informatique et libertés* » au secteur des communications électroniques. La directive européenne « *vie privée et communications électroniques* » du 12 juillet 2002 (JOCE 31 juill. 2002, n° L 201) établit la règle en droit communautaire. (9) Bien qu'à la lecture du dispositif législatif, l'exception tende à devenir le principe ! (10) Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données de communications électroniques (JO 26 mars 2006, p. 4609) adopté en application de l'article 34-1 du Code des postes et communications électroniques (Code des P et CE) et codifié aux articles R. 10-12 et suivants du Code des P et CE. Sur ce décret, voir RLDI 2006/17, n° 501. (11) Article dont les dispositions ont été créées par la loi sur la sécurité quotidienne du 15 novembre 2001 (JO 16 nov. 2001), confirmées par la loi sur la sécurité intérieure du 18 mars 2003 (JO 19 mars 2003) puis complétées par la loi relative à la lutte contre le terrorisme du 23 janvier 2006 (JO 24 janv. 2006). Voir *op. cit.*

termes du décret, les fournisseurs d'accès (12) et les opérateurs de téléphonie mobile.

Dans un contexte mondial de lutte contre le terrorisme, la réactivité étatique fut prompte. La recherche et la poursuite des infractions ont motivé l'intervention du législateur, dans une finalité de lutte contre le terrorisme, mais aussi de lutte contre la contrefaçon de masse (13). Le traitement des données dans le cadre de la lutte contre la contrefaçon devrait d'ailleurs connaître un nouvel essor, si la récente décision du Conseil d'État (14) conduit la CNIL à faciliter la tâche aux sociétés de perception et de répartition de droits dans leur recherche d'actes de téléchargement illicite commis par les internautes.

La conservation des données de connexion par les hébergeurs reste cependant à préciser. La LCEN attend donc le décret d'application de son article 6-II, dont le projet récemment publié devrait dissiper les suspens...

La loi du 1<sup>er</sup> août 2000 (15) exigeait déjà la conservation par les hébergeurs et les fournisseurs d'accès des données de connexion permettant d'identifier les personnes à l'origine de la création de contenus. En application de l'article 49-3 de la loi, le juge a estimé que dès lors que les données d'identification d'un créateur de contenus « *présentent un caractère manifestement fantaisiste ne permettant pas l'identification de la personne déclarée* », l'opérateur s'expose à l'engagement de sa responsabilité délictuelle pour négligence (16). Les dispositions de la loi du 1<sup>er</sup> août 2000 furent néanmoins modifiées par la LCEN, dont l'article 6-II dispose : « *les personnes mentionnées aux 1 et 2 du I (les fournisseurs d'accès et les hébergeurs) détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires (...).* »

*L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa (...).*

*Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation ».*

Contrairement au Code des P et CE, l'obligation de rétention des données visées par la LCEN ne concerne pas la poursuite d'infractions, mais l'identification des créateurs de contenu. Cette obligation s'inscrit dans le régime juridique global applicable aux hébergeurs et aux fournisseurs d'accès, dont font partie les dispositions de l'article 6 de la LCEN sur la responsabilité des opérateurs.

Sauf à les juxtaposer, la loi n'établit aucun lien direct entre la responsabilité des prestataires et l'obligation de conservation et de communication des données. Cependant, on peut aisément envisager l'hypothèse où un hébergeur aura connaissance de l'existence de contenus illicites, « *ou de faits et circonstances faisant apparaître ce caractère illicite* » (LCEN, art. 6 I 2), grâce aux nombreuses données qu'il aura obligatoirement conservées en application de la loi. Même s'il n'est pas soumis à une obligation générale de surveiller les informations qu'il transmet ou stocke, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites (LCEN, art. 6 I 7), l'opérateur n'aura-t-il pas forcément connaissance, par le biais des données conservées, de faits ou circonstances faisant apparaître le caractère illicite de certains contenus? La responsabilité de l'opérateur risque ainsi d'être mise en œuvre dans des circonstances jusqu'à présent inédites?

À l'égard du droit communautaire, l'initiative du législateur français relative à l'obligation de conservation des données par les hébergeurs peut sembler assez téméraire. En effet, la directive du 15 mars 2006 relative à la conservation des données de connexion (précitée) exclut de son champ d'application

les fournisseurs d'hébergement. Sans que cette exclusion soit toutefois explicite, les dispositions de la directive ne concernent que les opérateurs de téléphonie et les opérateurs de l'accès à Internet et de courrier électronique.

Cette initiative du législateur national pourrait obliger la France à procéder à une notification spécifique à la Commission européenne en vertu du principe de « *transparence* » des législations des États-membres en matière de services de la société de l'information (17).

*La collecte et le traitement des données personnelles étant l'exception au principe, le texte s'applique à indiquer les conditions restrictives dans lesquelles l'exception doit s'exercer.*

## B. – Description

La collecte et le traitement des données personnelles étant l'exception au principe, le texte s'applique à indiquer les conditions restrictives dans lesquelles l'exception doit s'exercer.

Première observation, l'article 1<sup>er</sup> du projet de décret contient de longues listes de catégories de données soumises à l'obligation de rétention, distinguant entre l'identification des créateurs de contenus et la relation des opérateurs avec leurs abonnés.

### 1. – L'obligation de conserver les données permettant d'identifier l'origine de la création de contenus

Le projet de décret distingue entre les données conservées par les fournisseurs d'accès d'une part, et par les hébergeurs d'autre part.

Les fournisseurs d'accès sont tenus de détenir et de conserver :

(12) La qualification d'« *opérateur de communications électroniques* » étant très largement définie car également applicable aux « *personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit* » (article 4 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, dont l'objectif est de soumettre au respect de la loi des établissements tels que les cybercafés). (13) La loi du 6 août 2004 modifiant la loi de 1978 « *informatique et libertés* » permet aux sociétés de perception et de répartition des droits d'auteur et droits voisins ainsi qu'aux organismes professionnels défendant ces droits de collecter et traiter les données personnelles (dont les données relatives à une communication électronique) relatives aux infractions aux droits dont ils assurent la gestion et la défense. Sur cette question, voir notamment RLDI 2005/12, n° 334, spéc. p. 51 s. (14) Le Conseil d'État (décision du 23 mai 2007, accessible sur <legalis.net>), voir RLDI 2007/28 n° 912, obs. Costes L., vient d'annuler la décision de la Commission nationale informatique et libertés (CNIL) du 18 octobre 2005 qui avait refusé de valider le dispositif technique de surveillance du réseau Internet mis en place par la SACEM, la SDRM, la SCPP et la SPPF visant à repérer les internautes soupçonnés d'échanger illégalement des fichiers musicaux et à leur envoyer des messages d'avertissement (sur la description de ce dispositif et sur la décision de la CNIL, voir *op. cit.*). La CNIL doit donc prendre une nouvelle décision, que l'on peut mal imaginer contredire ce désaveux par le Conseil d'État. (15) Loi 2000-719 du 1<sup>er</sup> août 2000 (JO 2 août 2000) modifiant la loi du 30 septembre 1986 relative à la liberté de communication. (16) CA Paris, 7 juin 2006, *Tiscali Media c/Dargaud Lombard, Lucky Comics* : « (...) en manquant à l'obligation légale mise à sa charge par les dispositions précitées (art. 43-9 de la loi du 1<sup>er</sup> août 2000), la société [...] a commis une négligence, au sens de l'article 1383 du code civil, et, dès lors, engagé sa responsabilité délictuelle puisque une telle négligence est constitutive d'une faute qui est en lien direct avec le préjudice subi (...) » (arrêt disponible sur <legalis.net>). (17) Directive n° 98/34/CE du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information, dite directive « *transparence* » (JOCE 21 juill. 1998, n° L 204, p. 37), modifiée par la directive n° 98/48/CE du 20 juillet 1998 (JOCE 5 août 1998, n° L 217, p. 18). Notons que le projet de décret d'application de l'article 6 IV de la LCEN relatif à la mise en œuvre du droit de réponse sur les services de communication publique en ligne a été communiqué aux services de la Commission européenne en application de la directive « *transparence* ».

- l'identifiant de la connexion (ex. : adresse IP) ;
- l'identifiant attribué par le système d'information à l'abonné ;
- les date et heure de début et de fin de connexion, les caractéristiques de la ligne de l'abonné.

Les hébergeurs sont tenus de détenir et de conserver :

- l'identifiant de la connexion à l'origine de la communication ;
- l'identifiant attribué par le système d'information au contenu, objet de l'opération ;
- l'identifiant attribué par le système d'information à la connexion ;
- le type de protocole ou de réseau utilisé ;
- la nature de l'opération ;
- les date et heure de l'opération ;
- les pseudonymes utilisés.

## 2. - L'obligation de conserver les données fournies par l'utilisateur lors de la souscription d'un contrat avec l'opérateur

D'autres catégories de données sont soumises à l'obligation de rétention par les fournisseurs d'accès et les hébergeurs, sans distinction, lors de la souscription d'un contrat de prestation de service avec un utilisateur.

Lors de la souscription d'un contrat ou lors de la création d'un compte par un utilisateur, le fournisseur d'accès et l'hébergeur sont tenus de détenir et de conserver :

- les nom et prénom ou la raison sociale ;
- les adresses postales associées ;
- les pseudonymes utilisés ;
- les adresses de courrier électronique associées ;
- les numéros de téléphone ;
- les mots de passe et informations associées.

Lorsque la souscription du contrat ou du compte avec l'utilisateur est payante, les prestataires sont tenus de détenir et de conserver les données relatives au paiement :

- le type de paiement utilisé ;
- le montant ;
- le numéro de référence du moyen de paiement ;
- les date et heure de la transaction.

À la première lecture du texte, quelques constatations s'imposent. En premier lieu, tous les acteurs de l'internet (hébergeurs et fournisseurs d'accès) sont concernés par ce texte, et ce y compris :

- les entreprises qui donnent accès au réseau internet à leurs salariés dans le cadre de leur activité professionnelle ;
- les cybercafés ;
- les responsables de services en ligne (blogs, webradios, etc.) ;
- les opérateurs de téléphonie qui offrent de manière courante des services multimédia.

Indépendamment des aspects techniques et pécuniaires, la philosophie de ce projet de décret peut être résumée ainsi : connaître et conserver l'ensemble des identifiants et contenus créés sur les réseaux numériques.

Dans ce contexte, la rédaction du texte soulève de nombreuses questions et, à travers celles-ci, une vive critique.

## II. - CRITIQUE DU PROJET DE DÉCRET

La critique et l'analyse répondent à des questions simples et pragmatiques : « *quoi?* », « *qui?* », « *pourquoi?* », « *comment?* ».

Toutefois, même si ce questionnement revêt l'apparence de la simplicité, il révèle les nombreuses incohérences du texte.

### A. - « *Quoi?* » ou l'objet de la conservation

Selon la directive du 15 mars 2006, la rétention des données de connexion exclut les données révélant le contenu des communications électroniques (18). Seul le « *contenant* » des communications est visé par l'obligation de conservation (19).

Cependant, l'article 6-II de la LCEN et son projet de décret d'application visent précisément la conservation des données « *permettant d'identifier l'origine de la création de contenus* ». Si ces données ne révèlent pas forcément en elles-mêmes le contenu des communications, mais seulement « *l'origine de leur création* », la frontière est pour le moins ténue.

C'est précisément en raison de la nature des données détenues par les hébergeurs, plus proches du « *contenu* » que du « *contenant* », que ces derniers ont été exclus du champ d'application de la directive du 15 mars 2006 (voir *supra*). Ceci serait d'ailleurs un argument de plus pour soutenir la nécessité d'une notification du législateur national à la Commission européenne. En vertu du principe de protection des données relatives à une communication électronique, qualifiables de données à caractère personnel (20), l'exception de conservation s'inscrit dans un dispositif limitatif où les listes de données conservées, de nature exhaustive, sont censées encadrer strictement l'exercice de l'exception.

La rédaction du projet de décret frappe tout d'abord par la longueur des listes de données concernées (voir *supra*). Cela ne devrait pas surprendre car parmi les données relatives aux contenus, à peu près tout est visé ! Sont en effet concernés non seulement les communications, mais tout contenu de type éditorial publié sur internet.

Nous critiquons la rédaction du décret du 24 mars 2006 (21) et le caractère ouvert de la liste des données conservées, risquant de réduire le principe de non-conservation des données à peau de chagrin. Cette critique n'aurait donc pas lieu d'être ici, devant une énumération aussi pointilleuse (même si rien dans la rédaction du projet de décret ne garantit le caractère limitatif des listes de données). Toutefois, bien que le juriste ne doive pas se plaindre des énumérations rébarbatives garantes du strict exercice des exceptions, l'obligation de conserver des données aussi personnelles que les pseudonymes, numéros de téléphone, mots de passe et autres numéros de référence du moyen de paiement (en d'autres termes, le numéro de carte de crédit par exemple), donne lieu à quelques interrogations légitimes si l'on veille à la protection des droits fondamentaux, dont le droit au respect de la vie privée (22).

De telles données sont-elles indispensables au stade du processus de conservation, préalable à celui de l'identification et de la personnalisation des données qui ne peut s'effectuer que dans le cadre d'une procédure judiciaire ? Plus que de simples données « *de connexion* », les données visées par le projet de décret ne laissent aucun doute sur leur nature intrinsèquement personnelle. Ces données sont « *relatives à une communication électronique* », certes, mais la plupart d'entre elles s'éloignent de la simple connexion aux réseaux pour s'approcher dangereusement de la révélation des contenus et rejoindre ainsi la sphère de la vie privée.

La technique est-elle si peu fiable que la conservation des seules données relatives à la connexion *stricto sensu* (tel que l'identifiant, le type >

(18) Article 1-2 de la directive du 15 mars 2006. Le principe est également posé par l'article 34-1, V° du Code des P et CE. (19) L'obtention du contenu des communications échangées doit faire l'objet d'une demande classique, mais très contraignante, devant la Commission nationale de contrôle des interceptions de sécurité (CNCS, autorité administrative indépendante régie par la loi du 10 juillet 1991). (20) Voir la loi n° 2004-801 du 6 août 2004 (JO 7 août 2004) adaptant la loi n° 78-17 du 6 janvier 1978 « *informatique et libertés* » au secteur des communications électroniques. (21) Voir RLDI 2006/17, n° 501. (22) Article 8 de la Convention européenne des droits de l'Homme.

de protocole utilisé, les date et heure de la connexion) ne permettrait pas d'identifier ultérieurement les personnes correspondant à ces données? L'article 1<sup>er</sup> du projet de décret s'achève par les dispositions suivantes :

« La contribution à une création de contenu comprend les opérations portant sur :

- des créations initiales de contenus,
- des modifications des contenus eux-mêmes,
- des modifications de données liées aux contenus,
- des suppressions de contenus ».

Par « contribution à une création de contenu », le projet de décret précise qu'il peut tant s'agir des créations initiales que des modifications ou suppressions des contenus, mais aussi des modifications des données qui leur sont liées. Pourquoi le projet de décret apporte-t-il ces précisions après avoir listé les catégories de données devant être conservées? Faut-il entendre que ces dernières ne feront l'objet d'une conservation qu'à l'occasion d'une « contribution à une création de contenu »? Le projet de décret ne donne aucune indication sur la portée exacte de ces précisions.

### B. – Qui est en charge de la conservation et pour qui celle-ci est-elle réalisée?

Les données et les contenus doivent être conservés par les hébergeurs et les fournisseurs d'accès, sachant que les notions de prestation d'hébergement et de fourniture d'accès sont particulièrement larges au sens de la loi et permettent d'englober nombres d'opérateurs, même non professionnels (23).

Le champ d'application du projet de décret est donc extrêmement vaste. En effet, un simple employeur ou une personne physique peut être qualifié d'« opérateur de communications électroniques » et donc être soumis aux dispositions légales.

L'une des nombreuses critiques formulées par les opérateurs consiste à dire qu'il leur est techniquement impossible de conserver les données émises pour chaque connexion ainsi que les contenus créés, modifiés ou effacés.

La situation devient alors paradoxale : si les professionnels et les experts techniques d'un secteur d'activité constatent une impossibilité dans l'application de la loi, comment le quidam néophyte de l'informatique pourra-t-il se conformer à ses obligations?

À ce jour, le pouvoir réglementaire ne semble pas avoir pris conscience de la difficulté technique, notamment de l'ampleur des moyens informatiques devant être déployés pour satisfaire l'obligation légale de conservation des données.

Les destinataires des données et contenus conservés sont tant les autorités judiciaires que les autorités administratives.

La nécessité pour les autorités judiciaires d'avoir accès à ces données ainsi qu'aux contenus dans le cadre d'actes réprimés par le Code pénal est aisément compréhensible. Étant rappelé que la constatation des actes répréhensibles s'inscrit dans le cadre d'une procédure édictée par le Code de procédure pénale, et ce afin de garantir plus particulièrement les droits de la défense.

Cependant, les autorités administratives interviennent dans un cadre préventif, notamment pour la prévention des actes de terrorisme (article 5 du projet de décret). Afin de garantir les droits

des individus, dont le respect de leur vie privée, il conviendrait de ne pas imposer un régime similaire concernant la répression et la prévention. Au stade de la prévention, nul acte répréhensible n'ayant été commis, la loi ne peut exiger les mêmes obligations.

Par ailleurs, le texte prévoit que dans le cadre des missions de prévention, le pouvoir de demander la communication des données conservées est dévolu aux seuls agents spécialement habilités. Cette garantie est sommaire, puisque le texte ne prévoit pas de contrôle *a priori* par la Commission nationale des interceptions de sécurité des demandes formulées par lesdits agents.

En d'autres termes, il n'y a pas d'opposition possible aux demandes de communication des données, ni de la part des prestataires internet, ni de la part des autorités administratives indépendantes.

Enfin, les demandes de communication des données n'ont pas à être motivées par les agents. Le risque d'arbitraire découlant de ces faibles garanties permet d'affirmer qu'une fois encore, les droits des individus ne sont pas dûment respectés.

*La détermination de la durée de conservation des données est essentielle à l'encadrement de l'exception au principe de protection des données personnelles.*

### C. – « Comment ? »

Arrêtons-nous sur les conditions de mise en œuvre de l'obligation de conservation des données de connexion à la charge des hébergeurs et des fournisseurs d'accès. Quelles garanties juridiques (1) et techniques (2) propose le projet de décret? Combien de temps les données doivent-elles être conservées (3) et à quel coût (4)?

#### 1. – Quelles garanties juridiques?

L'article 3 du projet de décret précise que la conservation des données de connexion s'effectue dans le cadre des dispositions relatives à la loi « Informatique et libertés » (24). Les données de connexion sont, en effet, qualifiables de données à caractère personnel puisqu'elles permettent d'identifier de manière directe ou indirecte un individu.

Il convient de rappeler que la loi « Informatique et libertés » met à la charge du responsable du traitement des données toutes précautions utiles au regard de la nature des données collectées et des risques présentés par le traitement. Notamment, le responsable du traitement doit empêcher que les données collectées soient déformées, endommagées ou qu'un tiers non autorisé puissent y accéder.

En tant que données à caractère personnel, les données de connexion et relatives aux contenus sont suffisamment sensibles pour exiger qu'indépendamment de l'avis de la CNIL, des garanties soient prises concernant la collecte, la conservation et l'accès des données.

À la lumière de l'article 3 du projet de décret, tel ne semble pourtant pas être le cas. En effet, même si le texte se rapporte explicitement aux dispositions de la loi « Informatique et libertés », cette référence demeure imprécise :

Nulle préconisation concernant le niveau de garantie, comme par exemple la référence à une norme de standardisation ou à un standard de sécurité minimale (habilitation nécessaire du personnel, encadrement de la sous-traitance, etc.).

Nulle recommandation relative à la possibilité pour les individus d'accéder, de rectifier ou de s'opposer à la collecte des

(23) Voir l'article 4 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme (précité). (24) Loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 (précité).

données. Ces droits sont pourtant fondamentaux dans le cadre du respect de la vie privée.

Nulle définition des « *normes techniques en vigueur* » n'est préconisée afin de conserver les supports dans lesquels sont stockées les données.

Nulle définition des conditions dans lesquelles l'intégrité et la confidentialité des données sont garanties.

Malgré ce manque de garanties, et le flou juridique en découplant, le projet de décret soumet les hébergeurs et les fournisseurs d'accès à l'obligation d'« *extraire* » les données dans un « *bref délai* », à la demande de l'autorité judiciaire.

Cette obligation de conservation et de communication des données suscite quelques interrogations.

À quel titre les autorités habilitées vont-elles exiger la communication des données conservées? Selon quelle procédure du Code de procédure pénale?

Dans quelles conditions les hébergeurs et/ou les fournisseurs d'accès procèdent-ils à l'extraction des données? Quelles sont les garanties de non-modification des données lors de cette opération? Comment délimiter le périmètre de l'extraction des données? Qui supervise cette opération d'extraction? Comment les droits de la défense sont-ils garantis?

Qu'est ce qu'un « *bref délai* »? Qui détermine ce « *bref délai* »? En cas de non respect de ce « *bref délai* », une prolongation est-elle possible?

Cette liste de questions est loin d'être exhaustive. Néanmoins, ce questionnement permet de mettre en exergue la carence du projet de décret. Cette faiblesse du texte engendre pour les opérateurs une lourde responsabilité, sans que celle-ci ne bénéficie d'aucune condition de limitation.

Les hébergeurs et les fournisseurs d'accès sont soumis à l'obligation de conserver les données relatives à l'identification de leurs abonnés, au paiement et aux contrats ainsi que les données relatives aux contenus, le contexte juridique de la mise en œuvre de cette obligation demeurant incertain.

Cependant, l'absence de conservation des données de connexion est lourdement sanctionnée par une amende de 75 000 euros d'amende et un an d'emprisonnement pour les personnes physiques et les dirigeants de personnes morales (LCEN, art. 6-IV-1). À ces peines peuvent s'ajouter des sanctions s'appliquant aux sociétés (interdiction de gestion ou d'exercer une activité professionnelle, etc.) ou encore des sanctions concernant les atteintes aux droits des personnes résultant des traitements informatiques (25).

### 2. – Quelles garanties techniques?

Selon le projet de décret, les données doivent être conservées « *sur des supports et dans des formats d'enregistrement conformes aux normes techniques en vigueur* » (article 3 du projet de décret). Toutefois, aucune norme technique n'est explicitement spécifiée pour la gouverner des opérateurs soumis à l'obligation de conservation.

On peut aisément envisager que les « *normes techniques en vigueur* » évoquées sont des standards ISO (Organisation internationale de normalisation). Cependant, il aurait été utile que le projet de décret préconise certaines normes concernant le respect de

l'intégrité des données ou leur non répudiation, et ce afin d'éviter toute contestation ultérieure, notamment dans le cadre d'une procédure judiciaire.

Par ailleurs, le décret prévoit que les modalités de transmission aux autorités compétentes, à la demande de ces dernières, doivent être réalisées « *selon des modalités assurant leur sécurité, leur intégrité et leur suivi* ». Ces modalités devront être définies par une convention conclue avec le prestataire concerné (cadre contractuel) ou, à défaut, par un arrêté conjoint du ministre de l'Intérieur et du ministre de la Défense (cadre réglementaire).

Le texte reste cependant silencieux concernant les modalités de conservation des données après leur transmission aux autorités administratives ou judiciaires. À titre d'unique indice, le projet de décret dispose que ces données seront conservées pendant trois ans, délai pendant lequel la Commission nationale de contrôle des interceptions de sécurité pourra émettre un avis sur les modalités de transmission des données, accéder à ces dernières et demander certains éclaircissements.

### 3. – Quelle durée de conservation?

La détermination de la durée de conservation des données est essentielle à l'encadrement de l'exception au principe de protection des données personnelles. Si exception il y a, elle doit au moins être limitée dans le temps.

Sans surprise, à l'instar du décret du 24 mars 2006 (précité), le projet de décret opte pour une durée de conservation des données d'un an (26) (article 2), conformément aux dispositions de la directive du 15 mars 2006 (27).

Les données sont conservées pendant un an « *à compter du jour de la création des contenus* ». Voici que ressurgit la délicate question de la détermination de la date de création des contenus sur internet.

La jurisprudence s'est prononcée à maintes reprises à cet égard, dans des affaires concernant l'application aux contenus numériques des délais de prescription des délits prévus par le droit de la presse (28). La solution consacrée par la chambre criminelle de la Cour de cassation (29), et confirmée depuis (30), ne distingue pas entre la presse écrite et internet : la loi de 1881 s'applique aux contenus numériques, avec un délai de prescription courant à compter de la date du premier acte de publication, c'est-à-dire à compter de la première mise à disposition du contenu au public.

Cependant, l'application de cette règle aux contenus diffusés numériques, de nature changeante, complique la tâche du juge. Dans quelle mesure la modification d'un site internet caractérise-t-elle une nouvelle publication donnant naissance à un nouveau délai de prescription? Les juges du fond ont donné une interprétation particulièrement extensive du principe, à tel point que le résultat s'apparentait parfois à faire des infractions commises sur internet des infractions continues, aux délais de prescription sans cesse renouvelés dès la moindre modification d'un site web constituant, selon les juges, de nouveaux actes de publication. >

(25) Articles 226-16 à 226-24 du Code pénal. Les peines pouvant aller de 5 ans d'emprisonnement à 300 000 euros d'amende. (26) Bien que l'AFA préconise une durée de conservation de trois mois (voir <<http://www.afa-france.com/deontologie.html>>). (27) La directive harmonise la durée de conservation en prévoyant une durée de conservation minimale de six mois et maximale de deux ans (art. 7). (28) Aux termes de l'article 65 de la loi du 29 juillet 1881, l'action publique et l'action civile résultant des crimes, délits et contraventions se prescrivent en matière de presse, après trois mois révolus, à compter du jour où ils ont été commis, soit du jour de la publication de l'écrit poursuivi. (29) Cass. crim., 30 janv. 2001, n° 00-83.004, Juris-Data n° 2001-008852; JCP G 2001, II, 10515; D. 2001, p. 1833, note Dreyer E.; Comm. com. électr. 2001, n° 6, p. 35, obs. Lepage A. (30) Cass. crim., 16 oct. 2001, n° 00-85.728, Juris-Data n° 2001-011587; Comm. com. électr. 2001, comm. n° 132; Légipresse 2001, III, p. 205, obs. Dreyer E.; Cass. crim. 27 nov. 2001, n° 01-80.134 et 01-80.135, Juris-Data n° 2001-012268; Comm. com. électr. 2002, comm. n° 162 et Cass. crim., 19 sept. 2006, n° 05-87.230, Juris-Data n° 2006-035552; Comm. com. électr. 2006, comm. n° 132. Les juges du fond se sont ralliés massivement au principe édicté par la Cour de cassation (voir par exemple, CA Poitiers, 11 déc. 2001, Comm. com. électr. 2002, comm. n° 110; CA Paris, 27 fév. 2002, Réseau Voltaire et a. c/C. L., Comm. com. électr. 2003, comm. n° 33; CA Paris, 29 janv. 2004, LICRA, MRAP et a. c/Costes, Légipresse 2004, III, p. 50; CA Paris, 2 mars 2005, Comm. com. électr. 2005, comm. n° 143).

Cette tendance à l'interprétation extensive de la notion de mise à disposition du public risque-t-elle d'influencer la mise en œuvre du futur décret d'application de la LCEN sur la conservation des données de connexion? Le délai de rétention d'un an « à compter du jour de la création des contenus » va-t-il renaître dès la moindre modification des contenus? Entre la notion de « création » de contenu et celle de « publication », il y a cependant une petite différence. La première invite davantage à l'interprétation extensive que la seconde. La notion de « création » est en effet plus vague que celle de « publication », cette dernière se référant à la mise à disposition effective du public et s'inscrivant dans le cadre du droit de la communication.

Peut-on ainsi imaginer qu'un contenu, dès lors qu'il est créé et avant même qu'il soit mis à disposition du public, puisse ouvrir droit à l'exigence de conservation des données qui lui sont relatives? Si l'on s'en tient à la lettre du projet de décret (qui entend pas « contribution à une création de contenu » toute création initiale, modification ou suppression de contenus; voir *supra*), il semble qu'une réponse positive s'impose, au dam de ceux qui tentent de prévoir la bonne mise en œuvre d'un tel dispositif!

L'interprétation extensive de la notion de publication par les juges du fond a toutefois été tempérée par la Cour de cassation (31). La tendance jurisprudentielle favorable au renouvellement des délais de prescription, et donc favorable à la répression, risquait en effet de dépasser l'objectif visé par la loi, sur le fondement de seuls arguments d'ordre technique relatifs à la notion de « publication » sur internet.

Les juges limiteront-ils de la même façon l'interprétation de la notion de création de contenus en prenant conscience que le délai de conservation des données ne peut être indéfiniment renouvelé? Si la jurisprudence s'est tempérée concernant la prescription des crimes et délits en matière de presse sur internet, il risque d'en aller différemment de l'identification des créateurs de contenus illicites, notamment dans le cadre d'enquêtes antiterroristes. Face à l'autorité de tels arguments, le juge ne pourra éviter le danger de l'allongement de la durée de conservation des données que sur le seul terrain de la protection du droit au respect de la vie privée.

Enfin, à l'expiration du délai de rétention, qu'advient-il des données conservées? Celles-ci seront-elles supprimées ou simplement anonymisées (32)?

On aurait pu légitimement attendre de ce projet de décret un niveau satisfaisant de garanties techniques et juridiques. Hélas, la lecture du texte est décevante à cet égard.

#### 4. – À quel coût?

Un mécanisme de compensation financière au bénéfice des opérateurs procédant à la rétention des données est prévu par le projet de décret, dans l'attente d'un futur arrêté déterminant les tarifs de cette indemnisation (33).

Rappelons que la rétention des données donne lieu à deux types d'investissement à la charge des opérateurs :

- les frais de collecte et de stockage des données afin de répondre aux nouvelles obligations légales de rétention (dépenses engagées en amont) ;
- les frais liés aux demandes de communication des données conservées (dépenses engagées en aval).

Toutefois, seuls les seconds investissements sont visés par le projet de décret (34). À l'instar du décret du 24 mars 2006, les frais nécessaires à la conservation elle-même des données ne sont pas pris en compte. Ceux-ci exigent pourtant de lourdes dépenses, impliquant des développements techniques, matériels et logiciels afin de collecter les données n'étant actuellement pas conservées, de les stocker

dans des conditions de sécurité et d'accessibilités appropriées et de les traiter dans les délais compatibles avec les enquêtes judiciaires.

C'est d'ailleurs en raison de l'absence de considération de ces investissements par le législateur que l'AFA (Association des Fournisseurs d'Accès) avait menacé d'agir devant le Conseil d'État à l'encontre du décret du 24 mars 2006 (35). Ceci explique pourquoi les tarifs correspondants au décret n'ont pu être établis par arrêté pour les fournisseurs

d'accès et les hébergeurs, mais pour les seuls opérateurs de téléphonie fixe et mobile (36).

Le législateur ne saurait ignorer les revendications des prestataires internet à l'égard des tarifs de leur indemnisation, eux seuls étant en mesure d'estimer les coûts réellement engendrés par les exigences de la loi. Les rédacteurs du projet de décret ne semblent pas avoir tiré la leçon des précédentes contestations des fournisseurs d'accès et de l'actuelle impasse dans laquelle se trouve la négociation de la tarification prévue par le décret du 24 mars 2006.

Ce projet de décret d'application de l'article 6-II de la LCEN est l'un des derniers textes rédigés par l'ancien gouvernement. La nouvelle équipe dirigeante va-t-elle s'inscrire dans la continuité? La question reste entière.

Dans l'attente des avis consultatifs de la CNIL et de l'ARCEP (Autorité de régulation des communications électroniques et des postes) sur le projet de décret, l'interception des données de connexion semble être une préoccupation constante pour le ministère de l'Intérieur, non seulement en terme d'activité législative, mais aussi encore plus concrètement. En effet, un nouveau centre tech-

*On aurait pu légitimement attendre de ce projet de décret un niveau satisfaisant de garanties techniques et juridiques. Hélas, la lecture du texte est décevante à cet égard.*

(31) Cass. crim., 19 sept. 2006 (précité). La Cour a cassé l'arrêt d'appel aux termes duquel « chaque mise à jour d'un site Internet constitue une réédition ». En l'espèce, la mise à jour du site Internet n'ayant pas affecté le contenu du texte litigieux, la Cour a estimé qu'il n'y avait pas de nouvelle publication. (32) C'est dans le but de se conformer à la directive européenne du 15 mars 2006 que Google a annoncé avoir réduit le délai de conservation des logs de connexion de ses utilisateurs à 24 mois. Au-delà de ce délai, le service n'a cependant garanti que l'anonymisation des données, et non leur effacement (voir <zdnet.fr>, actualité du 15 mars 2007). (33) Article 4 du projet de décret ajoutant un article R. 213-2 au Code de procédure pénale : « Les tarifs relatifs aux frais mentionnés au 24° de l'article R. 92 correspondant à la fourniture des données conservées en application de l'article 6 II de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, sont fixés par un arrêté du ministre de l'économie, des finances et de l'industrie et du garde des sceaux, ministre de la justice. Cet arrêté distingue les tarifs applicables selon les données requises, en tenant compte, le cas échéant, des surcoûts identifiables et spécifiques justifiés, supportés par les (hébergeurs et fournisseurs d'accès) requises par les autorités judiciaires pour la fourniture de ces données ». (34) Article 4 (précité) et article 10. (35) L'AFA critiquant l'absence d'une « juste rémunération » au bénéfice des opérateurs. (36) Arrêté du 22 août 2006 pris en application de l'article R. 213-1 du Code de procédure pénale (modifié par le décret du 24 mars 2006) fixant la tarification applicable aux réquisitions ayant pour objet la production et la fourniture des données de communication par les opérateurs de communications électroniques (JO 1<sup>er</sup> sept. 2006, p. 13010; RLDI 2006/20, p. 33). À titre d'exemple, concernant les opérateurs de téléphonie mobile, le tarif de l'identification d'un abonné à partir de son numéro d'appel ou du numéro de sa carte SIM est fixé à 6,50 euros; l'identification d'un abonné à partir du patronyme ou de la raison sociale à 13 euros. Les actes les plus « onéreux » concernent les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication (tarification jusqu'à 35 euros, notamment pour la fourniture du détail des trafics d'un abonné sur une période indivisible d'un mois).

nique d'interception des données de connexion a été récemment mis en place en application de la loi « *antiterrorisme* » de janvier 2006, dans les nouveaux locaux des services de renseignement de la police nationale, sous l'administration de UCLAT (Unité de coordination de la lutte antiterroriste).

Comme nous l'avons évoqué précédemment, le rôle des acteurs de l'internet, qui comptent parmi les maillons essentiels de l'économie numérique, tend à se transformer, aux frais de ces derniers, en un véritable rôle d'auxiliaire de justice.

La rigueur de la loi fait peser sur l'économie numérique un ris-

que non négligeable de délocalisation des activités des prestataires internet à l'extérieur des frontières de l'Union européenne. Face à l'irrésistible prolifération législative sur le traitement des données relatives aux communications électroniques, la vigilance est de mise dans l'application des textes, notamment au regard de la nécessaire protection du droit au respect de la vie privée, mais aussi du droit au libre exercice des activités économiques. Tous les acteurs du réseau internet ont-ils les moyens d'assurer cette vigilance? Si la question est cruelle, elle ne doit pas être abandonnée. ♦