Les nouveaux défis de la conservation des données de connexion

Par Benoit Tabaka
Chargé d'enseignement à l'Université Paris V – René Descartes
Membre du Comité éditorial de Juriscom.net
http://tabaka.blogspot.com

e-mail : benoit@tabaka.org

S'il ne fallait trouver qu'un seul et unique mot permettant de résumer simplement les opinions exprimées par de nombreux acteurs en matière de conservation des données de connexion, ce serait sans doute « sourire ».

Souriez, vous êtes fliqués ! La formule est facile mais elle est devenue usuelle lorsque l'on aborde cette question. En effet, l'internet n'est pas un mécanisme de télématique anonyme ; c'est, comme le définit le Code des postes et communications électroniques, un outil de communication au public en ligne. Partant de là, les activités opérées sur la toile mondiale deviennent visibles, pouvant être notamment préjudiciables à une personne physique ou à une entreprise d'où la nécessité de mettre en œuvre des outils permettant d'identifier ces fameux internautes. La solution choisie est de nature technique : imposer aux intermédiaires de conserver des données d'identification.

Cette obligation est apparue, en France, au sein de la loi du 1er août 2000, lorsque le Parlement a créé au sein de la loi du 23 septembre 1986 un article 43-9 imposant aux fournisseurs d'accès (article 43-7) et aux hébergeurs de données (article 43-8) de procéder à la conservation de données permettant l'identification de leurs utilisateurs. Ce texte a été complété par les dispositions de la loi du 15 novembre 2001 sur la sécurité quotidienne, créant le cadre juridique de la conservation et de l'accès de ces données.

Rappelons-le, ces dispositions – aujourd'hui codifiées à l'article L.34-1 du Code des postes et communications électroniques – posent le principe de l'effacement des données relatives au trafic collectées par les opérateurs de communications électroniques, voire, leur anonymisation une fois la communication terminée.

Ce principe d'effacement, souvent oublié, a été tempéré progressivement par trois exceptions, de manière à permettre aux opérateurs de conserver des données à des fins de facturation, à des fins de protection de leurs propres réseaux et ou de leur imposer une telle conservation afin d'y offrir un accès aux autorités judiciaires sur réquisition. Une double limite est néanmoins fixée : le délai de conservation ne peut dépasser douze mois et les données conservées ne peuvent porter sur le contenu consulté par l'internaute. Un décret d'application est aujourd'hui attendu afin de fixer la liste des données et la durée exacte de conservation.

En sommeil jusqu'au début de l'année, le régime de la conservation des données relatives à l'établissement d'une communication électronique est revenu sur le devant de la scène en raison de deux phénomènes cumulatifs : le débat, au niveau européen, d'un projet de décision-cadre[1] tentant d'unifier les divers régimes prévus par les Etats membres et, également, des décisions de justice venues préciser le champ d'application du dispositif français.

Au final, ces mouvements imposent aux acteurs de s'interroger à nouveau sur ce régime particulier, faisant apparaître au grand jour les réels problèmes de la conservation des données de connexion, dépassant largement la dichotomie traditionnelle quelle durée/quelles données.

[1] Projet de décision-cadre 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, 28 avril 2004, <http://www.senat.fr/europe/textes_europeens/e2616.pdf>.

I. Qui es-tu, fournisseur d'accès à l'internet ?

Premier défi : déterminer qui est soumis au régime de la conservation des données de connexion. La réponse à cette question n'est pas simple ; le régime juridique français prévu en la matière n'atteignant pas l'objectif de valeur constitutionnelle d'intelligibilité de la loi. Heureusement, et comme le dit l'adage, « *l'obscurité de la loi est un appel à l'intelligence du juge* ».

Cette intervention quasi-divine du magistrat est illustrée par un arrêt de la Cour d'appel de Paris du 4 février 2005[2]. Découverte par les cyber-veilleurs du Forum des droits sur l'internet[3], largement commentée[4] depuis, cette décision est d'une importance forte dès lors qu'elle confirme l'idée[5] selon laquelle une entreprise peut être qualifiée de fournisseur d'accès à l'internet et donc soumise à ce régime de conservation des données de connexion.

En l'espèce, une entreprise (*World Press OnLine*) a été victime du jour au lendemain de la démission de deux de ses représentants à l'étranger à la suite de la réception par ceux-ci d'un courriel anonyme vantant la mauvaise santé financière de leur employeur. Envoyé depuis une adresse gratuite et anonyme, ce courriel a pu être identifié comme ayant été adressé depuis une adresse IP attribuée à la *BNP Paribas*. La société victime s'est donc retournée vers le banquier afin d'obtenir l'identité de leur salarié à l'origine dudit message. Face à un silence persistant, *World Press Online* saisit la justice et obtient gain de cause, tout d'abord par une ordonnance de référé du Tribunal de commerce de Paris du 12 octobre 2004, puis par cet arrêt confirmatif de la Cour d'appel de Paris.

Dans cette décision, rendue sous l'empire de la loi du 1er août 2000, les magistrats posent le principe selon lequel « *en sa qualité, non contestée, de prestataire technique au sens de l'article 43-7 de la loi du 1er août 2000, la Société BNP PARIBAS est tenue, en application de l'article 43-9 de ladite loi, d'une part, 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 elle est prestataire et, d'autre part, à communiquer ces données sur réquisitions judiciaires* ».

Cette solution mérite d'être analysée au regard du régime alors applicable. Aux termes de l'article 43-9 de la loi du 23 septembre 1986, « *les prestataires mentionnés aux articles 43-7 et 43-8 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 elles sont prestataires* », les autorités judiciaires ayant la possibilité d'en requérir communication.

L'article 43-7 de la même loi vise « *les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée* », l'article 43-8 faisant référence aux « *personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services* ». Sont ainsi visés par ces textes les hébergeurs de données et les fournisseurs d'accès à l'internet professionnels, c'est-à-dire ceux « *dont l'activité est d'offrir* » un accès à l'internet. L'entreprise ne se situe dans aucune de ces définitions.

---

[2] CA Paris, 14ème Ch., 4 février 2005, BNP Paribas c/ Société World Press OnLine, *Foruminternet.org*, <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=867>.

[3] « Entreprise : accès tu fourniras, données tu conserveras », *Foruminternet.org*, 1er mars 2005, <http://www.foruminternet.org/actualites/lire.phtml?id=868>.

[4] T. Verbiest et P. Reynaud, « BNP Paribas est un fournisseur d'accès au réseau ! », *Droit-technologie.org*, 9 mars 2005, <http://www.droit-technologie.org/1_2.asp?actu_id=1052> ; F. Brousse, « Conservation des données : les entreprises au même régime que les FAI », *JournalduNet.com*, 22 mars 2003, <http://www.journaldunet.com/juridique/juridique050322.shtml> ; I. Boubekeur, « Une entreprise peut se voir attribuer la qualité de fournisseur d'accès à l'internet », *Juriscom.net*, 4 avril 2005, <http://www.juriscom.net/actu/visu.php?ID=661>.

[5] V. Sédallian, « La responsabilité de l'employeur en tant que fournisseur d'accès à internet », *Légicom* 2002/2 n°27 p.47 ; X. Lemarteleur, « Mémoire - L'employeur : un fournisseur d'accès à l'internet comme les autres ? », *Juriscom.net*, 29 octobre 2003, <http://www.juriscom.net/uni/visu.php?ID=377>.

Seulement, les dispositions de la Convention sur la cybercriminalité du 23 novembre 2001 – non encore ratifiée par la France mais déjà partiellement transposée par la loi sur la sécurité quotidienne – soumettent à un régime de conservation « *toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique* », intégrant en conséquence les entreprises. C'est donc, plus dans l'esprit que dans le texte de la loi française, qu'il faut rechercher une application des dispositions des articles 43-7 et suivants aux sociétés privées. Tel est le cheminement qu'a, sans doute, réalisé le juge en l'espèce, même s'il peut s'avérer faux. Il aurait fallu viser les dispositions introduites au sein du Code des postes et communications électroniques qui sont, seules, issues de la Convention sur la cybercriminalité.

Aujourd'hui, le nouveau régime de la conservation des données de connexion, fixé par l'article 6-I-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique et à l'article L. 34-1 du Code des postes et communications électroniques ne lèvent point, dans la lettre, cette ambiguïté. Il ne fait pas de doute, néanmoins, que les magistrats seraient tentés de suivre cette première décision tant elle s'inscrit dans l'objectif recherché par la loi française et, en particulier, la loi sur la sécurité quotidienne.

De même, bien que cela n'a point encore été jugé, d'autres acteurs pourraient être qualifiés de fournisseurs d'accès à l'internet au sens de la loi française. Il en serait ainsi des fournisseurs d'accès *Wifi* (particuliers ou *hotspots* professionnels) ou de points d'accès publics à l'internet – qu'ils relèvent du secteur public ou du secteur privé. A défaut de pouvoir communiquer de telles informations, l'opérateur pourrait être ainsi poursuivi en justice afin de retenir sa responsabilité civile[6], sur le terrain de la faute, voire pénale sur le terrain de la complicité.

II. Que fais-tu, fournisseur d'accès à l'internet ?

La loi pour la confiance dans l'économie numérique soumet les fournisseurs à des obligations annexes : obligation d'information et de fourniture de solutions de filtrage et blocage de l'accès à un site sur demande judiciaire. Sont-elles applicables aux entreprises ainsi transformées en fournisseurs d'accès ?

La réponse doit être négative. Le raisonnement est le même qu'en matière de définition. Dès lors que la soumission des entreprises à l'obligation de conservation est issue de la convention sur la cybercriminalité, seules ces dispositions – transposées en droit français à l'article L. 34-1 du Code des postes et communications électroniques – leur sont applicables. En conséquence, le reste du dispositif inséré – ou confirmé – par la loi pour la confiance dans l'économie numérique demeure applicable aux seuls prestataires dont l'activité, sous-entendue économique, est celle de fournir un accès à l'internet : les vrais fournisseurs d'accès. L'interprétation stricte de la notion figurant dans la loi du 21 juin 2004 sera d'autant plus nécessaire que le non-respect des obligations de conservation au sens de ce texte est pénalement sanctionné. Néanmoins, deux difficultés demeurent.

A. Le fournisseur d'accès : « Je vérifie ? »

Le fournisseur d'accès, quelle que soit sa nature, est-il tenu en matière d'identification à une obligation de vérification voire de résultat en la matière ? Il s'agit là du deuxième grand défi de la problématique de conservation des données de connexion. Cette question s'est posée à l'occasion des affaires « *Ouvaton* ». Dans ces affaires qui opposaient la régie publicitaire de la RATP (*Metrobus*) aux « anti-pubs », le Tribunal de grande instance de Paris avait été amené à se pencher sur la question de la validité des données permettant l'identification d'un utilisateur. En l'espèce, *Metrobus* n'ayant pas réussi à identifier les responsables du site incriminé, à l'aide des données communiquées par l'hébergeur, avait (re)saisi la justice à son encontre en arguant du non-respect de la première ordonnance enjoignant cette communication.

Dans une seconde ordonnance, en date du 2 février 2004, le tribunal avait estimé que « *les divers renseignements communiqués, et notamment les adresses IP des ordinateurs à partir desquels la*

[6] L. Thoumyre, « Affaire ESCOTA : un employeur jugé responsable d'un site litigieux réalisé par son salarié », *Juriscom.net*, 1er juillet 2003, <http://www.juriscom.net/actu/visu.php?ID=274>.

connexion pour l'ouverture de compte du site litigieux a été réalisée auprès du prestataire d'hébergement, doivent être considérés comme satisfaisant à l'injonction et de nature à permettre à la requérante d'obtenir les éléments d'identification des éditeurs du site ».

En pratique, le prestataire n'avait ici qu'un rôle d'intermédiaire : communiquer les données en sa possession sans vérifier si celles-ci n'étaient exactes. Cette position a été critiquée, notamment par mon collègue, et non moins ami, Yann Tesar qui affirmait « *qu'il soit possible de s'interroger sur cette solution au regard de la finalité du texte (l'article 43-9 n'impose à l'hébergeur aucune obligation de vérification). Quel pourrait être l'intérêt en effet d'une obligation légale de communication et de conservation de données erronées ?* »[7]. Il semble avoir été entendu récemment par le Tribunal de grande instance de Paris qui, dans une nouvelle affaire[8], a retenu la responsabilité de l'hébergeur qui avait communiqué des données d'identification farfelues.

Pour le fournisseur d'accès professionnel, cette obligation d'identification semble moins préoccupante dès lors qu'il possède des données précises sur ses utilisateurs – notamment en matière de facturation permettant d'assurer une telle obligation.

Pour l'entreprise, c'est une autre paire de manches et un réel défi. La situation est particulièrement délicate en matière de codes d'accès mutualisés ou liés à un ordinateur laissé en libre accès. Il lui reviendra alors de mettre en œuvre des outils techniques permettant d'opérer le contrôle des outils informatiques ou des utilisateurs sur le lieu du travail.

B. Le fournisseur d'accès : « J'essaye d'identifier ! »

En matière d'identification, un troisième défi, plus problématique à la fois pour les entreprises mais également pour les fournisseurs d'accès traditionnels, surgit. D'après les derniers chiffres publiés par *Médiamétrie*[9], la France compterait l'équivalent de 24 millions d'internautes. Or, bien évidemment, il est impossible à l'ensemble des prestataires d'attribuer des adresses IP uniques à tous ces utilisateurs, les opérateurs français n'en ayant pas obtenu l'allocation d'un nombre suffisant.

Pendant de nombreuses années, cette question était mineure : les internautes étaient quasiment tous en bas débit, n'étaient pas connectés en permanence et peu d'entreprises avaient accès au réseau internet. Seulement, avec la généralisation des offres haut débit (et des systèmes de voix sur IP nécessitant une connexion permanente), le nombre d'adresses IP utilisées simultanément a augmenté de manière exponentielle. Résultat : comment permettre à tout internaute de pouvoir surfer à tout moment ?

Une réponse technique a été mise en place : la mutualisation d'adresses IP, appelée plus communément la translation d'adresses (*Network Address Translation* ou NAT). « *Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement "une traduction") entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle* »[10]. En pratique, cela a pour effet de permettre à plusieurs internautes appartenant à un même réseau (entreprise ou fournisseur d'accès) de surfer sur l'internet avec la même adresse IP.

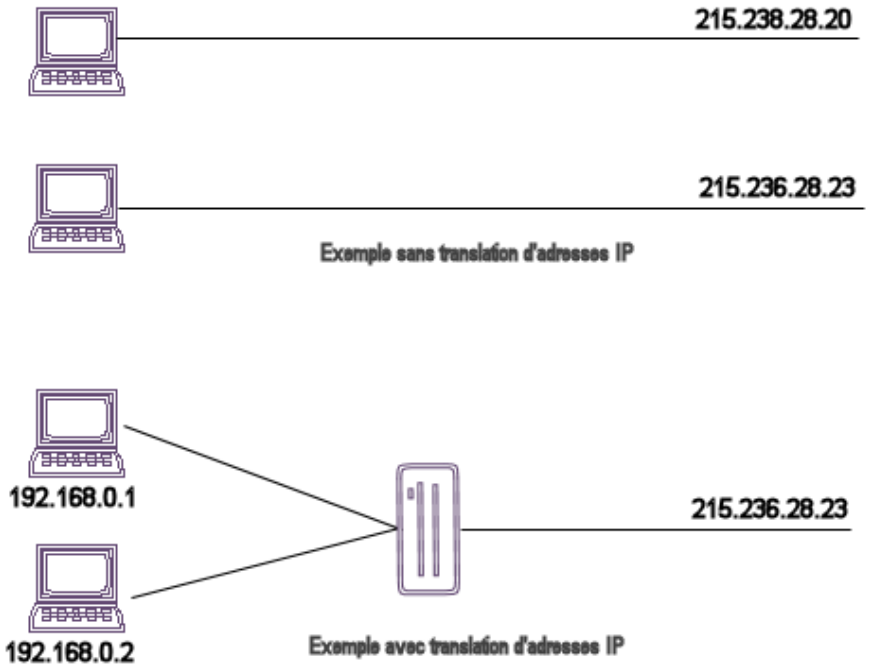
---

[7] Y. Tesar, « Metrobus remis sur les rails. "Où va-t-on ?", demande le juge », *Juriscom.net*, 4 février 2004, <http://www.juriscom.net/int/visu.php?ID=427>.

[8] TGI Paris, 3ème Ch., 16 février 2005, Dargaud Lombart, Lucky Comics c/ Tiscali Media, *Legalis.net,* <http://www.legalis.net/jurisprudence-decision.php3?id_article=1420>.

[9] « La France compte 24 millions d'internautes », *ZdNet.fr*, 29 mars 2005, <http://rss.zdnet.fr/actualites/internet/0,39020774,39214650,00.htm>.

[10] Définition donnée par *Commentcamarche.net* : NAT (*Network Address Translation*), <http://www.commentcamarche.net/internet/nat.php3>.



Problème : comment identifier l'utilisateur ayant commis l'infraction derrière un routeur opérant une telle translation ? Dans une situation où le fournisseur d'accès y a recours, l'autorité judiciaire devra accéder aux données de connexion conservées par le fameux « translateur » ; seules ces données permettant de déterminer, par exemple, que c'est monsieur Dupont qui s'est rendu sur le site internet pour diffuser des messages diffamatoires ou injurieux.

A ce niveau là, deux contraintes – l'une technique, l'autre juridique – s'oppose au recours à ces fameuses tables de translation. D'une part, les prestataires conservent au maximum pendant une durée de 5 jours les données y figurant. Afin d'assurer une identification pendant une durée d'une année comme l'exige la loi, il faudrait donc multiplier par 73 les capacités des serveurs en la matière. C'est sans doute à cause de ces contraintes techniques que *BNP Paribas* dans l'affaire précitée n'avait pas été en mesure, comme le rapporte la cour, d'identifier précisément le salarié à l'origine du courriel incriminé.

D'autre part, ces éléments sont associés, par nature, à des données de contenus puisque l'adresse du site internet visité par l'internaute est stockée[11]. Or, l'article L. 34-1-V précise que « *les données conservées et traitées (…) 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* ». L'alinéa 2 de cette disposition ajoute en outre, qu'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* ».

Le problème est donc important : pour identifier l'utilisateur – conformément à l'article L. 34-1 – les prestataires sont aujourd'hui tenus de conserver des données de contenus, en infraction avec les mêmes dispositions de l'article L. 34-1.

[11] En effet, en cas de translation d'adresses IP, pour déterminer quel internaute s'est rendu sur tel serveur, il est nécessaire de rechercher dans les *logs* du routeur quel est l'utilisateur (adresse IP interne au réseau) qui s'est rendu sur ledit serveur. Les adresses des sites ou serveurs visités sont donc conservées.

Deux solutions s'offrent alors aux acteurs. La première est la patience : attendre le déploiement du protocole IPV6 qui a notamment pour objectif d'éliminer la pénurie d'adresses IPV4 que l'on rencontre actuellement. Pendant ce laps de temps, la situation délicate demeure néanmoins. La seconde est d'analyser le dispositif de l'article L. 34-1 comme permettant une telle conservation de données de contenus à condition que ces données ne servent exclusivement qu'à identifier les utilisateurs. En clair, en cas de recours à une technique de translation d'adresses, il reviendra au prestataire de procéder à l'identification de l'utilisateur ; seul le résultat de l'opération pouvant alors être transmis. Il est vrai que les deux solutions ne sont pas satisfaisantes, la pratique ayant complètement dépassé l'encadrement juridique prévu initialement.

Conclusion

Au final, la conservation des données de connexion est à l'aube de ses défis. De nouveaux acteurs sont soumis à cette obligation, les limites techniques actuelles rendent difficiles l'identification des utilisateurs. Avec le temps, les prestataires devront aussi s'adapter à l'évolution de la cybercriminalité.

Aujourd'hui, celle-ci est focalisée sur des infractions quasi-instantanées dans leur commission et leur découverte (propagation de virus, *phishing*, escroquerie, etc.). Les milliers d'identifications demandées auprès des prestataires, en particulier membres de l'AFA, sont quasiment toutes fructueuses. Mais la criminalité évolue, certaines infractions lourdes (blanchiment d'argent, etc.) nécessitent des enquêtes de plusieurs années et les identifications deviennent de plus en plus impossibles. On comprend mieux les demandes récurrentes des autorités judiciaires d'avoir un délai de conservation équivalent à celui de la prescription en matière de délit, soit trois années.

B.T.