WIFI et conservation des données : Les obligations du fournisseur de services

PAR EMILIE BAILLY & EMMANUEL DAOUD (CABINET VIGO)

Donner accès à Internet constitue aujourd'hui pour certains professionnels (cybercafés, hôtels, bars ou autres lieux de restauration avec le développement des zones « Wi-Fi » ...) une prestation essentielle attendue par leurs clients. Ce service est, toutefois, soumis à des obligations strictement encadrées par la loi.

En effet, si en principe la navigation et la communication sur Internet reposent sur l'anonymat et l'effacement des données relatives au trafic, la loi contraint les personnes qui offrent un accès au réseau Internet à conserver les données techniques de leurs clients, pour les transmettre éventuellement aux services de police.

1. La conservation des données personnelles

La loi pour la confiance dans l'économie numérique du 21 juin 2004 (dite LCEN) impose aux FAI la conservation des 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 elle est prestataire » (article 6 II). Ainsi, le FAI doit, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre la mise à disposition de l'autorité judiciaire d'informations, pouvoir "déconfidentialiser" les données si l'autorité judiciaire lui en fait la demande.

La loi n° 2006-64 du 23 janvier 2006, relative à la lutte contre le terrorisme, à étendu cette obligation à l'ensemble des 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.

L'article L.34-1 du code des postes et des communications électroniques (CPCE), modifié par la loi du 23 janvier 2006, tend à soumettre les personnes offrant au public à titre professionnel une connexion à l'Internet aux mêmes obligations que les opérateurs de communications électroniques classiques, s'agissant des obligations de conservation de données permettant l'identification des personnes utilisatrices des services fournis.

Ainsi, en fournissant un accès Wifi au public à partir d'une connexion Internet, l'on endosse les mêmes responsabilités que le FAI.

2. Qui est concerné par la loi ?

Il s'agit de toutes « 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 ».

Selon le député Alain Marsaud , la disposition s'applique notamment :

> aux personnes dont l'activité même est d'offrir un service payant de connexion en ligne, que l'on qualifie généralement de « cybercafé » ;
>
> aux personnes qui offrent à leurs clients, dans un cadre public, ou à des visiteurs une connexion en ligne, tels les hôtels, les compagnies aériennes... ;
>
> aux fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne WIFI, généralement par l'utilisation de cartes prépayées permettant d'accéder à ce réseau, mais parfois également à titre gratuit.

3. Quelles sont les données à conserver ?

La loi renvoie au pouvoir réglementaire le soin de déterminer, par décret en Conseil d'État soumis à la Cnil, les catégories de données que les opérateurs doivent conserver et la durée de cette conservation.

Le décret du 24 mars 2006 a ainsi créé un nouvel article R.10-13 du CPCE, qui décrit les catégories de données à conserver. Il s'agit :

> des informations permettant d'identifier l'utilisateur (par exemple : adresse IP, numéro de téléphone, adresse de courrier électronique) ;
>
> des données relatives aux équipements terminaux de communication utilisés ;

des caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

des données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

des données permettant d'identifier le ou les destinataires de la communication.

Les données concernées sont, à titre d'exemple, les « log » de connexions (heures de connexion et durée de la connexion), l'adresse IP, ...

En revanche sont prohibées les conservations qui porteraient sur le contenu des correspondances (comme l'objet ou le texte d'un email) ou des informations consultées (contenu des pages Internet visitées).

La CNIL avait estimé que « cette rédaction ne permet pas aux opérateurs de mesurer précisément l'obligation qui leur est faite de conserver certaines données en dérogation au principe général d'effacement et d'anonymisation posé par la loi. Cette incertitude juridique est d'autant plus préjudiciable que le non-respect de cette obligation est sanctionnée pénalement » .

Quoi qu'il en soit, il semble que la conservation des données ne garantisse pas l'identification de l'utilisateur, c'est-à-dire la connaissance de son état civil. En effet, le décret du 24 mars 2006 n'a pas retenu l'hypothèse consistant à demander aux exploitants de « cybercafés », d'hôtels ou de bars qui offrent une connexion Wi-Fi, de relever l'identité de leurs clients. Il prévoit seulement la conservation des « données permettant l'identification ». Il s'agit donc, pour ces « fournisseurs de Wi-Fi » de recueillir des informations qui, mises bout à bout, constituent un faisceau d'indices permettant l'identification.

Le décret du 24 mars 2006 renvoie à un arrêté le soin de déterminer la nature des données susceptibles de faire l'objet d'une réquisition. On aurait pu espérer y trouver de plus amples précisions quant aux obligations des « fournisseurs de Wi-Fi », cependant, l'arrêté du 22 août 2006 ne vise que les prestations requises aux opérateurs de téléphonie mobile et fixe mais pas aux opérateurs internet.

En tout état de cause, il ne ressort pas des dispositions qui précèdent aucune obligation de relever et de conserver l'identité de ses clients pour fournir une connexion à la charge du « fournisseurs de Wi-Fi ».

Les « fournisseurs de Wi-Fi » peuvent donc choisir d'offrir cette prestation sans procéder à l'identification des personnes. Ils ne sont alors tenus de détenir que les données techniques créées par l'utilisation de leurs services.

Dans ces conditions, il n'existe aucune obligation de constitution de fichiers nominatifs des utilisateurs pour les services de communication électroniques offerts au public sans nécessité d'identification.

4. Combien de temps doit-on conserver les données ?

Le décret du 24 mars 2006 fixe la durée de conservation des données à un an, durée au-delà de laquelle elles devront être anonymisées.

Ce délai de conservation court dès l'enregistrement des données.

5. Quelle sanction ?

Tout manquement à l'obligation de conservation des données expose la personne à laquelle incombe cette obligation aux sanctions visées à l'article L. 39-3 du CPCE, soit un an d'emprisonnement et 75.000 euros d'amende pour les personnes physiques, et 375.000 euros pour les personnes morales (en application de l'article 131-38 du code pénal).

6. Quelles sont les conditions de communication des données ?

Les données de trafic, ainsi conservées, ne peuvent être consultées par la police et la gendarmerie nationales que dans un cadre judiciaire. Les articles 60-1, 77-1-1 et 99-3 du code de procédure pénale, disposent respectivement que l'officier de police judiciaire au cours d'une enquête de flagrance, le procureur de la République ou l'officier de police judiciaire, sur autorisation du procureur, au cours d'une enquête préliminaire ainsi que le juge d'instruction ou l'officier de police judiciaire par lui commis au cours de l'instruction, peuvent « requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptible de détenir des documents intéressant l'enquête ou l'instruction, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de leur remettre ces documents [...] ».

En dehors de ce cadre judiciaire, l'article L34-1-1 du CPCE prévoit un dispositif de réquisition administrative

pour prévenir le terrorisme. Ainsi, certains agents individuellement habilités des services de police et de gendarmerie spécialisés dans la prévention du terrorisme peuvent se faire communiquer certaines données de trafic générées par les communications électroniques. Les demandes de ces agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur.

Le fait, sans raison valable, de refuser de fournir les informations ou documents ou de faire obstacle au déroulement d'une enquête est puni de trois mois d'emprisonnement et/ou de 30 000 euros d'amende (Article L39-4 du CPCE).

7. Et HADOPI dans tout ça ?

La loi du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet a modifié l'article L. 34-1 du CPCE de façon à permettre aux opérateurs de communications électroniques de communiquer à l'HADOPI les données à caractère personnel et informations relatives à leurs abonnés recueillies en application de l'article L. 34-1 du CPCE.

Après les péripéties que l'on sait, la loi HADOPI a finalement été promulguée et le décret du 5 mars 2010 a mis en place le « Système de gestion des mesures pour la protection des œuvres sur internet » sur lequel seront enregistrées les données à caractère personnel et informations relatives aux abonnés recueillies auprès des opérateurs de communications électroniques par l'HADOPI. Selon le décret du 5 mars 2010, ces données sont les suivantes :

Nom de famille, prénoms ;

Adresse postale et adresses électroniques ;

Coordonnées téléphoniques ;

Adresse de l'installation téléphonique de l'abonné.

Or, comme on l'a vu, depuis la loi du 23 janvier 2006, les « fournisseurs de Wi-Fi » sont soumis aux mêmes obligations que les opérateurs de communications électroniques classiques.

Ils peuvent donc être amenés à répondre à une réquisition adressée par l'HADOPI.

Pour autant, et comme précédemment indiqué, il ne résulte ni de l'article L. 34-1, ni de l'article R.10-13 du CPCE une obligation pour celui-ci d'identifier les utilisateurs, ni de se faire communiquer préalablement à la connexion leurs noms, prénoms, adresses et coordonnées téléphoniques.

Ils doivent simplement disposer d'éléments permettant cette identification.

Les « fournisseurs de Wi-Fi » ne seront donc pas toujours en mesure de communiquer les données prévues par le décret du 5 mars 2010, mais uniquement des « données de trafic » ne permettant pas, pour le moins directement, d'établir une correspondance avec l'internaute contrevenant.

D'où les interrogations légitimes de certains quant à l'efficacité du dispositif en cas de connexion à la technologie wifi.

*Rapport du 16 novembre 2005 de Monsieur le député Alain Marsaud, fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République.

**Voir la délibération de la CNIL n°2005-254 portant avis sur un projet de décret relatif à la conservation des données de communications électroniques et modifiant le code des postes et des communications électroniques ; Voir également l'avis n° 2005-0875 du 7 octobre 2005 concernant le projet de décret relatif à la conservation des données des communications électroniques et modifiant le code des postes et des communications électroniques.

***Arrêté du 22 août 2006 pris en application de l'article R. 213-1 du code de procédure pénale fixant la tarification applicable aux réquisitions ayant pour objet la production et la fourniture des données de communication par les opérateurs de communications électroniques

****Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur internet »

Juin 2010, par Emilie BAILLY, Emmanuel DAOUD