Données de connexion : le temps de l'urgence ou l'urgence d'attendre ?

Par Franck Bergeron
Juriste NTIC

E-mail : franckbergeron@free.fr

« Ce ne sont pas les hommes qui gouvernent les sociétés,
ce sont les principe s; à défaut de principes, ce sont les situations.»
Pierre Joseph Proudhon

Introduction

Le projet de loi relatif à la lutte contre le terrorisme et portant diverses dispositions relatives à la sécurité et aux contrôles frontaliers[1], a été adopté par l'Assemblée nationale, le 29 novembre 2005 après déclaration d'urgence. Le texte prévoyant des mesures relatives à la généralisation de la vidéosurveillance près des lieux sensibles, le contrôle des voyageurs en partance vers certains pays, et l'installation aux péages de dispositifs de surveillance des voitures, comporte également des dispositions relatives à la conservation et à la communication des données de connexion.

Les dernières vagues d'attentats qui ont récemment frappé l'Europe ont en effet révélées avec quelle facilité les groupements terroristes pouvaient utiliser les réseaux de communications électroniques pour organiser et coordonner leurs actions. Fort de constat, le gouvernement a entendu compléter le dispositif législatif tel qu'il fut prévu dans la loi sur la sécurité quotidienne (LSQ) du 15 novembre 2001[2].

La LSQ a en effet créé, dans un article L. 34-1 du Code des postes et des communications électroniques (CPCE), un principe général d'effacement ou d'anonymisation de toute donnée relative au trafic, exception faite néanmoins de celles qui peuvent être conservées à des fins de facturation ou de sécurité du réseau des opérateurs, et celles qui peuvent être conservées aux fins exclusives d'enquêtes judiciaires pendant une période maximale d'un an. Un second régime, issu de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, impose aux fournisseurs d'accès à l'Internet ainsi qu'aux hébergeurs de détenir et conserver « *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* ». Un décret en Conseil d'Etat devait préciser le détail des données dont les opérateurs ont la charge d'assurer la conservation ainsi que la durée de celle-ci. Mais alors que ce décret est toujours attendu et qu'un livre blanc sur la sécurité intérieure face au terrorisme[3] est en cours de finalisation, le gouvernement a tout de même décidé de modifier ce dispositif.

Ainsi, le chapitre II du projet de loi consacré au « *contrôle des déplacements et communication des données techniques relatives aux échanges téléphoniques et électroniques des personnes susceptibles de participer à une action terroriste* » tend, d'une part, à élargir le cadre légal de la conservation des données de connexion (I) et, d'autre part, il institue un régime spécifique de communication de ces données aux autorités de police et de gendarmerie (II).

---

[1] Projet de loi relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, adopté en 1re lecture par l'Assemblée nationale, le 29 novembre 2005 : *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/ta/ta0506.asp>.

[2] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne (J.O. du 16 novembre 2001) : *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/dossiers/securite_quotidienne.asp>.

[3] Le livre blanc sur la sécurité intérieure face au terrorisme a pour objectif de préciser la nature de la menace terroriste et d'en mesurer les risques, d'évaluer les ressources humaines, ainsi que les moyens techniques et juridiques nécessaires au maintien d'un dispositif de protection adapté, d'informer les français et de définir les comportements à adopter : *Premier-ministre.gouv.fr*, <http://www.premier-ministre.gouv.fr/acteurs/communiques_4/preparation_un_livre_blanc_52923.html>.

I. L'élargissement du cadre légal de la conservation des données de connexion

L'article 5 du projet de loi conduit à étendre le dispositif actuel de la conservation des données de connexion, aux personnes qui permettent d'établir des connexions au réseau Internet comme notamment les cybercafés (A). Il consacre par ailleurs une véritable obligation de conservation de ces données (B).

A. Un dispositif étendu aux « fournisseurs de connexions »

L'article L. 34-1 du CPCE pose le principe de l'effacement des données relatives aux connexions par les opérateurs de communications électroniques, sous réserve des exceptions relatives aux enquêtes pénales ou à la facturation.

La définition de l'opérateur de communications électroniques figure à l'article L. 32 du CPCE. Il s'agit de « *Toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques* ». Seuls les opérateurs de téléphonie fixe et mobile ainsi que les fournisseurs d'accès à internet sont donc actuellement concernés.

Cependant, l'article L. 34-1 du CPCE aurait révélé certaines failles juridiques que le gouvernement ne souhaite pas voir exploitées par les réseaux terroristes. En effet, seules les données issues des connexions à l'Internet effectuées à partir d'abonnements dits « *classiques* » sont pour l'instant conservées. Il suffirait donc d'utiliser les services d'un cybercafé ou d'un point de connexion Wi-Fi ouvert au public pour pouvoir bénéficier d'une connexion à Internet totalement anonyme[4]. Les affaires *Reid* ou *Atta* auraient déjà mis en évidence l'utilisation de connexions alternatives par les réseaux terroristes pour leur propagande ou encore pour organiser leurs actions en toute confidentialité.

C'est la raison pour laquelle le gouvernement a souhaité revenir à l'esprit de la loi LSQ de 2001 en empêchant l'utilisation totalement anonyme de l'Internet en France. Pour ce faire, le projet de loi tend à « *préciser la définition des opérateurs de communications électroniques* », et à « *clarifier la situation juridique de ces fournisseurs d'accès en les assimilant explicitement aux opérateurs* »[5].

Mais qu'en est-il réellement ?

L' article 4, du projet de loi prévoit d'insérer un nouvel alinéa à l'article L. 34-1 du code des postes et des communications électroniques selon lequel, « *Les 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, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article* ».

La conservation des données de connexion concernerait donc les *« fournisseurs de connexions »* que sont :

- les cybercafés dont l'activité est d'offrir un service payant de connexion en ligne ;
- les hôtels ainsi que les compagnies aériennes offrant à leurs clients, dans un cadre public, ou à des visiteurs, une connexion en ligne ;
- les fournisseurs d'accès à des réseaux de communications électroniques accessibles via une borne Wi-Fi.

Ne seraient par contre pas concernées les personnes qui offrent une connexion en dehors d'une activité professionnelle, notion pour le moins difficile à cerner selon le rapporteur du projet de loi lui-

[4] Rapport n° 2681 déposé le 16 novembre 2005 par M. Alain Marsaud, rapporteur : *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/rapports/r2681.asp>.
[5] Extraits de l'exposé des motifs du projet de loi enregistré à la Présidence de l'Assemblée nationale le 26 octobre 2005 : *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/projets/pl2615.asp>.

même[6]. Ainsi, le secteur associatif pourrait échapper à ce dispositif de conservation et de communication des données de connexion[7].

Par ailleurs, les entreprises et les administrations ne devraient pas non plus être assimilées à des opérateurs de communications électroniques.

On se souvient en effet de l'arrêt de la Cour d'appel de Paris du 4 février 2005[8], dans lequel il a été affirmé qu'une entreprise pouvait être qualifiée de fournisseur d'accès à l'internet au sens de l'ancien article 43-7 de la loi du 30 septembre 1986, et que, dès lors, étant soumise aux obligations pesant sur cette catégorie de prestataire technique, elle devait « *détenir et 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* ».

Dans cette affaire cependant, la Cour ne s'était pas prononcée sur la qualification des personnes dont l'activité est d'offrir un accès à Internet et la banque elle-même n'avait pas jugé utile de contester cette qualification de prestataire technique. Rendue sous l'empire de l'ancienne législation, une solution identique pouvait dès lors être envisagée en application de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, dans la mesure où la LCEN a repris, au sein de son article 6-I, 1°[9], une définition quasi identique du fournisseur d'accès à Internet.

Cependant, deux critères interdisaient déjà toute assimilation des entreprises à des fournisseurs d'accès à Internet. L'article 6-I, 1° de la LCEN tout d'abord, introduit le critère de l'abonnement pour définir l'activité des prestataires techniques soumis à une obligation de conservation des données de connexion. Par ailleurs, la notion de « *mise à disposition d'un service de communication* » au public en ligne[10] est inapplicable aux connexions au réseau à Internet que sont susceptibles de proposer les entreprises ou les administrations à leurs seuls salariés ou agents.

La question se pose néanmoins pour les universités, notamment lorsque celles-ci proposent un accès au réseau au bénéfice de leurs étudiants.

Aussi, la CNIL avait-elle souhaité que le projet de loi liste précisément les personnes devant conserver les données techniques relatives à l'utilisation de l'Internet (les universités, les bibliothèques, les mairies qui proposent un accès à Internet…)[11].

Lors des débats parlementaires qui ont eu lieu le 24 novembre 2005[12], un amendement n° 69 allant dans ce sens a été soutenu par M. Mamère, Mme Billard et M. Yves Cochet. En réponse, le Ministre

---

[6] Rapport n° 2681 déposé le 16 novembre 2005 par M. Alain Marsaud, rapporteur : *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/rapports/r2681.asp> précité.

[7] La question se pose néanmoins concernant les points d'accès publics à Internet gérés par des associations.

[8] *Foruminternet.org*, <http://www.foruminternet.org/actualites/lire.phtml?id=868>. En l'espèce, une société avait accusé la rupture de deux contrats de représentation conclus avec des agents. L'un d'eux avait pris cette décision après avoir reçu un mèl anonyme lui indiquant que cette société allait fermer. Après quelques recherches, il est apparu que deux courriers électroniques mensongers avaient été envoyés depuis un poste informatique situé dans les locaux de la banque BNP *Paribas*. La société lésée demanda donc à la banque d'obtenir la communication de toute information permettant l'identification de l'expéditeur du message. En l'absence de réponse, elle décida de saisir la justice sur le fondement des articles 43-7 et 43-9 de la loi du 30 septembre 1986, applicables à l'époque des faits.

[9] Article 6-I, 1° de la LCEN « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens* ».

[10] Article L. 34-1 du Code des postes et des télécommunications : « *I. - Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic....* ».
Article L. 32-15° : *« On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ».*

[11] Délibération de la CNIL n°2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme : *Cnil.fr*, <http://www.cnil.fr/index.php?id=1883>.

[12] *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/cri/2005-2006/20060078.asp>.

de l'intérieur a pu indiquer que « *Les mairies, les universités, les bibliothèques ne sont pas concernées en principe, car leur activité ne consiste pas principalement à proposer des connexions Internet au public* ». Dans le même temps cependant, le Ministre a précisé que si l'on signalait aux autorités compétentes « *que telle université ou telle bibliothèque devenait une sorte de cybercafé déguisé, alors elle pourrait entrer dans le champ des personnes soumises à cette obligation de conservation de données au titre de leur activité accessoire* ». A cette occasion, le Ministre a fait allusion à Mohammed Atta, le chef des commandos kamikazes du 11 septembre 2001, « *qui avait entretenu une partie de son réseau à partir des postes Internet que l'université de Hambourg mettait à disposition de ses étudiants* », ainsi qu'à l'affaire *Reid* dans laquelle « *il a été prouvé que l'individu utilisait des cybercafés et une borne de connexion de l'aéroport de Roissy* ».

Refusant de lister dans un décret les personnes visées par le dispositif, le gouvernement a préféré laisser au juge le soin d'apprécier, sur la base de ces indications, si le champ d'investigation doit être étendu ou non.

Ces imprécisions pourront s'avérer lourdes de conséquences dans la mesure où le non-respect de l'obligation de communication des données de connexion est sanctionné pénalement par l'article L. 39-3 du CPCE[13]. Le principe de légalité des délits et des peines impose pourtant au législateur de définir les infractions « *en termes suffisamment clairs et précis pour exclure l'arbitraire* »[14].

En décidant d'étendre le dispositif à d'autres professionnels en fonction des circonstances, le gouvernement ne répond pas à cette exigence de clarté et de précision et le renvoi à l'appréciation du juge n'est évidemment pas suffisant. Telle a été la position du Conseil constitutionnel dans sa décision du 5 mai 1998 rendue à propos de la loi sur l'entrée et le séjour des étrangers en France et le droit d'asile[15]. Il a en effet été décidé qu' « *en soumettant à l'appréciation du ministre de l'intérieur la "vocation humanitaire" des associations, notion dont la définition n'a été précisée par aucune loi et de la reconnaissance de laquelle peut résulter le bénéfice de l'immunité pénale en cause, la disposition critiquée fait dépendre le champ d'application de la loi pénale de décisions administratives ; que, dès lors, nonobstant le pouvoir du juge pénal d'apprécier, conformément aux dispositions de l'article 111-5 du code pénal, la légalité de tout acte administratif, ladite disposition porte atteinte au principe de légalité des délits et des peines et méconnaît l'étendue de la compétence que le législateur tient de l'article 34 de la Constitution* ».

Une autre remarque mérite également d'être faite à ce stade. Les acteurs qui, à côté de leur activité principale, proposent un accès au réseau Internet, notamment par l'intermédiaire du réseau Wi-Fi, qu'il s'agisse des cybercafés, des restaurants, hôtels ou compagnies de transport, sont assimilés à des opérateurs de communication électronique c'est-à-dire, à des services de la société de l'information, tels qu'ils sont définis dans deux directives européennes de 1998[16]. Cette définition couvre les services « *fournis, normalement contre rémunération, à distance au moyen d'équipement électronique de traitement (y compris la compression numérique) et de stockage des données, à la demande individuelle d'un destinataire de services* ».

---

[13] « *I. - Est puni d'un an d'emprisonnement et de 75000 € d'amende le fait pour un opérateur de communications électroniques ou ses agents :*

1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise ».

[14] Décision n° 80-127 DC des 19 et 20 janvier 1981. Loi renforçant la sécurité et protégeant la liberté des personnes : *Conseil-constitutionnel.fr*, <http://www.conseil-constitutionnel.fr/decision/1980/80127dc.htm>.

[15] *Conseil-constitutionnel.fr*, <http://www.conseil-constitutionnel.fr/decision/1998/98399/98399dc.htm>.

[16] La définition des services de la société de l'information figure dans la directive 98/34/CE du Parlement européen et du Conseil 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 et dans la directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel.

Ainsi, les services qui ne comporteraient pas de traitement et de stockage des données et qui ne seraient pas fournis « *à distance* » , même s'ils impliquent l'utilisation de dispositifs électroniques, ne peuvent être qualifiés de services de la société de l'information. Les cybercafés, dans lesquels la prestation est fournie en présence physique des utilisateurs, ne peuvent donc êtres qualifiés d'opérateurs de communications électroniques.

Ils n'en demeurent pas moins astreints aux mêmes obligations de conservation des données de connexion.

B. L'obligation de « différer » à l'effacement des données de connexion

Dans sa version actuelle, l'article L. 34-1 du Code des postes et des communications électroniques prévoit l'effacement des données de connexion par les opérateurs, ainsi qu'un certain nombre d'exceptions, dont la conservation des données techniques pour les besoins des enquêtes. Le deuxième paragraphe de cet article dispose en effet qu'il « *peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques* ».

Cependant, en l'absence de décret d'application fixant la nature et le délai de conservation de ces données, cette disposition est difficilement applicable aux opérateurs. Certes, il a été constaté que ceux-ci conservent déjà certaines de ces données et les transmettent au juge sur la base de volontariat. La crainte était cependant que les cybercafés ainsi que les autres prestataires visés par le nouveau dispositif ne soient pas aussi diligents.

C'est la raison pour laquelle un amendement n° 11 tendant édicter une véritable obligation de conservation des données de connexion a été adopté. L'objectif du gouvernement est ici de clarifier la portée du nouveau dispositif législatif. Le projet de loi prévoit donc de modifier l'article L. 34-1 du CPCE afin d'imposer à toute personne offrant une connexion à Internet à destination du public « *de différer pour une durée maximale d'un an aux opérations tendant à effacer ou rendre anonyme certaines catégories de données techniques* »[17].

En outre, le Ministre de l'intérieur s'est engagé à soumettre rapidement le décret d'application de ce dispositif au Conseil d'État afin qu'il puisse être publié au plus tard, en janvier 2006.

Le projet de décret prévoit, dans sa rédaction actuelle, un certain nombre de données qui devront être conservées :

- les informations permettant d'identifier l'utilisateur ;
- les données relatives aux équipements terminaux de communications utilisés ;
- les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- les données permettant d'identifier le ou les destinataires de la communication.

Le contenu des courriers électroniques ainsi que les données de navigation (adresses des pages Internet visitées) ne sont donc pas concernées. L'obligation vise seulement les données de trafics permettant de connaître l'heure et la durée d'une connexion Internet, ainsi que le numéro de protocole Internet utilisé pendant cette communication (adresse « IP »). Cependant, avec la généralisation des offres au haut débit, le nombre d'adresses IP utilisées simultanément a considérablement augmenté ces dernières années, ce qui a conduit à les mutualiser. Dès lors, comment identifier chaque internaute ?

[17] Nous rappellerons que le non-respect de cette obligation est sanctionné pénalement par l'article L. 39-3 du CPCE.

La solution consistant à accéder aux tables de translation[18] pose problème car elle conduit à prendre connaissance des données de contenu. En effet, l'adresse du site Internet visité par l'internaute y est stockée, 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 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* ». Dès lors, en cas de recours à une technique de translation d'adresses, la seule solution acceptable juridiquement serait que le prestataire procède lui-même à l'identification de l'utilisateur et seul le résultat de l'opération devrait alors être transmis aux autorités[19].

Par ailleurs, une interrogation subsiste sur l'identification de la personne utilisant un système d'accès sans abonnement. En effet, la spécificité des cybercafés est d'offrir des accès à l'Internet sans possibilités d'identifier les clients, ni de cerner les connexions individuellement. En outre, pour renforcer la confidentialité des navigations d'un client à un autre et la sécurité des postes clients, toutes les traces sont souvent effacées sur le disque dur du terminal. Quant à la technologie Wi-Fi, elle repose sur une intermédiation entre le titulaire effectif d'un accès au réseau (la borne Wi-Fi) et l'utilisateur final qui est relié à celle-ci par une liaison radio rendant difficile toute identification.

Cependant, l'article L.34-1 du CPCE dispose que le décret d'application devra définir ces obligations « *selon l'activité des opérateurs et la nature des communications* », ce qui conduira peut-être à tenir compte des spécificités de chaque type d'opérateur ou de « *fournisseur de connexion* » concerné[20].

Il faut néanmoins reconnaître que la conservation de données de connexion d'utilisateurs non identifiés nuance considérablement l'efficacité d'un tel dispositif.

Enfin, l'obligation de conservation n'est pas sans poser d'autres difficultés. Premièrement, selon la CNIL, elle ferait peser une charge considérable sur les personnes visées (cybercafés, restaurateurs, compagnies de transport, etc.), que celles-ci auront sans doute du mal à mettre en œuvre. Par ailleurs, cette obligation pourrait ralentir substantiellement le développement de nouvelles solutions techniques d'accès au réseau Internet, comme le Wi-Fi[21].

Quoi qu'il en soit, les « *fournisseurs de connexion* » visés par le dispositif ne seront soumis qu'à cette seule obligation de conservation des données de connexion. En effet, la définition de l'opérateur de communications électroniques qui nous est donnée à l'article L. 32-15° du Code des postes et des communications électroniques[22] n'a pas été modifiée. Il faut en déduire qu'à l'avenir, ces acteurs ne seront pas considérés comme des opérateurs de communications électroniques. Ils n'auront donc pas, par exemple, à informer les utilisateurs concernés de l'existence de moyens techniques mis à leur disposition pour restreindre l'accès ou encore, l'obligation de filtrer certains contenus préjudiciables pour les tiers[23].

Ceci étant, opérateurs et « *fournisseurs de connexion* » devront se soumettre à une nouvelle procédure de communication des données vis-à-vis des services de police et de gendarmerie.

---

[18] La translation consiste 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 l'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.

[19] Benoît Tabaka, « Les nouveaux défis de la conservation des données de connexion », *Juriscom.net*, 25 avril 2005, <http://www.juriscom.net/documents/resp20050425.pdf>.

[20] Ainsi pour les cybercafés, il serait possible de demander aux gestionnaires de recueillir l'identité de l'ensemble des utilisateurs.

[21] Délibération de la CNIL n°2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme, *Cnil.fr*, <http://www.cnil.fr/index.php?id=1883>.

[22] *Legifrance.gouv.fr*, <"http://www.legifrance.gouv.fr/WAspad/UnArticleDeCode?commun=CPOSTE&art=L32">.

[23] Sur les obligations pesant sur les fournisseurs d'accès à Internet, voir le dossier du Forum des droits sur l'internet sur la loi pour la confiance dans 'économie numérique : *Foruminternet.org*, <http://www.foruminternet.org/publications/lire.phtml?id=734>.

II. Le droit de communication des données de connexion

La communication des données de connexion par les opérateurs et par les « *fournisseurs de connexion* » s'inscrit dans une procédure administrative (A), en dehors de tout contrôle du juge et de la CNIL (B).

A. Une procédure administrative prévue pour une durée déterminée

L'obligation d'inscrire systématiquement les demandes de communications de données de connexion dans un cadre judiciaire est apparue trop contraignante pour le gouvernement, selon lequel « *la plupart des vérifications nécessaires en pratique découlent d'éléments recueillis en amont de toute procédure judiciaire* »[24].

Le projet d'article 5 tend ainsi à permettre aux seuls services de police spécialisés dans la lutte contre le terrorisme de se faire communiquer, dans un cadre juridique administratif, certaines données de connexion, à l'exclusion de toute donnée de contenus. Les demandes seraient adressées par ces services aux opérateurs et prestataires mentionnés au I de l'article L. 34-1 du Code des postes et des télécommunications et aux 1° et 2° du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Les données techniques envisagées seraient celles « *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 appelants, la durée et la date des communications* ».

Les demandes ne pourraient être présentées que par les agents individuellement habilités des services d'enquêtes spécialement désignés pour lutter contre le terrorisme.

Afin de garantir le respect de la finalité du dispositif, certaines mesures sont envisagées :

- la motivation, la centralisation et l'enregistrement des demandes par l'*unité de coordination de la lutte antiterroriste* (UCLAT) ;
- la validation par une personnalité qualifiée, placée auprès du Ministre de l'intérieur et désignée par la *Commission nationale de contrôle des interceptions de sécurité* (autorité administrative indépendante régie par la loi n° 91-646 du 10 juillet 1991) sur proposition du Ministre de l'intérieur, pour une durée de trois ans renouvelable ;
- le contrôle *a posteriori* de cette même commission nationale à laquelle les demandes seront communiquées et qui pourra à tout moment procéder d'elle-même à des contrôles. En cas de manquement aux règles définies par l'article 5 ou, en cas d'atteinte aux droits et libertés, la commission pourra saisir le Ministre de l'intérieur d'une recommandation. Celui-ci disposera alors d'un délai de quinze jours pour lui faire connaître les mesures prises pour remédier aux manquements constatés ;
- l'établissement d'un rapport annuel d'activité.

Il est également prévu que les frais éventuels supportés par les opérateurs et les « *fournisseurs de connexion* » mis à la charge de l'Etat soient imputés sur le budget de fonctionnement du service demandeur. Cette mesure fait suite à une décision du Conseil constitutionnel du 28 décembre 2000 rendue à propos des dépenses réalisées par les opérateurs privés à la sauvegarde de l'ordre public[25].

---

[24] Débats du 23 novembre 2005, *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/cri/2005-2006/20060076.asp>.

[25] Décision n° 2000-441 DC - 28 décembre 2000 : *« Considérant que, s'il est loisible au législateur, dans le respect des libertés constitutionnellement garanties, d'imposer aux opérateurs de réseaux de télécommunications de mettre en place et de faire fonctionner les dispositifs techniques permettant les interceptions justifiées par les nécessités de la sécurité publique, le concours ainsi apporté à la sauvegarde de l'ordre public, dans l'intérêt*

Les modalités d'application de ces dispositions devraient être fixées par décret en Conseil d'Etat, après avis de la *Commission nationale de l'informatique et des libertés* et de la *Commission nationale de contrôle des interceptions de sécurité*.

Enfin, l'article 15 du projet de loi contient une « *clause de rendez-vous* ». Il y est en effet prévu que les dispositions des articles 3, 5 et 8 du texte seront applicables jusqu'au 31 décembre 2008.

B. La mise à l'écart du juge et de la CNIL

Ce droit de communication des services de police et de gendarmerie, même exercé sous le contrôle d'une personnalité qualifiée et d'une autorité administrative et indépendante, n'en demeure pas moins hors de portée de l'autorité judiciaire. Ce choix peut surprendre car l'obligation ici faite aux opérateurs ainsi qu'aux « *fournisseurs de connexions* » déroge aux principes fondamentaux de protection des libertés individuelles. Plusieurs amendements ont donc été présentés en vue de prévoir l'intervention d'un magistrat au cours des procédures de communication.

Les amendements n° 100 et 111[26] de M. Hunault prévoyaient ainsi que les demandes des services compétents soient autorisées par un juge des libertés et de la détention pour une durée maximum de quinze jours renouvelable une fois. L'utilisation des données ainsi collectées était faite sous son contrôle et il devait ensuite transmettre pour information les demandes des agents et les décisions prises par lui à la personnalité qualifiée placée auprès du Ministre de l'intérieur et à la *commission nationale de contrôle des interceptions de sécurité.* Cette personnalité qualifiée, un magistrat encore, devait être désignée conjointement par le Ministre de la justice et le Ministre de l'intérieur.

Cette procédure, inspirée de celle qui existe en matière d'autorisation d'interceptions de sécurité n'a pas reçu un écho favorable auprès des parlementaires et du gouvernement, le rapporteur du texte ayant estimé que « *le projet de loi met en place un système de police administrative préventive* », et qu'il n'y avait aucune raison de faire intervenir un magistrat.

On peut comprendre que l'intervention d'un magistrat au stade de l'autorisation des demandes de communication puisse paraître contraire à l'esprit du texte dont le Ministre de l'intérieur a pu préciser que l'objectif était d' « *agir en amont des attentats potentiels en permettant une meilleure collecte des renseignements* », tout en reconnaissant par ailleurs la difficulté de l'exercice « *car alors se pose la question d'une démarche administrative et non pas simplement d'une démarche judiciaire. En effet, il va de soi qu'il faut qu'un acte ait été commis ou commencé à l'être pour qu'un juge soit désigné. Or le travail de la police et de la gendarmerie, c'est justement de faire en sorte que cet acte n'ait pas lieu.* »[27]

Cet argument vient pourtant en contradiction avec l'adoption d'un amendement n° 12, présenté par M. Marsaud, tendant à codifier les dispositions de l'article 5 au sein du Code des postes et des communications électroniques et de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, et qui a également pour conséquence d'autoriser la réquisition des données techniques, non seulement pour la prévention mais aussi pour la répression du terrorisme.

Encore plus surprenante est l'idée d'une intervention de l'autorité judiciaire, au seul stade de la sanction d'une infraction. Le Conseil constitutionnel a en effet pu indiquer dans une décision n° 93-323 du 5 août 1993 relative à la loi sur les contrôles et vérifications d'identité[28] « *qu'il revient à l'autorité judiciaire gardienne de la liberté individuelle de contrôler en particulier les conditions relatives à la légalité, à la réalité et à la pertinence des raisons ayant motivé les opérations de contrôle et de vérification d'identité ; qu'à cette fin il lui appartient d'apprécier, s'il y a lieu, le comportement des*

---

général de la population, est étranger à l'exploitation des réseaux de télécommunications ; que les dépenses en résultant ne sauraient dès lors, en raison de leur nature, incomber directement aux opérateurs ».

[26] Voir la liste complète des amendements déposés en première lecture à l'Assemblée Nationale : *Assemblee-nationale.fr*, <http://recherche.assemblee-nationale.fr/amendements/resultats.asp?NUM_INIT=2615>.

[27] *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/cri/2005-2006/20060077.asp>.

[28] *Conseil-constitutionnel.fr*, <http://www.conseil-constitutionnel.fr/decision/1993/93323dc.htm>.

personnes concernées ».

Cette mise à l'écart du juge dans le nouveau dispositif de communication des données de connexion n'est donc pas très heureuse, elle laisse entendre que l'autorité judiciaire n'est pas capable d'intervenir dans l'urgence au stade de la prévention. Pire encore, c'est une négation de son rôle en matière de protection des libertés individuelles.

Dans les amendements qui ont été soutenus à l'Assemblée nationale le 24 novembre 2005[29], il a également été proposé que la personnalité qualifiée soit un magistrat nommé conjointement par le Garde des sceaux et le Ministre de l'intérieur ou, que celle-ci soit nommée sur avis conforme de la CNIL pour garantir davantage d'impartialité. Contre toute attente, Il a été objecté par le rapporteur du projet de loi qu' « *Il n'entre pas dans les missions de la CNIL de donner son avis pour ce type de nomination. La CNCIS serait plus compétente* ». Cet argument peut surprendre en effet, puisqu'à la lecture de la loi du 10 juillet 1991, consacrée en partie à la création de la *Commission nationale de contrôle des interceptions de sécurité*, on ne trouve pas plus d'indications sur la compétence de cette autorité administrative indépendante en matière d'avis sur la désignation de telle ou telle personnalité qualifiée que pour la CNIL dans la loi du 6 janvier 1978. Il n'était donc pas impossible d'associer la CNIL à cette désignation, il aurait même été souhaitable qu'elle le soit, compte tenu de la nature des données personnelles ainsi collectées et transmises aux autorités sans intervention du juge.

Par ailleurs, la CNIL souhaitait que les garanties procédurales soient complétées pour prévoir que l'enregistrement des demandes de communication lui soit également communicable. Les amendements n° 90 de MM. Dray et Floch et n° 71 de M. Mamère, Mme Billard et M. Yves Cochet déposés en ce sens n'ont pas été adoptés. Il était pourtant indiqué avec beaucoup de clairvoyance que l'intervention de la CNIL aux côtés de la *Commission nationale de contrôle des interceptions de sécurité* « *se justifie d'autant plus que le résultat de la collecte dans les « cybercafés » est destiné à nourrir des fichiers dont la CNIL assure la surveillance* »[30].

Conclusion

La volonté du législateur de modifier dans l'urgence le régime juridique de la conservation et de la communication des données de connexion mérite d'être relevé avec intérêt. Sans doute, le gouvernement sait mieux que quiconque les risques d'attaques terroristes qui menacent la sécurité nationale. Néanmoins, les nombreuses imprécisions et les imperfections du projet de loi, notamment la mise à l'écart du juge et de la CNIL, appellent à formuler de sérieuses réserves sur l'efficacité de ce dispositif et sur la garantie de nos libertés individuelles. Comme a pu l'exprimer le député Michel Vaxès au cours des débats, « *ce texte fait une concession à ceux-là mêmes qu'il veut combattre* ».

Sans doute, l'urgence aurait été de réunir le Parlement autour des conclusions du livre blanc sur la sécurité intérieure face au terrorisme ou, à tout le moins, de publier le décret d'application de la loi sur la sécurité quotidienne du 15 novembre 2001.

Adopté à une large majorité à l'Assemblée nationale (373 voix pour, 27 contre), le projet de loi sera en discussion au Sénat en séance publique les 15 et 16 décembre prochains.

Notons que parallèlement au débat français, les instances communautaires traitent également de ces questions. La Commission a présenté le 21 septembre 2005 une proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public et modifiant la directive 2002/58/CE.

Cette directive, qui a vocation à s'appliquer aux données relatives au trafic et aux données de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré à l'exclusion du contenu des communications électroniques, prévoit par ailleurs des durées de conservation d'un an pour les

[29] *Assemblee-nationale.fr*, <http://www.assemblee-nationale.fr/12/cri/2005-2006/20060079.asp>.
[30] [30] Voir la liste complète des amendements déposés en première lecture à l'Assemblée Nationale : *Assemblee-nationale.fr,* <http://recherche.assemblee-nationale.fr/amendements/resultats.asp?NUM_INIT=2615>.

données relatives au trafic concernant la téléphonie mobile et la téléphonie fixe, et de six mois pour les données relatives au trafic concernant l'utilisation d'internet. Elle a été transmise au Parlement pour un premier examen fixé au 13 décembre 2005.

F. B.