TÉLÉCOM et MANAGEMENT
SudParis
Département droit, économie, finances et sociologie (IDEFIS)

Étude de droit comparé en matière d'organismes de contrôle pour les interceptions téléphoniques

Réalisée par Claudine GUERRIER, professeur

Janvier 2009

INTRODUCTION :

Le secret de la correspondance intéresse le juriste depuis plusieurs siècles. Sous Louis XIV, dans un siècle où les vertus de la démocratie contemporaine étaient inconnues, la correspondance était évoquée officiellement avec componction. Ce respect s'explique par la religiosité de la société paysanne et par l'influence des valeurs religieuses dans l'aristocratie et la bourgeoisie. Pendant la période révolutionnaire, une morale laïque, inspirée du christianisme, se substitue à l'ancienne obligation de respecter l'église catholique et ses ordonnancements

. Avec Napoléon 1er, l'alliance entre le trône et l'Autel se reconstitue. Le code civil en tient compte. L'administration des postes se doit de protéger le secret de la correspondance transportée. Dans le code des Postes et des Communications électroniques, la question est abordée.

Le secret des correspondances est inviolable, mais des dérogations sont prévues :

-Les Postes doivent communiquer aux autorités judiciaires qui en font la demande en matière pénale les changements de domicile dont elle a connaissance.

Elles sont au service des juges d'instruction et participent à leur façon à la lutte contre la fraude fiscale.

-Un contrôle douanier est autorisé, pour les envois frappés de prohibition à l'importation, à l'exportation[1].

Par le moyen des télécommunications ou des communications électroniques, la correspondance est un échange de paroles[2]ou de signes[3].

Le terme « communications électroniques » est utilisé au sein de l'Union européenne depuis les directives du 7 mars 2002 : la directive cadre, la directive sur le régime déclaratif des communications électroniques, la directive sur l'accès et l'interconnexion en matière de communications électroniques, la directive sur le service universel des communications électroniques, la décision du 7 mars 2002 sur le spectre de fréquences. Le concept de communications électroniques correspond à la convergence des technologies : téléphonie, internet, informatique, audiovisuel. Les directives sont transposées en juillet 2003. Depuis la mi-2003 au sein de l'Union européenne, et en France, depuis 2004, on parle d'interceptions de communications électroniques. Ailleurs, on continue à parler d'interceptions de télécommunications.

Pendant longtemps, la téléphonie est un privilège. Les titulaires d'abonnements téléphoniques constituaient une minorité, au dix-neuvième siècle et dans la première partie du vingtième siècle. Aujourd'hui, presque tous les Français et résidents en France ont un abonnement, au fixe ou (et) mobile et beaucoup de Français ont accès à Internet. A l'étranger, dans tous les pays développés, l'accès à la téléphonie et à Internet est très répandu.

Les interceptions de télécommunications et de communications électroniques constituent donc une exception au principe du secret de correspondance.

La licéité est précisée au regard de la protection de la vie privée. Les modalités d'interceptions légales sont indiquées avec clarté. Ce processus s'applique à l'Etat-nation démocratique, qu'il se situe dans la sphère internationale ou la sphère européenne. Dans la mesure où le droit humanitaire est en cause, des conventions internationales ont été élaborées et la hiérarchie des normes imposée.

[1] Les envois sont passibles de droits ou de taxes perçus par le service des douanes ou soumis à des restrictions ou formalités à la sortie (exportation)

[2] Téléphonie fixe ou mobile

[3] Méls

La Déclaration universelle des droits de l'homme de 1948[4] est une référence incontournable, même si elle n'est pas toujours appliquée : elle évoque la protection de la vie privée. L'article 17 du pacte international relatif aux droits civils et politiques des Nations unies du 16 décembre 1966 reprend les mêmes notions sous une présentation quasi identique[5]. Ces deux textes font référence au cercle privé.

Le droit français mentionne le respect de la vie privée dans l'article 9 du Code civil[6] et dans la loi du 17 juillet 1970, soucieuse de renforcer la protection des libertés individuelles. La vie privée n'est cependant pas définie dans la loi de 1970. La jurisprudence fait apparaître, comme composantes de la vie privée, les opinions politiques, la dépouille mortelle d'une personne. Le droit pénal vise l'intimité de la vie privée, définie de façon restrictive par une partie de la doctrine (écrits de MM.Levasseur, Lindon, Bécourt) et de la jurisprudence (vie conjugale et sentimentale, en excluant parfois les aspects matériels de cette vie conjugale et sentimentale) ou de façon un peu plus extensive (vie familiale et certains événements de l'existence d'une personne). Le droit civil obéit à une finalité plus large, qui englobe les opinions politiques et religieuses, les éléments d'identification d'une personne, la santé, la vie professionnelle, dans des cas précis. Quant à l'intimité, elle implique, en droit pénal, pour reprendre la classification de Mme Lolies[7], d'ailleurs favorable à une conception relativement vaste tant sur le plan pénal que sur le plan civil, l'intimité personnelle, l'intimité relationnelle, l'intimité corporelle.

La Convention européenne des droits de l'homme, à travers son article 8, donne une légitimité à la sphère privée.

Quant à l'interception, elle est définie par le dictionnaire[8]comme le « fait de s'emparer de ».Il y a captation. L'interception est intentionnelle, volontaire, lucide. La cessation de l'interception induit une réflexion, puisque la finalité en est que la captation disparaît avec elle. En France, la loi de 1991 est relative « aux interceptions par voie de télécommunications »[9], puis aux interceptions par voie de communications électroniques. Elle s'intéresse aux interceptions téléphoniques, et aux interceptions réalisées par d'autres moyens de communication.

PREMIERE PARTIE : LE CONTRÔLE DES INTERCEPTIONS DE TELECOMMUNICATION

Les interceptions de télécommunication, dans les Etats occidentaux ont connu deux phases distinctes : la première tend à limiter le nombre des interceptions de télécommunication ; elle établit des organismes de contrôle ; elle correspond aux deux dernières décennies du vingtième siècle. La deuxième s'inscrit dans le courant sécuritaire qui recourt à la vidéosurveillance, à la biométrie. Les personnes publiques utilisent de plus en plus fréquemment les interceptions de télécommunication (téléphone, méls). Cependant, les organismes de contrôle subsistent ; ils constituent l'un des rares freins à l'idéologie sécuritaire qui se manifeste à la fin du vingtième siècle et au début du vingt-et-unième siècle.

---

[4] L'article 12 de la Déclaration universelle des droits de l'homme du 12 décembre 1948 précise : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions »

[5] L'article 17 du 16 décembre 1966 :

« 1.Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2.Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes »

[6] « Chacun a droit au respect de sa vie privée »

[7] Isabelle Lolies « La protection pénale de la vie privée », Presses universitaires d'Aix-Marseille, 1999

[8] Petit Larousse

[9] Loi n°91.64646 du 10 juillet 1991. Titre I : Des interceptions ordonnées par l'autorité judiciaire Titre II : Des interceptions de sécurité

Ces organismes de contrôle ont été mis en place en Europe à l'initiative de la CEDH, qui applique la Convention européenne de sauvegarde des droits de l'homme et qui s'intéresse tout particulièrement à l'article huit de la Convention, relatif au respect de la vie privée et au secret des correspondances. Aux USA, c'est la culture juridique fédérale qui est prise en compte.

PREMIERE SOUS-PARTIE / LA MISE EN PLACE DES ORGANISMES DE CONTRÔLE

I) Le rôle de la CEDH dans l'établissement des organismes de contrôle en matière d'interceptions de télécommunication : les pays membres du Conseil de l'Europe qui ont ratifié la Convention européenne de sauvegarde des droits de l'homme et notamment l'article 25 [10]de la Convention sont assujettis à la jurisprudence de la CEDH et sont tenus de l'appliquer.

A) L'affaire Klass et autres[11] :

1) Les faits :

Gerhard Klass, Peter Lubberger, Jürgen Nussbuch, Hans-Jürgen Pohl et Dieter Selb avaient saisi la Commission européenne des droits de l'homme le 11 juin 1971 en vertu de l'article 25 de la Convention.

Les requérants sont des ressortissants de la République fédérale d'Allemagne. Ils arguent de ce que l'article 10, alinéa 2, de la Grundgesetz et la loi du 13 août 1968 (Gesetz zur Beschränkung des Briefs, Post und Fermelde Geheimisses), promulguée en vertu de cette disposition, est contraire à la Convention. Ils admettent que l'Etat allemand a le droit de recourir à des mesures de surveillance. Ils attaquent la législation parce qu'elle n'oblige pas les autorités à aviser a posteriori les intéressés et qu'elle exclut tout recours contre les tribunaux. Ils avaient auparavant épuisé les voies de recours internes, ayant été déboutés par la Cour constitutionnelle fédérale.

Après la fin de la seconde guerre mondiale, les puissances d'occupation en Allemagne s'étaient chargées de la surveillance de la correspondance sur l'ancien territoire du Reich. Le gouvernement de la République fédérale d'Allemagne obtint par la suite de substituer aux droits des puissances son droit interne.[12]La loi du 24 juin 1968 est adoptée. Elle indique les motifs susceptibles de permettre les écoutes et les enregistrements téléphoniques. La surveillance n'est licite que si l'établissement des preuves ne peut être obtenu par aucun autre moyen. L'intéressé n'est pas prévenu des restrictions le concernant mais, depuis un arrêt de la Cour constitutionnelle fédérale, l'autorité responsable doit signaler les restrictions dès que la notification peut se faire sans compromettre le but de l'interception. Soulignons que les autorités responsables ont donné une interprétation restrictive de cet arrêt, ne voulant pas faire courir le moindre risque à la sécurité nationale.

MM.Lass, Lubberger, Nussbuch, Pohl et Selb estimaient avoir été l'objet d'écoutes téléphoniques, mais n'avaient aucune possibilité de le prouver. Ils n'ont pas hésité cependant à intenter des actions en justice. Ils ont été déboutés, notamment par la Cour constitutionnelle fédérale qui a souligné : « Pour pouvoir

[10] Cet article de la Convention permet les requêtes individuelles, quand le requérant a épuisé les voies de recours interne.

[11] CEDH, Affaire Klass et autres c.RFA, 6 septembre 1978

[12] Ce processus fut facilité par la cohabitation antagoniste de la RDA et de la RFA. Cette dernière, pour l'OTAN, se devait d'avoir un gouvernement doté de tous les attributs du pouvoir

former un recours constitutionnel contre une loi, il faut alléguer que cette dernière, et non un acte d'exécution, viole un droit fondamental »

De nombreux juristes allemands ont d'ailleurs prêté des intentions malicieuses à MM.Klass, Lubberger, Nussbuch, Pohl et Selb, prétendant qu'ils ne cherchaient pas à obtenir la protection des juridictions allemandes, mais à tester la réactivité du système à l'occasion de l'application de la loi du 24 juin 1968. Ces allégations, au demeurant, ne reposent sur aucune preuve.

Il est néanmoins certain que ces citoyens allemands étaient animés par une farouche détermination. Ainsi, après l'arrêt de la Cour constitutionnelle fédérale, ils saisissent la Cour européenne des droits de l'homme. De facto, ils considèrent avoir démontré par l'absurde que la loi de 1968 exclut les recours.

Le gouvernement allemand, de son côté, a fait valoir que les requérants n'avaient pas un intérêt pour agir : ils ne pouvaient se prétendre victimes. MM.Klass, Lubberger, Nussbuch, Pohl, Selb ne savaient pas s'ils avaient été l'objet d'écoutes téléphoniques. Ils ne prétendaient pas avoir établi une violation individuelle de leurs droits. Ils cherchaient, sur « la base de l'éventualité purement hypothétique d'être soumis à une surveillance, un contrôle de la législation allemande, prétendument litigieuse ».

La commission et la Cour européenne des droits de l'homme sont, selon le gouvernement, incompétents. Leur rôle est de contrôler la bonne application de la Convention quand un requérant s'estime victime d'une violation de ses droits et n'a pu obtenir satisfaction par les voies de recours internes, non pas d'entrer dans des arguties juridiques qui se dissimulent sous des arguments juridiques. La presse allemande de l'époque reflète[13]une certaine irritation contre ces hommes qui auraient l'outrecuidance de jauger la démocratie allemande.

2) Le droit

La commission estime que la Cour est compétente pour déterminer si les requérants peuvent se prétendre victimes. Les membres de la commission estiment qu'il ne faut pas regarder les requérants comme de simples victimes hypothétiques.

La question principale est la suivante : la Cour européenne des droits de l'homme doit-elle priver quelqu'un de la faculté d'introduire une requête parce que le caractère secret (et volontairement secret) des mesures litigieuses l'empêche de signaler une mesure concrète qui le toucherait spécifiquement ?

La finalité de la Convention européenne de sauvegarde des droits de l'homme est la protection de l'individu. Si le droit empêche un individu de prouver qu'il a subi un abus, la commission est d'avis qu'il faut interpréter largement le recours individuel. La commission indique que MM.Klass, Lubberger, Nussbuch, Pohl et Selb peuvent se présenter comme des victimes directes d'une violation de leurs droits. Les clauses procédurales de la Convention sont appliquées de façon à rendre efficace et non virtuel le système de requêtes individuelles.

La cour européenne accepte qu'un individu puisse, sous certaines conditions, se prétendre victime d'une violation entraînée par une législation sans devoir prouver que la règle lui a été appliquée. Il y a donc lieu de rechercher si, en raison de la législation contestée, les requérants ont été victimes d'une violation. Cette jurisprudence est essentielle : elle donne une interprétation extensive du droit de requête individuelle, qui ne doit pas être oblitérée par des mesures internes (« les clauses procédurales »).

[13] Y compris dans les journaux à grand tirage Die Welt, Der Spiegel

MM.Klass, Lubberger, Nussbuch, Pohl et Selb estiment qu'il a été porté atteinte à l'article huit de la Convention qui protège la sphère privée et la correspondance.
La réponse de la Cour comprend deux types d'argumentations :

- La Cour indique que, quand un Etat établit une surveillance secrète dont les personnes intéressées ignorent l'existence et qui, de ce fait, est inattaquable, l'article huit risque d'être vidé de son contenu. Une dérive est envisageable. La législation de la RFA aurait institué une surveillance qui expose chacun au contrôle de sa correspondance postale et téléphonique. La commission et la Cour admettent toutes deux que les conversations, par voie de télécommunications, même si elles ne sont pas explicitement citées au paragraphe 1 de l'article huit, sont comprises dans les notions de « vie privée » et de « correspondance ». Les interceptions administratives sont dans le champ d'application de l'article huit et la CEDH est compétente pour examiner si les interceptions ne violent pas l'article huit de la Convention.
- L'ingérence est-elle justifiée par exception ? Les requérants estiment que les pouvoirs confiés aux autorités allemandes sont susceptibles d'induire des abus et ne peuvent constituer un moyen de défense légitime pour la protection de l'Etat démocratique[14]. La Cour examine la loi de 1968 pour déterminer si elle contient des garanties suffisantes contre des abus. Après un examen minutieux, la Cour ne perçoit, ne reconnait pas le danger de tels abus. L'article huit de la Convention n'a donc pas été violé.

Cet arrêt concerne l'ensemble des Etats européens démocratiques. La RFA avait institué une loi qui était afférente aux interceptions, non seulement aux interceptions judiciaires, mais aux interceptions administratives. En 1978, la majorité des autres Etats européens n'ont pas de législation, mais procèdent à des interceptions de sécurité. Ils n'ignorent plus désormais que la requête individuelle d'un ressortissant pourrait être jugée recevable et que l'absence de garanties, prévues par la loi allemande, mais inexistantes dans certains pays voisins, pourrait amener la Cour européenne à déclarer que l'article huit a fait l'objet d'une violation. La Cour peut déclarer que les citoyens d'un Etat voient leur vie privée atteinte par une ingérence infondée, dans le cadre d'interceptions administratives.
Dans son arrêt du 6 septembre 1978, la Cour a conclu que la législation de 1968 avait un but légitime : la défense de l'ordre, la prévention d'infractions pénales. La loi allemande a défini des conditions strictes dans l'application des mesures de surveillance, le traitement des renseignements recueillis et a institué des organismes de contrôle. Tout cela est souvent inopérant dans plusieurs autres Etats-nations européens.

B) L'arrêt Malone :

L'affaire a été déférée à la Cour par la commission européenne des droits de l'homme le 16 mai 1983. A l'origine, James Malone a saisi la commission le 19 juillet 1978 en vertu de l'article 25. La requête individuelle est dirigée contre le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

1) Les faits :

[14] Le concept de démocratie et d'Etat démocratique est au centre de la Constitution de la RFA. Cf. Paul Grossmann, Demokratie in Deutscland als Problem und Aufgabe, Don Bosco Verlag, 1976

James Malone fut, le 22 mars 1977, inculpé de plusieurs délits de recel de biens volés. Son procès aboutit à une relaxe sur plusieurs points. Lors d'un procès suivant, il sera acquitté pour insuffisance de preuves[15].
Lors du premier procès, l'avocat de l'accusation reconnaît que James Malone avait fait l'objet d'écoutes téléphoniques en vertu d'un mandat délivré par le ministre de l'Intérieur.
James Malone, après son acquittement, engagea une action civile contre le préfet de police du Grand Londres, devant la Chancery Division de la High Court car il considérait que l'interception, la surveillance et l'enregistrement de ses conversations téléphoniques étaient illicites (ils avaient été effectués sans son consentement[16]), même s'ils se fondaient sur un mandat du ministre de l'Intérieur. Malone fut débouté.
James Malone estime en fait que ses correspondances postales et téléphoniques sont interceptées depuis plusieurs années. Il ne dispose pas de preuves mais appuie sa conviction sur des problèmes de distribution, des indices d'ouverture de courrier, des bruits dans son téléphone fixe. James Malone pense, en outre, que sa ligne a été reliée à un instrument de « comptage ». Au moment de son inculpation, ses correspondants firent l'objet de perquisitions domiciliaires ; James Malone ne croit guère à des coïncidences.
En Grande-Bretagne, l'interception des communications se pratique depuis longtemps en vertu d'un mandat délivré par le ministre de l'Intérieur.
Devant la Chancery Division, le vice-président défendit le système des interceptions « à l'anglaise ». Le vice-président affirma qu'il n'existait pas de droit de propriété sur le texte d'une conversation téléphonique. James Malone ne peut donc prétendre qu'il a subi un préjudice dans la mesure où une atteinte aurait été portée à ses droits patrimoniaux[17]. L'écoute téléphonique pratiquée dans les locaux du Post-Office n'équivaut pas à une violation de domicile. James Malone n'est pas susceptible d'invoquer la violation de domicile.
Surtout, le droit anglais ne garantit aucun droit général à l'intimité, ni aucun droit à échanger chez soi des conversations téléphoniques sans intrusion de tiers. En conséquence, James Malone, ayant épuisé les voies de recours interne, saisit la Cour européenne des droits de l'homme. Il a eu connaissance des conclusions de l'arrêt Klass. Ces conclusions lui paraissent ouvrir une voie à une éventuelle reconnaissance de ses droits.
La commission et la CEDH ont admis qu'un requérant victime d'interceptions pouvait introduire un recours individuel même en l'absence de preuves de l'acte présumé illicite. Dans son cas, le fait est allégué. Dans l'affaire Klass, la loi allemande prévoyait des garanties en matière d'écoutes administratives. James Malone et ses avocats sont convaincus que des garanties comparables ne peuvent être reconnues dans l'Etat de droit britannique. Entre le dépôt de la requête de James Malone et l'arrêt de la CEDH, le gouvernement britannique a réfléchi sur la nécessité de léférer dans le domaine des interceptions de télécommunications. Dans son rapport de janvier 1981 au Parlement, la commission royale sur la procédure pénale se penche sur l'opportunité d'une loi[18].
Le gouvernement ne suit pas ces recommandations. Il considère que le système des écoutes administratives est fiable, qu'il est en conformité avec les grands principes du droit anglais. Il ne convient pas de modifier ce qui a fait preuve de son efficacité et de sa licéité.

2) Le droit :

[15] Le système anglais aboutit à beaucoup d'acquittements pour « insuffisance de preuves. Le concept de preuve est privilégié dans le droit anglais, surtout en matière pénale

[16] En droit français, la notion de consentement est également essentielle, cf.Blin, JCP, Pen-368-372, n°15, Chavanne, Revue sc.crim, 1971, p 614, Pradel, D, 1971, chr, p.111, n° 20, D., 1981, p.332, Vitu, Droit pénal spécial, p.1650

[17] En France, il n'existe pas davantage de droit de propriété sur le texte d'une conversation téléphonique. Cette dernière est protégée par les droits extra-patrimoniaux.

[18] Rapport de la Commission royale sur la procédure pénale, janvier 1981 : « Nous recommandons dès lors que la loi réglemente l'utilisation par la police de mécanismes de surveillance »

Le gouvernement britannique ne nie pas la réalité des faits allégués par James Malone. Il sait que l'arrêt Klass a conclu que les échanges par voie de télécommunications sont compris dans les notions de « vie privée » et de « correspondance » au sens de l'article huit. L'interception est une ingérence d'une autorité publique, qui peut se justifier au nom de l'intérêt général. Enfin le Royaume-Uni se félicite des arrêts Sunday Times et Silver[19] où la notion de loi au sens de la jurisprudence de la CEDH, admet le « common law » et le « statute law »[20].

La question posée est de déterminer si le droit interne du Royaume-Uni, dans la pratique des interceptions administratives, présente des « normes juridiques accessibles » et des garanties suffisantes. Les juristes britanniques défendent la licéité de leurs traditions.

La CEDH ne suit pas leurs arguments. La Cour considère que le droit anglais et gallois relatif à l'interception de communications pour les besoins de l'autorité publique est obscur, peu accessible.[21] Un degré minimal de sécurité juridique fait défaut. Les interceptions sont acceptables dans une société démocratique si elles ne sont pas abusives. En Grande-Bretagne, le risque d'abus existe. Les garanties sont insuffisantes ; notamment, il n'existe pas d'organisme de contrôle. Ces abus pourraient induire des conséquences négatives pour le corps social et la société démocratique.

La Cour européenne des droits de l'homme applique le même raisonnement à l'interception téléphonique et au procédé de comptage. Elle condamne le Royaume-Uni, dans l'affaire James Malone, pour violation de l'article huit de la Convention européenne de sauvegarde des droits de l'homme. Le Royaume-Uni est tenu d'en tirer les conséquences et d'adapter son droit, en matière d'interceptions administratives, à la jurisprudence de la CEDH.

A l'occasion de l'arrêt Malone est jointe au jugement l'opinion concordante du juge Perretti. Ce dernier pose la problématique de la société démocratique, de ses exigences sécuritaires, face aux innovations technologiques. Le juge Perretti est assez pessimiste quant au bien-fondé de l'équilibre entre les nécessités de l'ordre public et la protection des libertés individuelles. Il insiste sur le péril que connaissent les sociétés démocratiques face à la tentation permanente des pouvoirs publics de bien cerner la situation des citoyens. Les fichiers, informatisés ou non, existent partout. Le « profil » ou profilage est une pratique délétère trop répandue. Les interceptions sont un instrument de cette quête/ enquête permanente. L'interception est efficace. La plupart des Etats qui ont ratifié la Convention européenne de sauvegarde des droits de l'homme comprennent la nécessité de légiférer pour mettre un terme aux abus. Même lorsqu'il s'agit d'interceptions afférentes au contre-espionnage, à la sûreté de l'Etat, la plupart des législations peuvent prévoir des modalités de contrôle.

Selon M.Perretti, des contre-mesures apparaissent justifiées : droit à l'effacement, droit à la restitution des bandes. L'individu, selon M.Perretti, est menacé par le développement des technologies nouvelles, par la société de l'information.

« La mission du Conseil de l'Europe et de ses organes est d'empêcher l'instauration de régimes et de méthodes qui feraient des « Big Brothers » les maîtres de la vie privée des citoyens. L'évolution des technologies et de la géo-politique est venue confirmer les pires craintes de M.Perretti.

C) La France :

[19] CEDH, Arrêt Silver et autres, 13 mars 1983, série A, n° 61, p.32-33

[20] Esssentiellement, le droit romano-germanique

[21] Il est ainsi sujet à des analyses divergentes : Rapport décision Cour supérieure de justice du grand-duché du Luxembourg, 20 novembre 1980, Cour de cassation des Pays-Bas, 10 avril 1979 ; Louis Petiti, Gaz.Pal, 1981, 1, doc.236

A ratifié la Convention européenne des droits de l'homme et notamment son article 25 en 1981[22]. Deux affaires, Kruslin[23]et époux Huvig[24] ont joué un rôle éminent dans la condamnation du système d'interceptions français. Nous analyserons l'affaire Kruslin

1) Les faits :

Les 8 et 14 juin 1982, un juge d'instruction de Saint-Gaudens, saisi de l'assassinat d'un banquier, Jean Baron, délivre deux commissions rogatoires. Par la seconde, il charge le chef d'escadron commandant la section de recherches de la gendarmerie de Toulouse de placer sous écoute un suspect, Dominique Terrieux. Du 15 au 17 juin, la gendarmerie intercepte dix-sept communications. Jean Kruslin, hébergé alors par M. Terrieux, dont il utilise l'appareil, a participé à plusieurs d'entre elles et notamment à une conversation avec un homme qui l'appelle d'une cabine publique à Perpignan.

Lors de l'entretien, Jean Kruslin et son interlocuteur évoquent implicitement une autre affaire de meurtre, commise contre M.Peré. Le 18 juin, la gendarmerie appréhende M.Kruslin chez M.Terrieux, le met en garde à vue au titre de l'affaire Baron, puis l'interroge sur l'affaire Peré. Devant la Chambre d'accusation de la Cour d'appel de Toulouse, Jean Kruslin demande l'annulation de l'enregistrement de la communication litigieuse. Cette dernière a été réalisée dans le cadre d'une procédure qui ne le concerne pas. La Chambre d'accusation déboute Jean Kruslin. Rien n'interdit d'annexer à une procédure pénale les éléments d'une autre procédure à condition que la jonction ait un caractère contradictoire. Dans son pourvoi devant la Cour de cassation, Jean Kruslin se réfère à l'article huit de la Convention européenne de sauvegarde des droits de l'homme : « L'ingérence des autorités publiques dans la vie privée (…) doit être d'une qualité telle qu'elle use de termes clairs pour indiquer à tous, de manière suffisante, en quelles circonstances elle habilite la puissance publique à opérer pareille atteinte ». La Chambre criminelle de la Cour de cassation rend un arrêt de rejet le 23 juillet 1985[25].

2)Le droit :

Condamné, Jean Kruslin introduit une requête individuelle devant la CEDH. Il allègue que l'article 368 du code pénal prévaut sur l'article 81 du code de procédure pénale, lequel n'autorise pas les interceptions téléphoniques en termes exprès. Selon le gouvernement, il n'existe aucune contradiction entre l'article 368 du code pénal et l'article 81 du code de procédure pénale. Ce dernier ne dresse pas une liste limitative des moyens dont dispose le juge d'instruction.

En matière de droit, par les rapports de la commission, les juristes français savaient que la France serait condamnée. Certaines personnalités souhaitaient que l'on prévînt une condamnation par une réforme législative rapide. D'autres soutenaient qu'il « était urgent d'attendre » : une anticipation aurait conforté les arguments de la commission.

Dans son rapport afférent à l'affaire Kruslin[26], la commission admet (ce qui peut conforter les pratiques françaises) : « Les écoutes téléphoniques s'opèrent en France selon une pratique qui s'inspire des règles du code de procédure pénale régissant d'autres actes qui peuvent être décidés dans le cadre d'une enquête judiciaire ».

La Cour européenne des droits de l'homme[27], quant à elle, énumère les mesures imaginées par le droit français :

- nécessité d'une décision d'un juge d'instruction, magistrat indépendant ;
- contrôle exercé sur les officiers de police judiciaire par le juge d'instruction

[22] Décret n° 81 917 du 9 octobre 1981
[23] CEDH, Kruslin, 24 avril 1990, Dalloz, 1990, 353, Notes Pradel
[24] CEDH, époux Huvig, 24 avril 1990
[25] Cour de cassation, crim, 23 juillet 1985, Bull.crim, n° 275
[26] Du 14 décembre 1988
[27] CEDH, Kruslin c.France, 24 avril 1990

- contrôle éventuel du juge d'instruction de la part de la Chambre d'accusation, des juridictions du fond, de la Cour de cassation ;
- exclusion de l'artifice, des stratagèmes, dans la mesure où lesdits stratagèmes sont une provocation ;
- obligation de prendre en compte les droits de la défense, en particulier la confidentialité des relations entre l'avocat et le suspect ou inculpé.

Néanmoins, ces règles sont insuffisantes, pas assez protectrices des libertés individuelles.
La commission relève les principales lacunes :

- l'absence de délimitation précise et expresse des situations permettant l'interception de communications téléphoniques ;
- l'absence de référence à la gravité des faits (crimes, délits, peines encourues).

La Cour européenne des droits de l'homme entre encore davantage dans les détails :

- les catégories de personnes susceptibles d'être mises sous écoutes judiciaires ne sont pas indiquées ;
- aucune précision ne concerne la nature des faits. La limitation de la durée de l'interception n'apparaît pas
- l'absence de données sur l'établissement des procès-verbaux de synthèse est dommageable ;
- les données sur la conservation, l'effacement, la destruction d'enregistrement, après non-lieu[28]ou relaxe[29], sont occultées.

La procédure est donc insuffisamment protectrice. « Le droit français, écrit ou non écrit n'indique pas avec assez de clarté[30]l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré de sorte que les requérants n'ont pas joui du degré minimal de protection prévu par la prééminence du droit dans une société démocratique ».
Dans cette conclusion, la CEDH se réfère à l'arrêt Malone ; ce dernier précisait que la loi (au sens large du terme) doit définir l'étendue et les modalités d'exercice d'un pouvoir d'interception, avec une netteté suffisante, compte tenu du but légitime poursuivi, pour fournir à l'individu une protection adéquate contre l'arbitraire.
La France est donc condamnée ; elle doit payer une amende à M.Kruslin comme elle devra payer une amende aux époux Huvig. Surtout, elle doit revoir l'état de son droit en matière d'interceptions de télécommunications. Elle doit suivre les recommandations de la CEDH. Elle doit créer un organisme de contrôle des interceptions de sécurité. Pour suivre les injonctions de la CEDH, le législateur français s'inspire surtout du rapport Scmelck.
Peu après sa nomination en tant que premier ministre en 1981, Pierre Mauroy charge une commission d'étude placée sous la présidence du premier président de la Cour de cassation, Robert Schmelck, d'une mission d'investigation sur les écoutes téléphoniques. La commission comprend des parlementaires, des magistrats, des professeurs de droit, des hauts fonctionnaires.
La commission demande que les interceptions judiciaires soient dotées d'un régime légal que l'on puisse insérer dans le code de procédure pénale. Elle conclut à la licéité de l'interception judiciaire dans le cadre de l'information, mais aussi à la licéité d'interceptions judiciaires en cas de flagrance et d'urgence sur demande du procureur de la République, et après confirmation prononcée par un juge d'instruction[31].

[28] Non-lieu : ordonnance du juge pénal qui abandonne l'action engagée contre un prévenu
[29] Relaxe : décision du juge pénal qui abandonne l'action engagée contre un prévenu
[30] Critique de l'insécurité juridique
[31] Sur ce point, la loi de 1991 sera plus soucieuse des libertés individuelles.

L'autorité judiciaire apparaît comme la gardienne de la liberté individuelle en conformité avec la jurisprudence du Conseil constitutionnel[32]. Le champ d'application des interceptions judiciaires se limite aux infractions graves. L'interception comme moyen de preuve, dans les limites décrites plus haut est le dernier recours, quand les autres moyens d'investigations se sont avérés inopérants ou inefficaces.
Les formalités sont clairement indiquées. La motivation sera obligatoire, la mise sous surveillance temporaire. Des modalités de transcription, de destruction des enregistrements sont prévues. Le secret professionnel sera respecté dans la mesure du possible.
En matière d'interceptions de sécurité, les propositions de la commission Schmelck tendent à conserver le corpus existant, dans la mesure où cela est compatible avec les recommandations de la CEDH.
Les interceptions de sécurité doivent avoir un caractère d'exception. La commission propose les motifs suivants : la recherche de renseignements intéressant la sécurité nationale, la prévention des atteintes à la sûreté de l'Etat, la prévention des atteintes à la sécurité publique, la prévention du grand banditisme et du crime organisé.
L'exécution des interceptions sera circonscrite : les renseignements qui n'ont aucun rapport avec les motifs légaux doivent être réduits ; les documents seront détruits dès qu'ils ne seront plus indispensables.
Une loi servirait de base juridique aux interceptions de sécurité. Un débat s'est instauré au sein de la commission : l'autorisation devrait être accordée par un magistrat de l'ordre judiciaire ou par une autorité gouvernementale.
Une partie des membres de la commission se sont ralliés à la solution du magistrat. Il y aurait ainsi unicité d'autorisation de l'ensemble des interceptions au niveau de l'ordre judiciaire. Toutefois la majorité des membres de la commission est favorable à l'autorisation gouvernementale. L'institution du juge bouleverserait l'édifice existant. De plus, les interceptions de sécurité concernent surtout l'exécutif. Le caractère d'urgence paraît peu conciliable avec une procédure d'autorisation préalable confiée à un juge. Ces mesures serviront de référence, même si le rapport Schmelck n'a pas de suite immédiate.
La commission Schmelck constate que le système des interceptions administratives n'a pas de fondement juridique incontestable.
Le rapport Schmelck ne fut pas suivi d'effets immédiats. Certes, une proposition de loi déposée le 29 avril 1983, par M.Gautier et trente-cinq autres députés, s'inspire du rapport et envisage la réglementation des interceptions judiciaires dans le cadre du code de procédure pénale. Comme la majorité des propositions de lois, elle ne vint jamais à l'ordre du jour.
Lors de la première cohabitation, le 9 avril 1986, M.Chirac, alors Premier ministre, s'engageait devant l'Assemblée nationale à limiter les écoutes téléphoniques qui devaient être décidées par l'autorité judiciaire ou exigées par la sécurité de l'Etat.
Le 18 avril 1986, le ministre chargé de la sécurité, M.Pandraud, puis le 5 avril 1986, le ministre de l'Intérieur, M.Pasqua, avisaient la presse qu'un projet de loi, inspiré du rapport Schmelck, était préparé. Un avant-projet de loi fut effectivement étudié, élaboré par les services du ministère de l'Intérieur. Le projet, quant à lui, ne fut pas discuté en Conseil des ministres.
Après les arrêts de la CEDH, Kruslin et Huvig, des initiatives se font jour. En septembre 1990, un syndicat de police[33] présente une quinzaine de propositions relatives aux interceptions téléphoniques, réclame un projet de loi et un débat parlementaire.
Un sénateur et des députés déposent des propositions de lois : ils ont tous travaillé sur le thème des écoutes téléphoniques, et certains ont collaboré au rapport Schmelck, qui n'avait

[32] Conseil constitutionnel, 9 janvier 1980
[33] Police (nom du syndicat)

pas encore été publié à l'époque[34] ; citons la proposition de M.Rudloff, déposée devant le Sénat le 25 octobre 1990, la proposition de loi de M.Toubon, déposée devant l'Assemblée nationale le 25 octobre 1990, la proposition de loi de M.Hyest, déposée en décembre 1990 devant l'Assemblée nationale. Ces travaux ne sont pas identiques : ils n'en convergent pas moins sur certains axes qui ont retenu l'attention du rapport Schmelck ou (et) de la Cour européenne des droits de l'homme.

Le 15 novembre 1990, la Commission nationale consultative des droits de l'homme adopte en réunion plénière un avis soulignant l'urgence pour le gouvernement de soumettre au Parlement un projet de loi afférent aux interceptions de télécommunications. Le principe du projet de loi est arrêté. Seul, le moment de l'annonce pose encore dilemme. Une « affaire » permet à l'exécutif de faire acte de vertu et de nécessité[35].

A l'occasion du débat sur la réglementation des télécommunications de 1990, le ministre des PTT, Paul Quilès, fait savoir que le gouvernement déposera un projet de loi qui tirera toutes les conséquences des arrêts rendus par la Cour européenne des droits de l'homme.

La loi du 10 juillet 1991 met en place un organisme de contrôle pour les interceptions de sécurité : la CNCIS. La plupart des Etats démocratiques ont institué des organismes de contrôle mais le courant sécuritaire du début du vingt-et unième siècle est à l'origine de bien des inflexions. Ces organismes prennent en compte la culture juridique de chaque Etat.

II) Les organismes de contrôle avant 2001 :

A) Les USA :

Les interceptions de télécommunications y ont toujours été assez fréquentes. Le régime des interceptions de télécommunication est mixte : il est afférent aux interceptions judiciaires et aux interceptions de sécurité. Les lois fédérales en matière d'interceptions de télécommunication sont l' « Omnibus Crime Control and Safe Streets Act », Titre III, connu sous la dénomination Title III, adopté en 1968, le Foreign Intelligence Surveillance Act[36]de 1978, la CALEA, de 1994. Le Title III concerne les interceptions judiciaires au niveau fédéral et au niveau des Etats, le FISA Act les interceptions de sécurité.

1) Le Title III : est relatif à tous les moyens de télécommunication, à l'exception des téléphones sans fil, qui utilisent la voie hertzienne. Le Title III autorise le recours aux interceptions de télécommunication dans le cas des meurtres, des kidnappings, les affaires de drogue ainsi que « toutes les actions qui attentent à la vie, à l'intégrité physique ou à la propriété ». Le quantum de la peine est fixé à un an d'emprisonnement. Le Title III ne permet pas que les interceptions soient présentées comme preuve dans les infractions non violentes comme cela a été jugé en février 1996 par la Cour Suprême de l'Etat de Floride. Une loi de l'Etat de Floride autorisait le recours aux écoutes téléphoniques dans le cadre d'une enquête sur les milieux de la prostitution. La police d'Orlando avait en effet été autorisée par un magistrat à réaliser des écoutes téléphoniques sur un éventuel réseau de prostitution dans cette ville. Mais la loi fédérale l'emporte sur les lois des Etats en matière d'interceptions de télécommunication. En l'espèce, la Cour Suprême de l'Etat de Floride a considéré que si la prostitution peut être dangereuse[37], il ne s'agit que d'un délit[38] passible de soixante jours d'emprisonnement[39]. Elle n'a pas totalement exclu le recours aux interceptions de

---

[34] Il fut publié lors de la première parution du Rapport d'activité de la CNCIS 1991-1992, La Documentation française, 1993

[35] L'inculpation en 1990 d'un PDG, d'employés, d'un enquêteur de police en activité, d'un détective, travaillant tous pour une société privée de sécurité, pour interceptions téléphoniques illicites

[36] FISA Act

[37] Les avocats de la défense soutenaient que la prostitution constituait une menace « vitale », dans la mesure où le VIH se transmet par voie sexuelle (Nous étions à une époque où les traitements actuels n'existaient pas et où un € séropositif (ve) avait une espérance de vie assez réduite

[38] Et non un crime

[39] Inférieure au quantum de la peine d'un an

télécommunication dans les affaires de prostitution, mais seulement si ces affaires induisent des violences ou des menaces de violences. Au New Jersey, par exemple, les motifs susceptibles de justifier une demande d'interception sont les suivants : meurtres, enlèvements, trafics financiers, corruptions, paris illégaux, coups et blessures volontaires, menaces terroristes, incendies volontaires, vol organisé, trafic de stupéfiants, trafic d'armes, faux, crime organisé. La procédure est complexe. Toutes les interceptions nécessitent l'obtention d'un mandat de justice. Pour que ce mandat autorisant la mesure d'interception soit délivré, plusieurs conditions doivent être réunies.

L'officier chargé de l'enquête doit faire une déclaration écrite sous serment où il expose de manière très détaillée les faits permettant de croire que l'interception apportera la preuve d'une activité criminelle. Au niveau fédéral, la demande doit être approuvée par le ministre de la justice[40] ou l'un de ses collaborateurs[41]. Au niveau des Etats ou du district, la demande doit être approuvée par le procureur général de l'Etat, ou le représentant du gouvernement au niveau local, le procureur du district[42] ou le procureur du comté[43] . Ces derniers doivent néanmoins être autorisés par une loi de l'Etat à prendre une telle mesure.

Dans une deuxième étape, la demande est tenue d'être approuvée par un juge fédéral ou un juge de l'Etat, qui autorise ou refuse l'interception de télécommunications. La demande doit comporter :

- le nom de la personne chargée de l'enquête, ainsi que l'agrément du repré sentant du gouvernement
- les faits qui justifient la demande, le crime ou le délit envisagés, l'identité de la personne suspecte, le type de communication faisant l'objet de la surveillance, les appareils utilisés
- Préciser si d'autres moyens ont été mis en œuvre , les raisons de l'échec.
- La durée de l'interception (trente jours ; des possibilités de dépassement existent
- En cas de renouvellement, analyse des premiers résultats

Avant de donner son accord, le juge doit déterminer s'il existe des indices concordants démontrant que le suspect commet, a commis, est sur le point de commettre une infraction sanctionnée par la loi ; il doit aussi démontrer que les informations nécessaires seront très vraisemblablement obtenues par une interception de télécommunications ; les autres procédures d'investigation ont échoué. L'interception de télécommunication est le dernier recours[44]. Le mandat comporte les nombreux renseignements utiles : l'identité de la personne interceptée, la na ture des installations effectuées sur les lignes à intercepter, la nature des communications interceptées, l'infraction qui justifie l'interception, le nom du service autorisé à procéder à l'interception, le nom de la personne qui a fait la demande et la durée de l'interception. Les procédures sont donc longues et complexes. En cas d'urgence, lorsque le danger est imminent[45], le Tile III autorise n'importe quel enquêteur ou officier chargé d'appliquer la loi, qui aura été nommé par l'Attorney General ou l'un de ses proches collaborateurs, ou par le procureur général d'un Etat ou par un représentant d'une administration locale, à réaliser une interception de télécommunication. Cette interception sera régularisée dans les 48 heures pour ne pas être déclarée illégale.

[40] L'Attorney General
[41] Deputy Attorney General, Associate Attorney General
[42] District Attorney
[43] County Prosecutor
[44] « Toutes les procédures telles que surveillance visuelle, l'interrogatoire des suspects, l'utilisation d'indica teurs, l'enregistrement des numéros appelés ou reçus de la ligne (DNR) doivent avoir été tentées avant d'envisager une mesure de surveillance téléphonique » in Fabienne Basset « Les écoutes téléphoniques administratives sous surveillance », DEA de droit public, Université de Rennes I, septembre 1996
[45] Danger de mort ou de blessures graves ou quand la sécurité nationale est menacée

Cependant, dans l'Etat de New York, même une situation d'urgence nécessite une décision du juge fédéral a priori. Le juge peut accorder une autorisation écrite temporaire d'une durée maximale de 24 heures, sur la base d'une demande verbale du procureur du district. La requête est enregistrée et transcrite ; la régularisation écrite intervient dans les 24 heures

Le Title III précise que certaines personnes protégées ne peuvent faire l'objet d'interceptions de télécommunications : il s'agit des avocats parce qu'ils assument les droits de la défense, et des prêtres, détenteurs du secret de la confession.

Le procès-verbal retranscrit uniquement les informations afférentes à l'infraction[46].

Les enregistrements et les transcriptions effectuées par l'agent sont remis au magistrat qui a pris la décision d'interception. Les enregistrements sont conservés par la justice pendant dix ans.

Le Title III Act a mis en place un système de contrôle. Tous les cinq jours durant la période d'interception, le procureur présente un rapport au magistrat qui a pris la décision pour que le dit magistrat puisse décider de poursuivre ou de faire cesser les interceptions. Par ailleurs, trente jours après que la décision d'autorisation ait été arrêtée, le juge doit établir un rapport sur la mesure d'interception qu'il a ordonnée, à l'Administration des tribunaux fédéraux[47]. Cette dernière joue un rôle essentiel en matière d'interceptions judiciaires : chaque année, l' Attorney General doit lui aussi transmettre un rapport à cette administration, pour l'ensemble des interceptions qui ont été réalisées au cours de l'année. L'administration des tribunaux fédéraux est à l'origine d'un rapport annuel sur toutes les mesures d'interception réalisées tant au niveau fédéral qu'au niveau des Etats. En 1992, sur 919 interceptions autorisées, 340, soit 37% concernaient des mesures prises au niveau fédéral ; 197 concernaient l'Etat de New York, 111 l'Etat du New Jersey, 80 l'Etat de Floride, 77 l'Etat de Pennsylvanie. Les 114 autres interceptions se répartissaient sur 18 autres Etats. Dans la dernière décennie du vingtième siècle, le nombre d'interceptions judiciaires réalisées chaque année aux USA, est de 780 en moyenne. Les services chargés des interceptions de télécommunication publient également chaque année leur rapport, comme le département de la police de New York. Au niveau fédéral ou au niveau des Etats, les tribunaux autorisent souvent le recours à des interceptions téléphoniques, à des pen-register[48], à des trop and trace[49]pour empêcher la commission d'actes criminels et recueillir les preuves dans le domaine des crimes et des associations de malfaiteurs. Les critères de la licéité sont un tantinet plus larges aux Etats-Unis qu'en Europe.

2) Le 25 octobre 1994, la Présidence a conféré force de loi à la CALEA[50] (Communication Assistance for Law Enforcement Act) ou loi sur la sur la téléphonie numérique. La CALEA doit permettre de faire face aux rapides mutations des technologies de télécommunications, affirmer l'obligation pour les opérateurs de télécommunications de prêter leur concours aux services autorisés à procéder à des interceptions de communications et à des identifications d'appel.

Bien avant le Patriot Act, des interceptions de télécommunications ont trouvé leurs fondements dans des Orders (décrets) du Président des USA ou règlements des administrations fédérales, assimilés aux décrets-lois[51] et dans la loi adoptée en 1978 la

[46] On parle de « minimization »

[47] Administrative Office of the United States Courts, the AO

[48] Disposition d'identification du numéro appelé

[49] Disposition d'identification du numéro appelant

[50] Public law, 103 414 47 USC 1001-1010

[51] Citons l'Executive Order (décret-loi) n° 12036 du 24 janvier 1978, remplacé par l'Executive Order 12333 du 4 décembre 1981 (Federal register, vol 46, n° 235, p 59941) ; Executive Order, 12334 du 4 décembre 1981 (Federal Register, vol 46, p 596), la création du « President's Intelligence Oversight Board » (Conseil

Foreign Intelligence Surveillance Act ou FISA (loi sur la surveillance des activités de renseignements extérieures). Cela correspond aux interceptions de sécurité.

- 3)La FISA : est l'une des conséquences législatives de l'affaire du Watergate survenue quelques années auparavant dans un domaine éminemment sensible qui n'était jusqu'alors régi que par les « executive orders » ci-dessus mentionnés.

Lorsque les juges de la Cour spécifique instituée par le FISA Act ont approuvé leur demande, ils donnent l'ordre à l'opérateur d'exécuter matériellement la décision.
En cas d'urgence, l'Attorney General, ou son délégué est habilité à autoriser une interception de sécurité, à condition que les juges soient prévenus et qu'une régularisation intervienne dans un délai de 24 heures.
Les autorisations de l'Attorney General, les demandes émanant des différents services, les autorisations accordées par les juges sont consignées dans des dossiers qui sont conservés pendant au moins dix ans.

3.1) Interceptions et vie privée :

Les informations obtenues grâce au système FISA sont entourées du secret et ne font l'objet d'aucune exploitation licite quand il s'agit de citoyens américains. En matière pénale, ces informations sont utilisables, après accord de l'Attorney General : la personne concernée et son avocat seront informés. La personne mise en cause est alors en droit de saisir le tribunal fédéral de première instance[52]territorialement compétent et d'invoquer la non-recevabilité des « preuves » recueillies par ces moyens spécifiques : elle tentera de démontrer que les preuves n'ont pas été rassemblées de manière licite, que la surveillance n'était pas conforme à la loi.
La décision du tribunal d'instance s'impose à tous les tribunaux fédéraux et aux tribunaux des Etats de la Fédération à l'exception des cours d'appel. La décision du tribunal d'instance peut être réexaminée devant les cours d'appel et la Cour suprême. Rappelons qu'aux USA, le quatrième amendement de la Constitution protège les citoyens « dans leurs personnes, leurs maisons, leurs papiers et leurs effets » contre les perquisitions et les saisies déraisonnables »

3.2)Le contrôle public :

L'Attorney General, premier responsable des mesures d'autorisation, est tenu (telle est la contrepartie de son pouvoir) de faire parvenir chaque année[53]un rapport à l'administration des tribunaux fédéraux et au Congrès sur l'application de la FISA. Le rapport mentionne notamment le nombre total de demandes, de renouvellements ; il précise combien de demandes ont été refusées. La lecture des rapports nous permet de savoir que la tendance à l'augmentation des demandes s'est précisée[54] et qu'aucune demande n'a été refusée. Une seule demande a été modifiée par un tribunal FISA.
Comme les archives des tribunaux FISA ne peuvent être consultées, il est impossible de déterminer si les juges respectent avec scrupule l'esprit et la lettre de la FISA ou s'ils privilégient une interprétation sécuritaire de la loi.
Chaque semestre, l'Attorney General informe aussi les commissions spéciales[55] du Congrès sur les activités de surveillance[56]. Ces commissions, au nombre de deux, ont le droit de réunir d'autres informations dans la mesure où lesdites informations sont indispensables au bon accomplissement de leur mission. Les commissions parlementaires informent une fois par an

---

présidentiel de surveillance des activités de renseignements, qui coordonne l'action des services de renseignements américains)

[52] District Court

[53] Article 107, FISA

[54] En moyenne, dans la dernière décennie du vingtième siècle, la moyenne des interceptions se situe à 500 autorisations par an

[55] Select Committees on Intelligence : « House Permanent Select Committee on Intelligence » et « Senate Select Committee on Intelligence »

[56] Article 108 (a), FISA

leurs chambres réunies en assemblées de l'application de la loi. Ces rapports présentent parfois des observations et des propositions. Les interceptions du FISA Act sont classées « secret-défense » ; c'est pourquoi elles ne sont pas aussi détaillées dans les rapports que les interceptions judiciaires ; en outre, ces rapports ne sont pas rendus publics.
Aux Etats-Unis, la personne concernée par ces mesures n'est pas informée. En revanche, il y est admis le concept de « personnes protégées » et la prise en compte de certains secrets professionnels.
Les conversations interceptées ne peuvent impliquer des avocats, des pasteurs, des prêtres. N'oublions pas que la fonction d'avocat est valorisée aux USA et que la religion a un caractère officiel. Le FBI doit interrompre l'interception dès qu'une personne protégée intervient.
En matière de peines encourues, la FISA prévoit une peine de 10 000 dollars au plus, de cinq ans d'emprisonnement au maximum, et les deux en cas d'abus de nature intentionnelle. L'article 110 de la FISA dispose que toute personne ayant subi un préjudice dû à une mesure de surveillance ou à une indiscrétion générée par cette mesure percevra des dommages-intérêts. Le système, complet, met en exergue la notion de souveraineté américaine et de citoyenneté américaine. Les statistiques, d'ailleurs incomplètes et éparses, permettent néanmoins de déterminer que les mises en cause d'interceptions sont assez rares aux Etats-Unis, par rapport à celles des écoutes.

3.3)Les garanties dans le cadre des modalités d'interceptions :

La FISA n'autorise que les interceptions des télécommunications effectuées au moyen de dispositifs électroniques, mécaniques ou autres[57].
Les interceptions sont motivées. Les termes génériques employés sont les suivants : « Informations concernant les activités de renseignements d'une puissance étrangère », ce qui correspond à la nécessité de protéger la sécurité des USA.
En voici la liste limitative :

- les attaques avérées ou possibles, le sabotage (infraction à l'article 105 du chapitre 18 du code pénal fédéral des Etats-Unis)
- le terrorisme international : c'est-à-dire, les actes de violence et les agissements qui mettent en péril la vie humaine, et constituent une violation des lois pénales américaines ou étrangères ; le lieu de l'attentat peut se situer sur le territoire américain, ou sur un territoire non américain. Le « terrorisme international » comprend aussi les activités menées avec l'intention d'intimider un gouvernement, ou d'exercer une influence sur un gouvernement par le meurtre, l'enlèvement ou le détournement, y compris hors du territoire américain.
- les activités clandestines susceptibles de nuire aux USA et de profiter à des services de renseignements étrangers.

Ces termes sont généraux, peut-être insuffisamment précis. Ils laissent une marge d'interprétation et d'appréciation aux responsables de la sécurité.
Une distinction est établie entre les citoyens américains et les étrangers résidant sur le territoire américain. Un ressortissant étranger est considéré comme l'agent d'une puissance étrangère s'il est en mesure de participer [58] à des activités de renseignements. Le citoyen américain, lui, ne sera assimilé à un agent d'une puissance étrangère que s'il se livre à des activités de renseignements en toute connaissance de cause[59].

[57] Article 101 (f) n° 1
[58] « may engage »
[59] Knowingly. Article 101 (b), FISA

Les demandes d'autorisation sont élaborées par les agents fédéraux[60] qui adressent une demande de surveillance au juge compétent[61]. La demande n'a aucun fondement juridique si elle ne reçoit pas l'agrément de l'Attorney General, dont le rôle est d'examiner les demandes correspondant aux motifs licites[62]. La demande est assortie de renseignements minutieux :

- l'identité de l'argent
- la procuration générale reçue par l'Attorney General du Président des Etats-Unis pour accorder de telles autorisations
- l'agrément de l'Attorney General
- l'identité (si elle est connue) de la personne à intercepter ou (si l'identité est inconnue) une description de la ou des personnes à surveiller
- un résumé des faits qui semblent justifier la demande d'interceptions
- une présentation des mesures envisagées en matière d'utilisation de fichiers informatiques (indications des procédures)
- une description des informations à rassembler, de la nature des communications à intercepter
- une « garantie » délivrée par le mandataire du Président des USA pour la sûreté nationale (ou par un haut fonctionnaire délégué que le Président aura nommé sur recommandation et avec l'approbation du Sénat parmi les responsables de la sûreté nationale ou de la Défense) sur la base de critères qui se veulent objectifs :
- les informations se font au profit d'une puissance étrangère[63]
- l'unique but de l'opération est l'obtention de ces informations
- la demande est déposée parce que les autres techniques d'enquête, habituelle et plus protectrices de la vie des citoyens, se révèlent inadaptées, non fiables
- un descriptif des moyens utilisés
- une déclaration précisant si une violation de domicile semble s'avérer indispensable
- une déclaration afférente aux demandes antérieures concernant les installations, les personnes, les locaux
- la durée prévue pour la surveillance :

Les agents qui sont à l'origine de la demande garantissent sous la foi du serment la véracité de leurs indications ou déclarations[64]. Les indications exigées par la loi en matière de demandes sont nombreuses : il convient d'éviter les abus et les dérives.

Dans les faits, la lourdeur administrative, les coûts de gestion induits par les traitements, ont amené les juges à accepter des formules types. Le gain de temps et d'argent ne risque-t-il pas d'occulter les intentions initiales de préservation des libertés individuelles ? C'est une possibilité.

Les tribunaux compétents[65]ont été invités à faire montre de vigilance afin que le formalisme ne supprime pas l'exposé des motifs. La procédure est cependant simplifiée lorsque les représentants d'une puissance étrangère sont soumis à surveillance ou à une interception.

Si les demandes d'autorisation sont soumises à l'agrément de l'Attorney General, ce sont les juges qui délivrent les ordonnances. Les juges sont des magistrats auprès des FISA

[60] Federal Officers
[61] Article 103, FISA
[62] Article 104 (a), FISA
[63] Article 101 (e), FISA
[64] Le Président Clinton a décidé que seul le directeur du FBI est habilité à signer. En cas d'empêchement, c'est le directeur de la CIA qui aurait délégation de signatures.
[65] Fisa Court

Court. Cette cour spécifique est composée de sept juges de district, désignés par le Président de la Cour Suprême des USA, pour une durée de sept ans. L'ordonnance est unilatérale[66], sans audition au tribunal de la partie concernée. Dans ce domaine où le secret est de mise, le principe de contradiction ne se justifie pas.

La durée habituelle prévue pour ces autorisations ne peut dépasser trois mois, mais elle est renouvelable[67]. Une exception s'applique aux agents des puissances étrangères, aux personnes morales dépendant des puissances étrangères : la durée peut atteindre un an.

L'autorisation du juge est indispensable pour réaliser une interception régie par le FISA Act. Il existe néanmoins deux exceptions. La première exception implique que les communications se font exclusivement entre des puissances étrangères ou que les moyens techniques de communication soient autres que vocal, et se trouvent sur un emplacement exclusivement sous le contrôle des puissances étrangères. Cette exception est justifiée par le raisonnement suivant : l'interception de telles communications porte très rarement atteinte à la vie privée des citoyens américains. Une procédure de « minimization » ; à ces conditions, l'autorisation d'une interception est accordée par le Président des USA, représenté par le ministre de la Justice, et ce pour une période dont le butoir est d'un an.

La deuxième exception est relative à la déclaration de guerre par le Congrès. Dans ce cas, le Président des USA, représenté par le ministre de la justice est susceptible d'autoriser des mesures d'interception de communications afin de surveiller les puissances étrangères , sans mandat de justice, pour une période limitée à quinze jours

En cas d'urgence, l'Attorney General ordonne des mesures sans l'agrément du juge ; il informe le tribunal FISA compétent dans les vingt-quatre heures et une demande de régulation est alors déposée.

L'ordonnance indique que l'opérateur de télécommunications[68], le propriétaire ou gérant d'immeubles sont tenus d'assister le service qui a fait la demande d'informations. Les personnes privées qui prêtent leur concours à ces mesures de surveillance ou d'interceptions se voient prescrire une obligation de confidentialité, qui s'applique dans tous les pays en matière de surveillance ou d'interception de sécurité.

La FISA a envisagé le refus de demande et les modalités de recours. Si une demande est refusée en tribunal de première instance, il est possible de saisir une autre juridiction dont les trois juges sont désignés par le président de la Cour suprême parmi les juges des tribunaux de district ou d'appel[69] ; le président de la Cour suprême désigne aussi le président du tribunal formé à cette occasion. Un juge de FISA Court est nommé pour sept ans, avec renouvellement annuel. La rééligibilité est interdite[70].

La décision du tribunal d'instance s'impose à tous les tribunaux fédéraux et aux tribunaux des Etats de la Fédération à l'exception des cours d'appel. La décision du tribunal d'instance peut être réexaminée devant les cours d'appel et la Cour suprême.

Par ailleurs, la sécurité des personnes est prise en compte. Si des constatations sont réalisées sur le territoire américain, à l'aide d'appareils dont la finalité est la surveillance selon la définition de la FISA, les informations sont détruites quand l'Attorney General constate que le contenu des données est susceptible de mettre en danger une personne- blessures ou homicides- au cas où l'on n'y procéderait pas.

Les autorisations de l'Attorney General, les demandes émanant des différents services, les autorisations accordées par les juges sont consignées dans des dossiers qui sont conservés pendant au moins dix ans.

---

[66] Ex-parte order

[67] Article 105 (d), FISA

[68] Specified communication or other common carrier

[69] Courts of Appeals

[70] Article 103, FISA

En 1992, il y eut 484 décisions de justice autorisant une mesure d'interception. Pendant la dernière décennie du vingtième siècle, la moyenne des interceptions est d'environ 500 par an.

B) Le Royaume-Uni :

Après l'arrêt Malone, la loi de 1985, « The Interception of Communication Act »[71]confie au ministre de l'Intérieur[72] la responsabilité de délivrer l'autorisation d'interception. Au Royaume-Uni, le régime n'est pas mixte (interceptions judiciaires/ interceptions de sécurité). L'utilisation des interceptions est toujours décidée par l'autorité administrative. Si une urgence intervient, sous réserve de l'accord téléphonique exprès du ministre de l'Intérieur, un autre ministre ou un haut fonctionnaire peuvent ordonner l'interception, à condition que la situation soit régularisée dans les 48 heures.

Les motifs sont peu nombreux :

- l'intérêt de la sécurité nationale[73]
- prévention ou découverte d'un crime grave[74]
- sauvegarde de la prospérité économique du Royaume-Uni

Ces motifs ne peuvent être invoqués que si les informations recherchées ne sont pas susceptibles d'être acquises par des moyens plus soucieux des libertés individuelles.

N'oublions pas que la Constitution coutumière britannique comprennent le principe du secret des conversations.

L'utilisation des données fait l'objet de multiples précautions. Sont déterminées le nombre de personnes ayant accès aux documents, l'étendue et le nombre de reproductions licites. Les documents ont vocation à être détruits.

1) Le contrôle par le « Commissioner »

Le premier Ministre nomme[75] une personne qui a pour mission de contrôler si l'exécutif exerce ses prérogatives en conformité avec la loi. La personne désignée est le « Commissioner »[76] qui est doté de compétences juridiques approfondies, qui est chargé ou qui a été chargé de fonctions judiciaires. Il est nommé pour trois ans par le Premier ministre et son mandat est renouvelable. Cette fonction s'exerce à temps partiel. Elle a notamment été remplie par un juge de la Chambre des Lords de Londres Le Commissioner perçoit une indemnité prévue dans les crédits budgétaires du Parlement. Tous les agents participant à l'exécution de l'interception facilitent l'action du Commissioner, lui communiquent les documents ou informations dont il a besoin. L'enquête est pointilleuse. Si elle révèle des manquements à la loi, le Commissioner rédige et fait parvenir un rapport au Premier ministre[77].

Le Commissioner établit par ailleurs un rapport général annuel sur les conclusions qu'il a tirées de la confrontation entre la loi et son application. Le rapport indique le nombre d'interceptions autorisées, qui s'élève à plusieurs centaines. Il est communiqué à la Chambre des communes et à la Chambre des Lords. Le Premier ministre peut empêcher la publication de passages du rapport destiné au Parlement et au chef du gouvernement, s'il

[71] Sur les interceptions de télécommunications et de correspondance

[72] D'après les directives du « Joint Intelligence Committee (JIC)

[73] Selon le rapport du Commissioner de la Sécurité nationale : terrorisme, espionnage, activités subversives qui mettent en danger la sécurité ou le bien public et qui visent à supprimer la démocratie parlementaire par le biais de mesures de violence (N 27.31)

[74] Selon le rapport du Commissioner, 1986 : crime grave-état des infractions qui ont recours à la violence, par lesquels un gain matériel important peut être tiré, auxquels un nombre certain de personnes ayant le même objectif participent, pour lesquels l'auteur qui n'a aucun antécédent judiciaire est passible d'une peine d'emprisonnement de trois ans (N 25)

[75] Paragraphe 88 de l'Interception of Communication Act

[76] Traduit en français par commissaire du gouvernement

[77] Sur les affaires douteuses

estime que les paragraphes incriminés sont susceptibles de porter atteinte à la sécurité nationale, à la prévention de la criminalité, à la sauvegarde du potentiel économique du Royaume-Uni. Une transparence relative est souhaitable, mais ne doit pas porter atteinte à la sécurité.

Dans la mesure où les rapports sont conçus par un juge, ces études contiennent des concepts, des interprétations juridiques. Les Commissioner ont pu élaborer une jurisprudence interne à la loi. Les zones d'ombre se sont atténuées et le nombre des interceptions a diminué après 1986, dans la mesure où le ministre de l'Intérieur s'est vu préciser quand il pouvait requérir des autorisations d'interceptions. Il s'agit donc d'une construction originale, où un magistrat éclaire l'exécutif sur la compréhension et la pratique pertinente d'une loi adoptée par le Parlement.

2) Le contrôle par un tribunal :

Une autre forme de contrôle est exercée par l'Interception of Communication Tribunal, dont les membres[78] ont tous une compétence juridique et une pratique juridique d'au moins dix ans. Les membres de ce tribunal sont désignés officiellement par la Reine, c'est-à-dire, dans les faits, par le Premier ministre pour une durée de cinq ans[79]. Ils appartiennent tous à la majorité parlementaire et leur impartialité ne peut être mise en cause. Le tribunal est saisi par les personnes qui pensent être l'objet de mesures d'interceptions. Cette réclamation est suivie d'une enquête et le tribunal se fait assister par le Commissioner qui possède tous les éléments susceptibles d'éclairer le tribunal.

Si le tribunal considère que la réclamation est fondée, qu'une mesure d'interception avérée est anticonstitutionnelle, il en informe l'auteur de la réclamation[80], adresse un rapport au Premier ministre, et promulgue une ordonnance qui sert de base à :

- la déclaration de nullité de la décision d'écoute illégale,
- l'ordre de détruire les documents, non seulement les originaux, mais aussi les copies, duplicatas,
- l'engagement de l'exécutif à verser des dommages-intérêts au requérant[81]

Si le tribunal s'aperçoit qu'il n'y a pas eu d'interceptions ou s'il est persuadé de la légalité de l'interception, il précise au particulier que ses droits n'ont pas été lésés. Le particulier n'est pas informé a posteriori des mesures de surveillance dont il est l'objet.

Le ministère de l'Intérieur a entouré cette disposition (la possibilité de déposer une réclamation) d'une publicité inédite. Non seulement une médiatisation a entouré l'adoption de la loi, mais des dépliants, avec formulaire de réclamation, ont été mis à la disposition du public dans les services de postes ou de télécommunications.

Cette publicité présente un caractère unique. Dans les autres pays, les requérants procéduriers sont obligés de rechercher dans les arcanes de la loi les éventuelles possibilités de réclamation qui s'offrent à eux. Ici, un mode d'emploi a été présenté aux citoyens. La démarche s'explique en partie par la condamnation du Royaume-Uni à l'occasion de l'arrêt « Malone » de la CEDH. Les ressortissants britanniques sont avisés qu'une voie de recours interne existe pour eux. Cet effet d'annonce a pour ambition de limiter les impacts négatifs que produit une condamnation pour violation de la Convention de sauvegarde des droits de l'homme. Le Commissionner a encouragé les services de renseignement, de police, des douanes, le ministre de l'Intérieur, les opérateurs, à collaborer.

---

[78] Au nombre de cinq, avoués ou avocats

[79] Renouvelables

[80] Cela est fort rare. Dans la plupart des cas, les interceptions sont perçues comme légales, paragraphes deux à cinq de l'Interception of Communication Act

[81] Le montant de l'indemnité est fixé par le tribunal

La situation a évolué depuis. Le 2 juillet 1996, la Chambre des Lords a rejeté l'appel introduit par monsieur Khan contre l'arrêt de mai 1994 rendu par la Cour d'appel d'Angleterre. Le rejet de l'appel est motivé : il ne convient pas de se prononcer sur l'admissibilité dans un procès pénal de preuves recueillies au moyen d'un système d'écoute dont la mise en place aurait supposé un délit d'intrusion et un dommage causé à une propriété immobilière. En effet, l'argumentation se fonde sur l'article six de la Convention européenne de sauvegarde des droits de l'homme ; la Convention n'appartient pas à l'ordre interne anglais. Selon le droit anglais, la police a agi de bonne foi[82]et les irrégularités n'ont pas rendu le procès inéquitable.

Un projet de loi a été présenté fin 1996. Ce projet concerne la police, mais implique des interférences avec « The Interception of Communication Act ». Il y est indiqué : « Aucune introduction ou interférence dans une propriété ou dans la télégraphie sans fil n'est illégale » si le « chef constable » l'estime nécessaire.

Le dispositif a été rejeté par la Chambre des Lords ; il fut très controversé[83]. Il a finalement été adopté et est devenu le « Police Act » du 21 mars 1997. Le ministère de l'Intérieur a publié en août 1997 un code de conduite explicitant les conditions dans lesquelles les services de police et de douanes peuvent pénétrer dans les domiciles privés, les bureaux, les chambres d'hôtel, pour y recueillir des informations destinées à la prévention ou à la répression d'activités criminelles, en utilisant des systèmes d'écoute. Des renseignements confidentiels détenus par des médecins, des avocats, des journalistes, des ministres du culte sont ainsi collectés. Les opérations sont autorisées par un officier supérieur des services de police ou des douanes ; un contrôle est exercé par un Commissioner.

L'examen de l'ensemble des textes britanniques en matière d'interceptions laisse une impression contrastée. L'accent est mis sur la sécurité, sur les moyens de rassembler des preuves par interceptions de télécommunications, même si des modalités de contrôle ont été instaurées. Par ailleurs, la vidéosurveillance existe depuis 1953 au Royaume-Uni et s'est développée dans la dernière décennie du vingtième siècle et la première décennie du vingt-et-unième siècle. L'Information Commissioner's Office[84], autorité de régulation en matière de protection des données personnelles affirmait en 1984, via son Président, Richard Thomas, que le Royaume-Uni « se dirigeait tel un somnambule vers une société de la surveillance. Le Rapport de l'ICO de 2006 dénonce les dangers d'une société de surveillance, via la combinaison des interceptions de télécommunications, la biométrie, la vidéosurveillance.

C) L'Allemagne :

La législation existait en RFA depuis le 13 août 1968. La loi G10, élaborée en application de l'article 10 de la Grundgesetz, a fait preuve d'une certaine fiabilité. Le régime est mixte. Les interceptions judiciaires peuvent être décidées par le juge d'instruction. En cas d'urgence, le Procureur est habilité à prendre la décision d'interception, à condition que la dite décision soit confirmée par le juge d'instruction dans les trois jours. Par ailleurs, les interceptions de sécurité sont autorisées par des personnalités exerçant un pouvoir exécutif. La loi G10 précise que les interceptions ne doivent être utilisées que si les autres moyens d'investigation sont voués à l'échec. La loi de 1968 a été complétée à plusieurs reprises, en particulier en 1978 : obligation est faite, après l'expiration de la mesure d'informer la personne qui en a été l'objet, à condition de ne pas compromettre la finalité poursuivie. En 1989, tous les opérateurs, et plus seulement l'opérateur historique ont été

[82] Elle s'est conformée à la directive de 1984 du ministre de l'Intérieur : « Instruments d'écoute cachés et surveillance visuelle à couvert »

[83] J.R.Spencer, « Bugging and burghary the police », The Cambridge Law Journal du 31 janvier 1997

[84] ICO

tenus de participer aux mesures d'interception. En 1992, la question des compétences respectives de la commission G10[85] et du Commissaire à la protection des données nominatives a été tranchée au profit de la première par une disposition législative s'appuyant sur le principe de spécialité.

1) Les autorisations :

Les interceptions judiciaires sont autorisées quand il existe des indices concordants et réels laissant présumer que la personne visée fait, a fait ou envisage de commettre un des actes répertoriés par la loi G10. Il s'agit de l'assassinat, de l'homicide volontaire, du viol, du trafic de stupéfiants et des délits les plus graves pour la sécurité de l'Etat, tels la haute trahison, l'atteinte à la sûreté extérieure de l'Etat, l'espionnage, les activités d'agents secrets, l'association de malfaiteurs. Comme au Royaume-Uni, l'interception implique qu'il n'existe pas d'autres moyens d'investigations. Les interceptions judiciaires sont ordonnées par le juge d'instruction. En cas d'urgence, le Procureur assume la responsabilité de la mesure qui est confirmée par le juge d'instruction dans les trois jours.

Les motifs et les autorités habilitées en matière d'interceptions de sécurité sont indiqués.

Les motifs sont, en 1968, les suivants :

- prévention ou répression des menaces contre l'ordre démocratique et libéral[86]
- protection de l'existence ou de la sécurité de la Fédération et du Land
- défense de la sécurité nationale, défense de l'ordre public, prévention des infractions pénales
- prévention des infractions à la sûreté extérieure de l'Etat
- prévention des infractions contre la Défense nationale
- prévention des infractions à la loi sur les étrangers
- prévention des menaces contre la sécurité des troupes de l'OTAN

Les autorités susceptibles de demander des interceptions de communication par télécommunications sont :

- le BFV, service fédéral de protection de la Constitution et du renseignement intérieur
- le BND, service de renseignement fédéral chargé du renseignement à l'extérieur
- le LFV, service chargé dans chaque Land de la protection de la Constitution
- le MAD, service de sécurité militaire

Les autorités qui peuvent délivrer des autorisations sont des personnalités incarnant l'exécutif : l'autorité suprême dans le Land pour le LFV, les ministres de l'Intérieur et le ministre de la Justice dans les autres cas.

L'autorisation prend une forme écrite. Elle est transmise au service demandeur et à l'opérateur de télécommunications. L'article 1, paragraphe 4, de la loi G10 fixe à trois mois la durée maximale de la mesure. Un renouvellement est possible.

Il existe également le recours au « contrôle stratégique », soit la surveillance exercée sur certaines liaisons entre l'Allemagne et l'étranger, destinée à collecter des informations qui ne sont pas individualisées[87]. Les motifs sont :

- l'agression armée
- les attentats terroristes sur le territoire allemand
- le trafic international de matériel de guerre ou de moyens de destruction massive bactériologique, chimique ou nucléaire

---

[85] Cf : infra

[86] La formulation s'explique par la situation particulière dans une Allemagne divisée alors en deux Etats, RFA et RDA. La RFA cherchait à se protéger contre les éléments de déstabilisation. Le caractère libéral du régime était identitaire pour la RFA

[87] Paragraphe trois de l'article un de la loi du 13 août 1968

- trafic de stupéfiants
- blanchiment d'argent
- faux monnayage

La surveillance ne permet pas de retenir des éléments contre des personnes identifiées.
Avec le contrôle stratégique, l'arrivée ou le point de départ de la liaison surveillée se situe à l'étranger, dans des zones à risque pour la sécurité allemande, définies par un arrêté du ministre fédéral de la Défense approuvé par le PKG. Le Conseil constitutionnel fédéral[88] a déclaré que les dispositions relatives aux différentes formes de contrôle stratégiques, insérées dans la loi G10 en 1994, étaient en grande partie incompatibles avec la Constitution.

2) Le contrôle :

Il est effectué par deux commissions, le PKG et la commission G10.
Une commission[89], dite G10 est composée de quatre membres et de quatre suppléants, qui sont désignés à l'issue d'un vote au sein d'un collège élu en son sein par le Bundestag, le PKG, organe de contrôle parlementaire des services de renseignement, après avis du Gouvernement, qui procède à une enquête de sécurité. Le PKG est composé de neuf parlementaires désignés par le Bundestag à la proportionnelle pour une durée de quatre ans. Il reçoit tous les semestres un compte-rendu du ministre fédéral de l'intérieur sur les interceptions intervenues, leur exécution, les résultats qu'elles sont parvenues à obtenir. Ce compte-rendu n'est pas relatif aux mesures individuelles mais aux questions de principe posées par l'application de la loi de 1968. Le PKG soumet au Bundestag en milieu et en fin de législature un rapport sur son activité de contrôle et présente annuellement un rapport spécifique sur l'exécution des interceptions stratégiques.
La commission G10 décide si les mesures d'interception soumises par le ministre fédéral compétent sont nécessaires. Elle surveille la régularité de l'exécution, la destruction des enregistrements, des transcriptions supports informatiques. Elle contrôle aussi si l'information a posteriori des personnes ayant fait l'objet d'une interception est effective. Elle peut entreprendre des vérifications soit de sa propre initiative, soit sur la base de plaintes de particuliers qu'elle instruit. Le mandat des membres de la commission coïncide avec une législature du Bundestag[90], expire après l'élection d'une nouvelle chambre. La renouvelabilité est possible. Les membres de la commission peuvent être parlementaires. Par contre, il y a incompatibilité avec un poste gouvernemental L'opposition est représentée au sein de cette commission[91]. Le président et son suppléant doivent être aptes aux fonctions de magistrats. Le mandat est irrévocable. La Commission a accès à tous les dossiers. Le collège élu est constitué de cinq députés du Bundestag que les ministres fédéraux informent régulièrement sur l'application de la loi. Ce collège procède à l'élection des membres de la commission[92] et approuve la désignation des zones sensibles ou dangereuses.
La Commission a un rôle décisionnel, et non facultatif. Aucune mesure d'interception ne peut être faite sans son autorisation à laquelle il est impossible de passer outre. En cas de décision négative, l'exécution de la mesure doit être immédiatement interrompue. Cependant, avec l'extrême urgence, l'interception est exécutée avec le seul accord du ministre ; ce dernier régularise rapidement la situation auprès de la commission G10.

---

[88] Arrêt du 14 juillet 1999
[89] Article 9, alinéa 4
[90] Le mandat, en fait, se perpétue au-delà d'une législature pour une durée maximale de trois mois afin de permettre l'organisation des élections de leurs successeurs.
[91] Contrairement à ce qui se passe au Royaume-Uni avec le tribunal
[92] Article 1er, alinéa 1 de la loi du 11 avril 1978, sur le contrôle parlementaire des activités fédérales de renseignement

Les décisions de la commission G10 sont collégiales : elles ne peuvent être arrêtées que si quatre de ses membres, titulaires ou suppléants sont présents. Elle travaille dans le secret, sous sa propre responsabilité, ne reçoit d'instructions de personne, ne communique pas de données informatives sur le nombre d'interceptions. Elle exerce son contrôle directement sur les opérateurs de télécommunications.
En ce qui concerne les mesures individuelles, le ministre fédéral allemand compétent informe la personne qui en est l'objet que la mesure a pris fin. Tous les mois, sont présentés à la commission G10, outre les projets d'interceptions, les notifications effectuées et les cas dans lesquels cette obligation de notification contrevient à des objections susceptibles d'y faire obstacle. Si la notification est de nature à remettre en cause l'objectif poursuivi par la mesure, la commission peut, à titre exceptionnel, dispenser le gouvernement de notifier ou décider qu'il sera sursis à cette démarche. Il n'y a pas de notification dans le cas du contrôle stratégique. Si, à l'occasion de la surveillance des transmissions hertziennes internationales, certaines personnes sur le territoire allemand soient interceptées, les informations collectées sont détruites dans un délai de trois mois ou notification est faite aux intéressés de l'atteinte qui a été portée au secret de leurs communications. La notification peut être exclue ou retardée dans les mêmes conditions que celles prévues pour les mesures individuelles. Cette règle de notification est à l'origine de recours devant les juridictions administratives qui ont tous été rejetés.
Enfin, la Cour constitutionnelle allemande peut être saisi par tout citoyen estimant que ses droits fondamentaux ne sont pas respectés : cela englobe les interceptions de télécommunication.

3) La loi de 1997 :

Elle met davantage l'accent sur la sécurité. Elle autorise les juges et les policiers allemands à procéder à des interceptions de conversation à distance et à des écoutes dans les logements privés pour les enquêtes judiciaires, quand il s'agit de faits particulièrement graves.
Les membres des professions soumises au secret professionnel peuvent être interceptés. Sont exclues les confessions auprès des ministres du culte et les conversations professionnelles des avocats en charge d'affaires pénales. Quant aux parlementaires, qui bénéficient de la légitimité élective, ils ne sont pas soumis à ces dispositions.
L'autorisation est accordée par une commission de trois magistrats. En cas d'urgence, l'autorisation est délivrée par un seul d'entre eux. L'autorisation est donnée pour une durée de quatre semaines ; elle est renouvelable. Si la personne interceptée est soumise au secret professionnel, l'exploitation des informations implique une autre autorisation.
Le gouvernement rend compte chaque année au Parlement des interceptions effectuées dans ce contexte particulier.
Le texte, très controversé, était en contradiction avec l'article 13 de la Grundgesetz. La Constitution a été modifiée en janvier 1998 pour que le corpus sécuritaire précédemment adopté entre en application.

D) L'Espagne :

Le secret des communications est garanti par l'article 18. 3 de la Constitution : « est garanti le secret des communications spécialement par poste, télégraphe et téléphone, exception faite du mandat judiciaire ». Les interceptions judiciaires sont donc visées par la Constitution.
Par ailleurs, aux termes de l'article 55, alinéas un et deux de la Constitution, le secret des communications téléphoniques peut être suspendu lorsque l'état d'exception ou de siège est proclamé en vertu d'une loi organique réprimant l'activité des bandes armées ou de mouvements terroristes. La loi organique du 1er décembre 1980 est un arsenal anti-terroriste. Elle autorise la suspension de tout ou partie des droits fondamentaux (

inviolabilité du domicile, secret des correspondances, droit à la liberté et à la sûreté) de certaines catégories de personnes en raison de leur appartenance à des groupes incriminés ou de leur participation supposée à des actes délictueux ou criminels.
Les motifs invoqués par l'article un paragraphe un sont les délits (ou crimes) contre l'intégrité physique, les détentions illégales de personnes sous menace de rançon, la possession ou détention d'armes, munitions, explosifs, l'atteinte à la sûreté extérieure de l'Etat, les délits ou crimes qualifiés de « terroristes » par le code pénal espagnol[93].
Les autorisations d'interceptions de télécommunications sont octroyées[94], par écrit, sous forme motivée, par l'autorité judiciaire compétente. En cas d'urgence, la mesure est prise par le ministre de l'Intérieur, le directeur de la sûreté de l'Etat : le juge est informé par écrit. Il rapporte ou conforme la décision dans un délai maximal de 72 heures. L'autorisation est accordée pour une durée de trois mois qui est renouvelable. La durée maximale de la première opération d'interception est fixée à trois mois, avec renouvelabilité possible.
Le contrôle est mi-judiciaire, mi-politique. Le résultat de l'interception doit être communiqué régulièrement au juge, qui est en mesure de rapporter la décision à tout moment. De plus, l'article 7 de la loi anti-terroriste de 1980 stipule que le gouvernement tient le congrès des Députés et du Sénat, au moins tous les trois mois, plus tôt si les groupes parlementaires en effectuent la demande, afin de déterminer l'utilisation qui a été effectuée des mesures prévues par la loi et des résultats obtenus.
Les personnes intéressées ne sont pas informées lorsqu'une telle notification nuirait au bon fonctionnement de l'Etat, mais la loi prévoit la responsabilité pénale et des indemnisations en cas d'abus.
L'Espagne, après des décennies de dictature, est devenue une démocratie[95]. Les exigences de liberté se concilient avec les mesures de sécurité prévues pour soutenir la jeune démocratie.
En février 1996, un juge espagnol chargé de mener une enquête sur les interceptions de télécommunications réalisées par les services secrets a rendu une ordonnance de non-lieu : les écoutes avaient pour but la protection de l'Etat[96].
L'équilibre entre défense de l'ordre public et maintien des libertés individuelles privilégie l'ordre public : l'Espagne se considère comme une société démocratique trop fragile pour ne pas préserver sa sécurité.

E) L'Italie : a un régime mixte, avec interceptions judiciaires et interceptions de sécurité. Le code pénal permet au Parquet, après autorisation préalable du juge compétent, d'intercepter les télécommunications, et uniquement pour les délits les plus graves. En fait, le code de procédure pénal autorise les mesures d'interception pour des délits[97] graves, tels le trafic d'armes, la contrebande, mais aussi pour des délits beaucoup moins graves, tels les injures, les menaces, molestations ou troubles à la personne par le biais des télécommunications.

---

[93] De nombreuses infractions ont trait aux revendications indépendantistes ou autonomistes
[94] Article 5,§ 1 de la loi espagnole de 1980 (anti-terroriste)
[95] Sur ce thème, cf : Guy Hermet, « L'Espagne en 1975, évolution ou rupture », Fondation nationale des sciences politiques, Paris, 1997
[96] Citation du juge in Vème Rapport d'activité de la CNCIS, 1996, La Documentation française, 1997.
« Le droit à l'intimité n'est pas absolu, pas plus qu'aucun des droits fondamentaux, ceux-ci pouvant s'incliner face aux intérêts constitutionnels importants. Les écoutes n'étaient pas destinées à l'espionnage des conversations en particulier mais au contrôle d'un espace radioélectrique dans lequel une ample gamme de signaux étaient émis. De telles pratiques sont justifiées afin que les sociétés démocratiques qui sont confrontées à des formes très complexes d'espionnage et de terrorisme soient capables de se défendre efficacement contre ces menaces »
[97] Article 266 du Code de procédure pénale

Pour les interceptions judiciaires, un registre, tenu par le Procureur de la République[98] récapitule les autorisations dans l'ordre chronologique de leur adoption. Le ministère public requiert l'autorisation du juge de l'enquête préliminaire. Il peut, dans les cas d'urgence, prendre lui-même le décret motivé, qui est alors communiqué dans les vingt-quatre heures au maximum au juge ; ce dernier valide l'opération dans les quarante-huit heures, sinon l'interception ne peut être poursuivie et les résultats ne peuvent être utilisés[99]. La durée légale des interceptions n'excède pas quinze jours ; l'interception est toutefois renouvelable, elle peut être prorogée par le juge par périodes de quinze jours par décret motivé si les conditions qui ont justifié l'interception perdurent. Les interceptions de sécurité sont autorisées par le ministre de l'Intérieur, qui, par décret, valide et proroge les demandes. Le Haut commissariat de lutte contre la mafia peut également autoriser des interceptions de télécommunication à titre préventif.

F) La Belgique :

L'inviolabilité des communications téléphoniques était consacrée par la loi du 13 octobre 1930.

L'article 109terD de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques est une référence obligée en matière de protection des données dans le secteur des télécommunications. Les premier et deuxième alinéas de cet article impliquent que constituent une infraction, sauf autorisation de toutes les personnes intéressées, le fait de prendre connaissance et d'identifier ou de modifier frauduleusement les données de toute nature transmises par voie de télécommunication en provenance d'autres personnes ou destinées à celles-ci.[100]. Aux termes du troisième alinéa de cet article, constitue une infraction le fait de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne. Si l'on compare le troisième alinéa aux alinéas précédents, selon le sénateur belge M.Van Quickenborne[101], on constate la disparition du caractère frauduleux ainsi que la notion de « données en matière de télécommunications en provenance d'autres personnes et destinées à celles-ci » relatives à une autre personne. Ainsi, les données en matière de télécommunications protégées par les dispositions du troisième alinéa sont beaucoup plus larges dans la mesure où elles comportent toutes les opérations effectuées sur un réseau, indépendamment de la question de savoir si les données sont adressées à une personne ou à une autre. Cet alinéa serait en contradiction avec le principe pénal de légalité précisé à l'article sept de la Convention européenne de sauvegarde des droits de l'homme, qui stipule que les comportements et les peines punissables doivent être définis avec doivent être définis avec précision. Est-il possible de contester avec succès cette disposition devant la CEDH.

Le ministre n'est pas d'accord avec cette interprétation. Les deux premiers points de l'article 109terD sont afférents à des messages et à des données transmis par voie de télécommunications. La finalité de ces textes consiste à étendre de manière significative la garantie du secret qui existait auparavant uniquement pour les communications téléphoniques et les télégrammes. Le second point va encore un peu plus loin et met un frein à l'enregistrement et la modification de l'information ou au repérage de l'origine ou de la destination.

---

[98] Article 226 ter du Code de procédure pénale

[99] Article deux du Code de procédure pénale

[100] Toute référence au contenu ou à l'enregistrement de l'information transmise par voie de télécommunications a été supprimée par la loi du 30 juin 1994, ci-dessous mentionnée

[101] Question n° 1095 de M.Van Quickenborne du 16 janvier 2001

Le troisième point de l'article 109terD concerne les données individuelles qui se rapportent aux personnes qui utilisent des services de télécommunications. Il s'agit notamment de données de facturation, du code secret d'une personne, de la conversation des numéros qu'elle appelle. Selon le ministre[102], ce qui est en cause, ce n'est pas la garantie du secret de la télécommunication, mais la garantie des données personnelles dans le secteur des télécommunications.

Cependant, le Conseil d'Etat de Belgique n'a pas fait part de son analyse. Il n'est pas possible de trancher de manière absolue.

La loi du 30 juin 1994 intitulée « Des écoutes, de la prise de connaissance et de l'enregistrement de communications et des télécommunications privées » réglemente[103] les interceptions judiciaires ; elle est relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. La règle consiste dans l'interdiction des interceptions de télécommunications.

L'exception réside dans l'article 90terD du Code d'instruction criminelle inséré dans la loi du 30 juin 1994, qui stipule que le juge d'instruction peut enregistrer des télécommunications privées moyennant le respect de conditions strictes : intervention d'un juge d'instruction, respect du principe de proportionnalité : liste d'infractions de l'article 90ter,§2 du Code d'instruction criminelle, limitation dans le temps de la mesure : un mois maximum renouvelable avec une durée maximale de six mois. Néanmoins, en cas de flagrant délit, dans les cas de prise d'otage ou de chantage, l'interception peut être ordonnée par le Procureur du Roi. Elle est alors confirmée dans les vingt-quatre heures par le juge d'instruction. La loi du 30 juin 1994 s'applique comme dans les autres pays à l'ensemble des télécommunications, c'est-à-dire aux conversations téléphoniques et aux courriels sur Internet.

Un contrôle parlementaire existe : chaque année, un rapport est remis au Parlement au sujet de l'application des dispositions relatives à l'interception des communications et télécommunications privées[104]. Les peines prévues pour des interceptions illégales sont de un an à trois ans d'emprisonnement et de 250 000 euros. Les interceptions de sécurité ne sont donc pas, à cette époque, conformes au droit. L'interception est judiciaire. Une seule exception est notable : l'interception miliaire, effectuée à des fins militaires par le Service général du renseignement et de la sécurité des forces armées. Les interceptions militaires sont émises à l'étranger. Le fondement est l'article 44 de la loi du 30 novembre 1998 afférente aux services de renseignements et de sécurité. Le gouvernement belge, interpellé par le Conseil d'Etat, avait renvoyé la réglementation des interceptions administratives, à un projet de loi distinct, consacré à la sûreté de l'Etat. Le comité permanent de contrôle des services de renseignement[105] recommande que les services de renseignement puissent utiliser un outil légal en matière d'interceptions de télécommunications.

G) La France :

En France, les lois sur les interceptions de télécommunications sont la loi du 10 juillet 1991 et la loi du 9 mars 2004 (partie sur les enquêtes préliminaires). Une distinction est établie entre les interceptions judiciaires et les interceptions de sécurité. Les interceptions judiciaires sont, dans le cadre d'une instruction, une interception autorisée par mandat du juge d'instruction, sur la base du quantum de la peine[106], pour une durée de quatre mois,

[102] Et il reconnait qu'il s'agit d'une interprétation

[103] Cf : Vandermeesch « La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes téléphoniques », Revue de droit pénal et de criminologie belge, n° 4, avril 1995, p 301

[104] Article 90decies du Code d'instruction criminelle

[105] Comité R

[106] Deux ans d'emprisonnement

renouvelable. La réforme annoncée en 2009 des juges d'instruction va induire des modifications qui ne sont pas connues. Les interceptions de sécurité sont demandées par des services, et notamment des services de renseignement du ministère de la Défense, du ministère de l'Intérieur, du ministère en charge des Douanes, autorisées par le Premier ministre, chef de l'administration qui travaille sur ce point avec des délégués. Les interceptions de sécurité sont justifiées pour des motifs limitativement énumérés : atteinte à la sécurité nationale, prévention des actes de terrorisme, prévention de certains crimes et délits, atteinte au patrimoine scientifique et économique. Un organisme de contrôle est créé : il s'agit de la CNCIS : commission nationale de contrôle des interceptions de sécurité.

1) L'historicité :

Jacques Toubon avait élaboré un projet de constitution d'une Haute Autorité ; d'autres idées se font jour. Elles font l'objet d'ardentes discussions.

1.1) Une Haute Autorité chargée de la protection de la vie privée[107] :

Sa finalité était d'empêcher, au nom de l'intérêt public, toute intrusion intempestive et non fondée légalement dans la vie privée des personnes physiques. Elle vérifie le respect de l'intégrité des communications privées[108]à la demande de toute personne estimant avoir un intérêt pour agir. Elle peut recueillir toutes les informations, provoquer toutes les auditions qu'elle estime opportunes pour l'accomplissement de sa mission[109].

Sa composition prend en compte le principe de la double légitimité : élection et compétence.

Elle est composée[110] de neuf membres désignés pour trois ans ou pour la durée de leur mandat :

- Deux députés et deux sénateurs élus respectivement par l'Assemblée nationale et par le Sénat, à la proportionnelle des groupes.
- Un membre ou un ancien membre du Conseil D'Etat, de grade au moins égal à celui de conseiller, élu par l'Assemblée générale du Conseil d'Etat
- Deux membres ou anciens membres de la Cour de cassation de grade au moins égal à celui de conseiller, élus par l'Assemblée générale de la Cour de cassation.
- Deux personnalités désignées en raison de leur compétence dans le domaine des libertés publiques et des télécommunications et proposées par les autres membres.

Cette Haute Autorité comprend sept personnes dont une majorité de magistrats, supposés présenter des garanties particulières en matière de respect, non seulement de la loi, mais des principes généraux du droit, et des élus qui sont désignés par les partis représentés à l'Assemblée nationale et au Sénat.

Le mode de désignation s'inspire un peu du rapport Schmelck[111], un peu de la CNIL. La Haute Autorité, dans la proposition de Jacques Toubon désigne un magistrat pour présider à des investigations[112]. Elle peut ordonner la cessation immédiate d'une interception illicite et porter les faits à la connaissance du procureur de la République.

D'autres idées sont développées. Certains parlementaires souhaitent une composition relativement large. C'est l'opinion de Jean-Jacques Hyest[113], c'est celle de François d'Aubert,

[107] Titre premier de la proposition de loi de Jacques Toubon : « De la Haute Autorité chargée de la vie privée »
[108] Cf : article 6 de la proposition de loi Toubon
[109] Cf : article 7 de la proposition de loi Toubon.
[110] Cf : article trois de la proposition de loi Toubon
[111] Auquel Jacques Toubon a contribué
[112] Cf : article 7 alinéa 2 de la proposition de loi de Jacques Toubon
[113] JOAN, 1ère séance du 13 juin 1991, p 3129, 3130

de Jacques Toubon. Georges Hage demande que les membres de la commission de contrôle ne soient pas désignés par le président de la République, mais par les responsables des assemblées parlementaires, que la volonté d'indépendance se manifeste plus clairement.
Quant à la présence de magistrats[114], elle apparaît comme une caution de sérieux et d'intégrité : les magistrats sont indépendants.

1.2) De nouvelles propositions :

Jacques Toubon, fort de son expérience, va présenter de nouvelles propositions : un membre serait désigné par le président de la République. La commission comprendrait également un député, un sénateur et deux magistrats, un magistrat du Conseil d'Etat (pour la juridiction administrative), un magistrat de la Cour de cassation (pour la juridiction judiciaire). Les magistrats sont introduits dans le cénacle. Le Conseil d'Etat, dans un avis[115], a certes indiqué que la Constitution n'oblige pas à placer sous le contrôle de l'autorité judiciaire les interceptions de sécurité qui sont des mesures de police administrative ne portant pas atteinte à la liberté individuelle. Le Conseil d'Etat n'interdit pas la représentation des magistrats dans la commission. Selon Jacques Toubon, ce dosage assure la diversité des origines, l'indépendance et l'efficacité de la commission.
Les cinq personnalités éliraient un président qui ne serait pas un parlementaire. Jacques Toubon considère qu'il ne peut y avoir cumul entre une fonction élective et la présidence d'un organisme de contrôle administratif, indépendant. Ce président jouerait un rôle de filtre[116], examinerait les documents et présenterait les dossiers les plus litigieux à l'appréciation de la commission. La plupart des juristes, quand il s'est agi de créer un organisme de contrôle se sont penchés sur la CNIL. Cette commission de contrôle paraît relativement démocratique et indépendante. Elle a réalisé un assez bon travail, dans un contexte difficile, où les libertés individuelles sont souvent menacées.
Néanmoins, la CNIL ne pouvait servir de référentiel. Son champ d'intervention est beaucoup plus vaste que celui de l'organisme chargé de contrôler la légalité des interceptions de sécurité. Il en résulte que la composition de cet organisme sera plus réduite. La confidentialité des dossiers sera plus facile à observer par un petit nombre de personnes physiques. Il convient aussi d'éviter des accointances avec l'Exécutif. Autrement, il est à craindre que l'organisme de contrôle ne soit pas apte à fonctionner normalement. En ce cas, le législateur serait discrédité.

2)La CNCIS :

De la commission dépend la crédibilité du travail de légalisation des interceptions de sécurité. Jacques Toubon le réaffirme[117]. Le texte présenté[118] devant l'Assemblée nationale ne convainc pas immédiatement mais le gouvernement est certain que le compromis fait progresser l'état de droit.

2.1) Le statut de la CNCIS et de ses membres

a) La CNCIS : une autorité administrative indépendante

---

[114] Jean-Jacques Hyest : « En cas de difficultés, la commission devrait pouvoir saisir le procureur de la République lorsqu'il s'agit non pas seulement d'infractions pénales, mais aussi d'écoutes illégales qui, en tout état de cause, sont constitutives d'infractions pénales. Si elles ont été autorisées, il faut non seulement les faire cesser, mais aussi sanctionner les responsables. Une simple recommandation n'aura guère d'efficacité », JOAN, 1ère séance du 13 juin 1991, p 3130

[115] Avis du Conseil d'Etat concernant l'article 66 de la Constitution en matière de représentation de l'autorité judiciaire au sein de l'organisme de contrôle

[116] Jaques Toubon : « Il y a en gros 3200 écoutes par an et la future commission ne doit pas être obligée de siéger tous les jours pour étudier les dossiers », JOAN, 2e séance du 13 juin 1991

[117] Jacques Toubon : « Les Français étant par nature d'un scepticisme total sur toutes ces questions, nous devons éviter de leur donner des raisons de l'être. Ils doivent, au contraire, être convaincus que nous faisons tout pour que progresse l'état de droit », JOAN, 2e séance du 13 juin 1991, p 3157, 2e colonne

[118] Article 13 de la loi

Les autorités administratives indépendantes sont une innovation juridique récente dont la finalité est de parvenir à un rapprochement entre l'exécutif et les citoyens, à un contrôle[119], à une régulation[120]. C'est la loi du 6 janvier 1978 sur l'informatique et les libertés qui entérine l'expression « autorité administrative indépendante » pour évoquer la CNIL. Cette dernière a longtemps bénéficié d'un prestige considérable dans le paysage juridique français, même si les autorités administratives indépendantes ne sont ni des juridictions, ni des démembrements du pouvoir, ni des commissions de sages. La CNCIS est plus modeste que la CNIL. Le législateur est circonspect.

b) Un président prépondérant :

Selon la loi du 10 juillet 1991, la CNCIS est présidée par une personnalité désignée, en raison de son autorité[121]et de sa compétence[122], pour une durée de six ans, par le président de la République, qui agit alors comme gardien de la constitution et des libertés individuelles, se situant de par ses fonctions au-dessus des partis[123] et n'étant pas partie prenante dans les interceptions de sécurité. En théorie, le président de la commission ne peut qu'être un personnage fort, capable de s'imposer à ses collègues et surtout de faire progresser une méthodologie de réflexion, voire de conception, dans le domaine des écoutes de sécurité. L'établissement d'une liste[124] par le responsable du Conseil d'Etat, soit le vice-président du Conseil D'Etat et le Premier président de la Cour de cassation est-elle une garantie de bonne nomination ? Les personnes en charge des deux juridictions françaises, juridiction administrative, juridiction judiciaire ne peuvent que désigner un juriste reconnu par ses pairs, ayant une bonne réputation, et susceptible de ne pas déplaire au président de la République. N'y a-t-il pas risque d'autocensure ? Le Premier président de la Cour de cassation et le vice-président du Conseil d'Etat font partie des corps constitués. Ils souhaitent ne pas s'attirer l'ire silencieuse du chef de l'Etat. L'audace leur est quasi interdite ; l'absence d'audace ne signifie pas que les deux représentants des juridictions opteront pour un président falot. S'ils le faisaient, ils se déconsidéreraient eux-mêmes. Le président de la République n'est pas toujours le prince de Machiavel. Il convient de composer avec lui, mais non de plier devant lui. L'autocensure semble inévitable, mais est relativement limitée. Le président de la CNCIS est compétent dans le domaine juridique, doté d'une vaste expérience, apte à communiquer avec les premiers personnages de l'Etat.

c) Le mode de désignation des membres de la CNCIS

Le mode de désignation des autres membres de la commission pose davantage problème. Le député et le sénateur sont désignés par le président de l'Assemblée nationale et le président du Sénat. Les partis sont écartés du processus[125]. Le législateur voulait ainsi éviter tout risque de démagogie, mais il prive, au moins symboliquement, ces membres d'une légitimité élective[126]alors que cette démarche avait été adoptée, sans dommages, par la CNIL. Le domaine des interceptions de sécurité semble au législateur plus sensible que celui des fichiers automatisés.

---

[119] CADA

[120] ARCEP

[121] Reconnaissance par les pairs

[122] Diplômes et expérience professionnelle

[123] Le président de la République, parce qu'il est élu au suffrage universel, ne représente plus son parti d'origine, mais l'ensemble des Français

[124] Où le président de la République choisit le président de la commission

[125] « Les partis et les groupements politiques concourent à l'expression du suffrage ». Article 4 de la constitution de 1958

[126] Le même raisonnement s'applique à tous les membres de la CNCIS. Les hommes (ou les femmes) figurant sur la liste à partir de laquelle le président de la République choisit le président auraient pu être élus par leurs pairs.

Nommés par le président de l'Assemblée nationale et le président du Sénat qui, eux-mêmes, sont élus à leur poste dans le cadre d'une relative concorde avec le chef du gouvernement, ne risquent-ils pas d'être la voix du Premier ministre, de ne pas exercer de vision critique à l'égard des décisions prises par le chef du gouvernement ? Ce danger de dépendance a été mentionné à l'occasion de la désignation des membres du CSA. Certains juristes répondent que « la fonction fait l'homme ». Le membre de la CNCIS s'applique à mériter la confiance de l'organisme de contrôle[127]. De plus, il est irrévocable, et son mandat n'est pas renouvelable. D'éventuelles pressions seraient sans effet. L'irrévocabilité et la non-renouvelabilité du mandat sont les contreparties de la désignation par les présidents de l'Assemblée nationale et du Sénat. Il est peu probable que l'exécutif provoque la démission d'un membre de la CNCIS devenu indésirable. C'est la CNCIS elle-même qui constaterait un éventuel empêchement. L'organisme, dans sa dimension collective, paraît à l'abri de toute dérive.

En revanche, le régime des incompatibilités est quelque peu limité puisqu'il se contente d'interdire le cumul d'un mandat avec le poste de membre du gouvernement. Il n'est pas prévu que les membres de la CNCIS ne doivent posséder aucun intérêt[128] dans le matériel des interceptions de sécurité. Or, ce genre de dispositions est souvent inclus dans le statut des membres des organismes de contrôle et de régulation. Il est vrai qu'en 1991, la question des matériels paraissait relativement secondaire, surtout par comparaison avec le contrôle de la légalité des motifs. Enfin, la CNCIS n'est pas une entité régulatrice.

Jacques Toubon présente un amendement[129] qui remodèle la composition de la CNCIS. Cette dernière comprendrait les trois membres envisagés par le gouvernement et deux magistrats, élus par l'Assemblée générale du Conseil d'Etat et de la Cour de cassation. Le président serait choisi parmi les non-parlementaires. Dans cette modélisation, il n' y a pas de corrélation entre le mode de désignation des parlementaires et le mode de désignation des magistrats. François Massot[130]plaide dans ce sens mais ne convainc pas Jacques Toubon. Ce dernier rappelle que, dans les organismes de contrôle, la désignation repose souvent sur le mode électoral tant pour les parlementaires que pour les magistrats. Parce qu'il n'est prévu qu'un seul député, un seul sénateur, la désignation est politique. L'attelage comprend alors des politiques et des juristes.

La commission des lois, a priori, n'est pas totalement convaincue par le mode de désignation politique. Le garde des Sceaux concède que des magistrats pourraient être introduits dans la commission de contrôle, à condition qu'ils soient désignés par les autorités responsables du Conseil d'Etat et de la Cour de cassation. Dans ces conditions, le président pourrait être choisi

---

[127] Sur le statut de membre du CSA, voir les articles 1er et 4 de la loi du 30 septembre 1986

[128] Incompatibilité avec des intérêts directs ou indirects (actions, obligations)

[129] Amendement n° 47 présenté par Jacques Toubon : « Il est constitué une commission de contrôle des interceptions de sécurité publique. Cette commission est une autorité administrative indépendante. Elle estchargée de veiller au respect des dispositions du présent titre. Elle est composée de cinq membres nommés pour trois ans ou pour la durée de leur mandat :

- une personnalité désignée, en raison de son autorité et de sa compétence, par le président de la République
- un député désigné par le président de l'Assemblée nationale
- un sénateur désigné par le président du Sénat
- un membre ou un ancien membre du conseil d'Etat, de grade au moins égal à celui de conseiller, élu par l'Assemblée générale du Conseil d'Etat
- un membre ou un ancien membre de la Cour de cassation, de grade au moins égal à celui de conseiller, élu par l'Assemblée générale de la Cour de cassation

La Commission élit en son sein, parmi ses membres non parlementaires, pour trois ans, un président, JOAN, 2ème séance du 13 juin 1991, p 3158, 2e colonne

[130] François Massot : « Un système identique serait préférable : ces deux conseillers devraient chacun être désignés par le président de leurs assemblées », JOAN, 2ème séance du 13 juin 1991, p 3158, 2e colonne

parmi les non-parlementaires[131]. Référence est faite à la commission chargée de contrôler les comptes des partis politiques et des campagnes électorales[132]. Cette allusion fait réagir plusieurs parlementaires qui préfèrent nettement le modèle de la CNIL, favorable au principe électif.

Un amendement de François d'Aubert et de Paul-Louis Tenaillon tend à favoriser le principe électif, au bénéfice de magistrats[133]. Un amendement de J-J Hyest introduit des magistrats mais sans référence à la désignation élective, qui se heurte à l'hostilité du gouvernement[134]. L'amendement n°77 est adopté. Le président est élu pour six ans. François Massot propose un amendement rédactionnel[135]. Parce que le mandat des membres de la commission n'est pas renouvelable, il faut envisager le cas où un membre de la commission serait désigné pour remplacer une personnalité ayant cessé ses fonctions avant le terme. L'amendement est adopté.

Après le vote à l'Assemblée nationale, la nouvelle commission est très différente de celle qui avait été conçue par le gouvernement. Un examen en commission des lois, un vote du Sénat permettent de revenir aux sources, avec quelques aménagements.

La commission des lois renvoie dos à dos le dispositif gouvernemental et le dispositif de l'Assemblée nationale. L'augmentation du nombre des membres de la commission est inadaptée aux finalités. Le principe électif induit un dysfonctionnement : le président serait élu par cinq personnalités, dont deux seraient inéligibles[136]. La commission des lois propose que le nombre des membres de la commission soit réduit à trois et et que le président soit une personnalité désignée par le premier président de la Cour de Cassation et le vice-président du Conseil d'Etat.

Michel Dreyfus-Schmidt, au nom du parti socialiste, élabore une contre-proposition[137] : le président serait un magistrat, qui travaillerait à plein temps, il serait un filtre institutionnel et serait désigné par le président de la République. La magistrature serait donc représentée par le premier personnage de la CNCIS. Le député et le sénateur seraient nommés par les présidents

---

[131] Henri Nallet : « Cette notification de la composition de la commission de contrôle rendrait dès lors possible, ce qui est souhaitable, que le président de la commission de contrôle soit désigné par les commissions non-parlementaires », JOAN, 2ème séance du 13 juin 1991, p 3159, 1e colonne

[132] Idem : « Je pense notamment à la commission chargée, aux termes de la loi de 1990, de contrôler les comptes des partis politiques et des campagnes électorales, et dont les deux membres issus de la Cour de cassation et du Conseil d'Etat sont désignés par leurs présidents », JOAN, 2ème séance du 13 juin 1991, p 3159, 1ère colonne

[133] L'amendement n°68, présenté par François d'Aubert et Paul-Louis Tenaillon, est ainsi rédigé : « Après le 5e alinéa de l'article 14, insérer les alinéas suivants : « Un conseiller d'Etat élu par l'Assemblée générale du Conseil d'Etat pour une durée de six ans ; deux conseillers de la Cour de cassation élus par l'Assemblée générale de la Cour de cassation pour une durée de six ans », JOAN, 2ème séance du 13 juin 1991, p 3159, 2ème colonne

[134] L'amendement n° 77, présenté par M.Hyest et les membres du groupe de l'Union du centre, est ainsi rédigé : « Après le cinquième alinéa de l'article 14, insérer les alinéas suivants : « Un conseiller d'Etat élu par l'Assemblée générale du Conseil d'Etat pour une durée de six ans ; deux conseillers de la Cour de cassation élus par l'Assemblée générale de la Cour de cassation pour une durée de six ans », JOAN, 2ème séance du 13 juin 1991, p 3159, 2ème colonne

[135] Un amendement de François Massot n° 14, ainsi rédigé : « Les membres de la commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. A l'expiration de ce mandat, par dérogation au huitième alinéa ci-dessus, ils peuvent être nommés comme membres de la commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans », JOAN, 2ème séance du 13 juin 1991, p 3160, 2ème colonne

[136] Les parlementaires, les membres du Sénat et de l'Assemblée nationale

[137] L'amendement n° 41, présenté par Michel Dreyfus-Schmidt, les membres du groupe socialiste et apparentés, est ainsi rédigé : « La commission est présidée par un membre ou un ancien membre de la Cour de cassation ou du Conseil d'Etat de grade au moins égal à celui de conseiller désigné par le président de la République pour une durée de six ans. Elle comprend en outre, un député et un sénateur désignés par les présidents du Sénat et de l'Assemblée nationale en tenant compte de l'équilibre entre les assemblées et de la diversité de leur composition. Le député est désigné pour la durée de la législature, le sénateur après chaque renouvellement partiel du Sénat », JO Sénat, séance du 25 juin 1991, p 2086, 1ère colonne

de l'Assemblée nationale et du Sénat, avec un équilibre entre les majorités et les oppositions. D'après Michel Dreyfus-Schmidt, le Conseil constitutionnel n'a rempli pleinement sa mission qu'à partir du moment où ses membres n'appartenaient pas à la même famille politique[138]. Il ne s'agit pas de renouveler cette erreur.

La commission des lois souligne qu'un président désigné par le président de la République ne pourrait être considéré comme indépendant[139]. Le Sénat n'est pas convaincu. De même, il semble impensable de donner des directives au président de l'Assemblée nationale quant aux nominations.

La commission mixte paritaire se réunit. Un compromis est trouvé sur la présidence. La commission est présidée par une personnalité désignée, pour une durée de six ans, par le président de la République sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'Etat et le premier président de la Cour de cassation[140]. Une décision est prise pour qu'un équilibre soit instauré entre la représentation sénatoriale et la représentation de l'Assemblée nationale. Si le député nommé par le président de l'Assemblée nationale appartient en 1991 à l'UDF ou au RPR, le sénateur sera socialiste ou inversement.

Le législateur s'est refusé à institutionnaliser le rôle de l'opposition, dont les méandres, les contours, les stratégies sont très différents de ce qui existe en Allemagne ou en Grande-Bretagne, où la minorité compose un cabinet fantôme. Néanmoins, la cohabitation de ces deux élus[141]est une garantie d'équilibre pour la démocratie. Enfin, le député et le sénateur sont les délégués des autorités constitutionnelles que sont le président du Sénat[142] ou le président de l'Assemblée nationale ; les mandats sont assurés jusqu'au renouvellement effectif.

Les collaborateurs des membres de la CNCIS contribuent, eux aussi, à l'image de la CNCIS.

La présence d'un commissaire du gouvernement était prévue dans le projet de loi. Elle ne paraît pas utile à l'Assemblée nationale[143]. Dans une commission indépendante, un commissaire du gouvernement, même s'il ne siège pas au moment des délibérations, risquerait d'être mal perçu.

Le garde des Sceaux fait valoir que ce commissaire n'interviendra pas dans le fonctionnement de la commission, mais facilitera son travail[144]. Devant le Sénat, l'amendement Jacques Thyraud[145] tente de rétablir l'institution du commissaire du gouvernement. Le rôle du

---

[138] Michel Dreyfus-Schmidt : « Le Conseil constitutionnel n'a pas rempli le rôle que l'on attendait de lui tant que ceux qui désignaient les hommes appelés à y siéger furent de la même couleur politique : il y avait une trop grande homogénéité », JO Sénat, séance du 25 juin 1991, p 2085, 2ème colonne

[139] Marcel Rudloff : « A l'heure actuelle, et sans doute pour de longues années encore, une personnalité désignée par le président de la République sera à jamais considérée par l'opinion publique et par les usagers du droit comme insuffisamment indépendante. Il faut regarder les choses en face », JO Sénat, séance du 25 juin 1991, p 2086, &ère colonne

[140] Article 13 définitif de la loi du 10 juillet 1991

[141] Quand le président Jacques Chirac décida de dissoudre l'Assemblée nationale en 1997, le député désigné et délégué par le président de l'Assemblée nationale continua à assumer ses fonctions jusqu'à l'élection d'un nouveau président de l'Assemblée nationale et la désignation d'un nouveau membre dans la CNCIS

[142] Habilité à assurer l'intérim du chef de l'Etat en cas de décès

[143] Un amendement n° 15, présenté par François Massot, est ainsi rédigé : « Supprimer le dernier alinéa », JOAN, 2ème séance du 13 juin 1991, 2ème colonne

[144] Henri Nallet : « Le commissaire du gouvernement ne délibère pas, il est là pour faciliter le travail de la commission, pour servir de lien, pour lui donner des informations. Afin d'offrir des garanties complémentaires aux citoyens, la commission aura intérêt à avoir affaire à un commissaire du gouvernement, qu'elle pourra interroger. Celui-ci, spécialisé, assurera la transparence et permettra à la commission d'entretenir, sur le plan de l'information, de meilleures relations avec l'autorité publique, qui décide des interceptions. Sans vouloir être paradoxal, je dirai qu'il serait très utile, pour que soient mieux défendus, mieux protégés les citoyens, qu'un commissaire du gouvernement siège auprès de la commission », JOAN, 2ème séance du 13 juin 1991, p 3160, 2ème colonne

[145] L'amendement n° 28 présenté par M.Thyraud est ainsi rédigé : « Un commissaire du gouvernement désigné par le Premier ministre siège auprès de la commission », JO Sénat, séance du 25 juin 1991, p 2084, 2ème colonne

commissaire sera conforme à celui qui s'exerce au sein de la CNIL, sans aucun danger pour cet organisme de contrôle. A la CNIL, le commissaire présente les dossiers, est un interlocuteur officiel, mais n'a pas de voix délibérative. Certes, la CNIL comprend beaucoup plus de membres que la CNCIS : l'activité du commissaire du gouvernement n'en sera que plus précieuse à la CNCIS. L'amendement n'en est pas moins repoussé. Il n'y aura pas de commissaire de gouvernement à la CNCIS.

Les rapporteurs

Un amendement présenté devant l'Assemblée nationale[146]propose l'institution de rapporteurs qui seraient désignés parmi des membres des grands corps et qui faciliteraient les travaux des membres de la CNCIS. Le législateur ne tient pas à alourdir, même indirectement, le texte des lois. La présence de rapporteurs est finalement perçue comme superfétatoire.

Le règlement intérieur

A l'Assemblée nationale, François Massot propose l'établissement d'un règlement intérieur[147]. Cette amélioration rédactoriale est acceptée, dans un souci de sécurité juridique, votée, dans les mêmes termes par l'Assemblée nationale et le Sénat. Le règlement intérieur est adopté en 1998.

Devant le Sénat, M.Le Breton et les membres du groupe de l'Union centriste proposent d'insérer l'alinéa ainsi formulé[148] : « Des agents de la commission sont nommé par le président ». Cet alinéa, s'il provient du Sénat, va dans le même sens que l'Assemblée nationale : la commission, autorité indépendante, doit pouvoir, sous la responsabilité de son président, disposer de son personnel. Il s'agit d'une nouvelle amélioration rédactoriale. L'amendement est voté sans difficulté. La seule réserve est émise par Henri Nallet, alors garde des Sceaux : elle concerne la provenance de ces agents[149]. Cette remarque peut renvoyer à un acte réglementaire. La composition finale est don assez proche de la composition initiale. La fluctuation, les navettes ont pourtant permis de clarifier certains choix et d'affiner certains alinéas. Les membres de la CNCIS, autres que le président, sont désignés selon le principe de parité majorité/ opposition explicité plus haut[150].

Les deux premiers membres furent les rapporteurs de la loi de 1991, François Massot, député des Alpes-de-Haute-Provence, avocat au barreau de Paris, Marcel Rudloff (UDF-UC), sénateur du Bas-Rhin, ancien bâtonnier du barreau de Strasbourg[151]. Ces hommes souhaitaient, au même titre que Paul Bouchet, que la CNCIS fût une autorité prise en considération. Marcel Rudloff ayant été nommé au Conseil constitutionnel, il fut remplacé par Jacques Thyraud, avocat au barreau de Romorentin, sénateur du Loir-et-Cher, premier vice-président de la CNCIS. Jacques Thyraud fut très actif lors de la discussion de la loi.

Ces personnalités étaient à même de se dévouer pour la CNCIS. Elles tenaient toutes à ce que l'organisme de contrôle fût dynamique, efficace, maintint un équilibre entre ordre public et libertés individuelles. Quelle que soit l'intégrité d'une personne, cette dernière ne peut travailler avec pertinence si ces fonctions sont mal définies.

---

[146] L'amendement n° 69 présenté par François d'Aubert et Paul-Louis Tenaillon est ainsi rédigé : « La commission peut se faire assister par des rapporteurs désignés par son président parmi les membres du Conseil d'Etat, de la Cour des comptes, de l'Inspection générale des finances. Les rapporteurs sont astreints au respect du secret dans les mêmes conditions que les membres de la commission », JOAN, 2ème séance du 13 juin 1991, p 3161, 1ère colonne

[147] Amendement n° 16, présenté par François Massot : « La commission établit son règlement intérieur », JOAN, 2ème séance du 13 juin 1991, p 3161, 1ère colonne

[148] L'amendement n° 44 rectifié, présenté par M.Le Breton et les membres de l'Union centriste, est ainsi rédigé : « Les agents de la commission sont nommés par le président », JO Sénat, séance du 25 juin 1991, p 2089, 2ème colonne

[149] Henri Nallet, JO Sénat, séance du 25 juin 1991, p 2091, 1ère colonne

[150] Vœu unanime de la commission mixte paritaire repris par le ministre délégué à la justice lors de l'adoption par le Sénat des conclusions de cette commission.

[151] Les premiers membres sont des juristes : non pas des magistrats, mais des avocats

2.2) L'Etat de droit, les fonctions de la CNCIS, la sécurité

La commission n'a de justification que si elle exécute correctement son travail de contrôle.

a) Le contrôle des autorisations du Premier ministre

Une délivrance des autorisations en concordance avec les motifs

Ce contrôle des autorisations, même s'il ne se traduit pas par des sanctions, justifie l'existence de la CNCIS : il s'agit de déterminer si la délivrance des autorisations est en concordance avec les motifs.

Les parlementaires vont contribuer à l'élaboration de l'article consacré au contrôle des autorisations. François Massot[152] et Jacques Toubon[153]vont y jouer un rôle éminent. Tous deux définissent les modalités de contrôle des autorisations en se référant à un ancien article 16. Une passe d'armes parlementaires a lieu. François Massot, dans un premier temps, déclare retirer son amendement à condition que Jacques Toubon consente à substituer à « communications » « correspondance par voie de communications » et à supprimer « communications privées » et substituer « illégalité » à « illicéité ».

Devant l'objection du garde des Sceaux, qui souligne que l'amendement de Jacques Toubon est imprécis, François Massot mentionne la possibilité d'une fusion, puis souligne les aspects positifs de son propre texte. Jacques Toubon s'est déclaré, entre temps, hostile à l'expression « problème de légalité » entériné par le Conseil d'Etat. Jacques Toubon rappelle que l'avis du Conseil d'Etat ne lie pas le gouvernement. Un trop long délai d'intervention est dangereux[154].

L'amendement Massot est adopté. Une lecture du texte permet de remarquer que la loi utilise le mot « peut » (au cas où la commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle peut s'adresser au Premier ministre) et non le mot « doit ».. Cela signifie-t-il que la commission, qui remplit une mission de contrôle, n'a pas l'obligation de recommander au Premier ministre d'interrompre l'interception ? Jacques Thyraud[155]souhaite transformer le « peut » en « doit », autrement dit, en jargon juridique[156] : « peut adresser » devient « adresse ».

Jacques Thyraud insiste : il serait anormal qu'après avoir constaté des irrégularités, la commission n'en tire pas la conséquence. Le rapporteur Marcel Rudloff déclare que cette obligation est une charge pour la commission, libre, responsable, et, en tant que telle, habilitée à décider si elle attire ou non l'attention du Premier ministre. L'amendement est finalement voté.

---

[152] Un amendement n° 17, présenté par François Massot, est ainsi rédigé : « Insérer l'article suivant : « La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de 48 heures au plus tard au président de la CNCIS. Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa. Au cas où la commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle peut adresser au Premier ministre une recommandation tendant à ce que cette interception soit interrompue. Il est alors procédé ainsi qu'il est indiqué aux deuxième et troisième alinéas de l'aricle 16 », JOAN, 2ème séance du 13 juin 1991, p 3161, 2ème colonne

[153] Un amendement n° 48 présenté par Jacques Toubon est ainsi rédigé : « Toute personne peut demander à la commission la vérification du respect de l'intégrité de ses communications privées. Le Premier ministre communique sans délai au président de la commission les décisions concernant les autorisations. Si le président de la commission en décide ainsi, la commission se réunit pour statuer sur la légalité de l'interception. Si la commission estime que l'interception est illégale, elle adresse au Premier ministre une recommandation tendant à ce que l'interception soit interrompue et porte les faits à la connaissance du procureur de la République. La commission statue dans les 24 heures qui suivent la communication prévue au deuxième alinéa du présent article », JOAN, 2ème séance du 13 juin 1991, p 3101, 2ème colonne

[154] Jacques Toubon : « Si une personne est mise pendant quatre ou cinq jours sur écoute et que l'on s'aperçoit ensuite qu'il ne fallait pas le faire, que se passera-t-il ? », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

[155] Amendement de Jacques Thyraud n° 29, JO Sénat, séance du 25 juin 1991, 1ère colonne

[156] Le présent a une valeur impérative

L'ancien article 16 est supprimé. L'alinéa suivant est proposé : « La commission porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et au ministre chargé des télécommunications ».
Le Premier ministre informe sans délai la commission des suites données à la recommandation[157]. Certains parlementaires voudraient que la commission eût des prérogatives plus importantes. Les recommandations semblent insuffisantes. Une injonction aurait été efficace mais elle s'avère impossible puisque le gouvernement dispose de l'administration et que la commission, autorité administrative, ne peut ordonner au Premier ministre d'interrompre une interception de sécurité qu'elle considérerait comme illégale (avis du Conseil d'Etat).
Recommandations et contingentement
Les recommandations sont pertinentes : comme le souligne Michel Dreyfus6Schmidt, la commission doit avoir la possibilité d'attirer l'attention du Premier ministre sur les inflexions de sa politique en matière de contingentement[158].
Henri Nallet, garde des Sceaux, réagit assez vivement : la commission peut toujours adresser au Premier ministre des observations et ce sur tous les sujets qu'elle juge utile, y compris le contingentement. Il est donc inutile d'envisager une recommandation. Le terme « recommandation » aurait plus d'impact s'il n'était relatif qu'à la régularité des interceptions[159].
Michel Dreyfus-Schmidt a en tête le scénario suivant : le Premier ministre décide de doubler ou de tripler le contingent. Cette augmentation bouleverse l'économie des interceptions de sécurité. Dans ce cas, la CNCIS doit adresser immédiatement, non pas une observation, mais une recommandation à laquelle le Premier ministre sera tenu de répondre immédiatement. Elle n'attendra pas la remise du rapport.
Le Sénat a su faire preuve d'imagination et anticiper sur des situations imprévisibles qui causeraient des dommages aux libertés individuelles.
b) Le contrôle des interceptions de sécurité, les réclamations, les rapports de la CNCIS
Le contrôle des interceptions de sécurité à l'initiative de la CNCIS ou sur réclamation
Le gouvernement présente un article 15[160] et un article 16[161].
Les initiatives de la CNCIS
La commission procède au contrôle des écoutes et vérifie s'il y a conformité avec les dispositions précédentes. Un député et un groupe parlementaire demandent l'accès direct aux

[157] Amendement n° 58, présenté par le gouvernement devant le Sénat, JO Sénat, séance du 25 juin 1991, p 2092, 2ème colonne
[158] Un amendement n° 42 rectifié, présenté par Michel Dreyfus-Schmidt et les membres du groupe socialiste et apparentés, est ainsi rédigé : « Entre le premier et le second alinéa du texte proposé par l'amendement n° 8 pour remplacer le dernier alinéa de l'article 14 bis, insérer un alinéa ainsi rédigé : « La commission peut notifier au Premier ministre une recommandation concernant le contingent et sa répartition ». Un amendement n° 43 rectifié, présenté par Michel Dreyfus-Schmidt et les membres du groupe socialiste et apparentés, substitue aux mots « sa recommandation » les mots « ses recommandations », JO Sénat, séance du 25 juin 1991, p 2092, 2ème colonne ; p 2093, 1ère colonne
[159] Henri Nallet : « Il semble préférable de réserver l'emploi du mot « recommandation » aux observations de la commission qui portent sur la régularité des interceptions » », JO Sénat, séance du 25 juin 1991, p 2093, 1ère colonne
[160] Projet d'article 15 : « De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du présent titre », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne
[161] Projet d'article 16 : « Si la commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que celle-ci soit interrompue. Cette recommandation est notifiée au Premier ministre, au ministre ayant proposé l'interception et au ministre chargé des télécommunications. Le Premier ministre informe la commission des suites données à sa recommandation », JOAN, séance du 13 juin 1991, p 3163, 2ème colonne

informations nominatives recueillies par voie d'écoutes téléphoniques. Cette exigence s'inspire de la loi du 6 janvier 1978 « Informatique et libertés » qui protégeait les données nominatives et prévoyait un droit d'accès pour les personnes physiques. Le procédé des interceptions de sécurité est assimilé aux fichiers automatisés. Une différence est cependant notable : le fichier automatisé appartient au droit commun et est utilisé par le droit commercial. L'interception de sécurité, soumise au droit public, défend l'ordre public.
George Hage craint un risque d'arbitraire. Ce point, apparemment secondaire, restera litigieux tout au long des années 1990. Deux logiques, qui se sont conciliées dans la loi de 1991, apparaissent antagonistes : la logique de l'ordre public, sécuritaire[162], et la logique des droits de l'homme[163].
A l'Assemblée nationale, l'illustration est claire : elle se réfère à la mafia. Parce que la mafia menace l'ordre public, aucun membre de la mafia ne peut avoir connaissance des interceptions dont il serait l'objet[164]. La réponse ne cherche pas l'esquive : même un membre de la mafia sera protégé par les droits de l'homme[165]. Il n'existe pas de citoyen rejeté hors des libertés individuelles, constitutives du régime démocratique. Pour la majorité de l'Assemblée nationale, un tel raisonnement met en cause l'interception de sécurité elle-même. L'amendement est rejeté.
D'autres discussions portent sur des points qui relèvent, non pas de l'idéologie, mais de l'élargissement du contrôle. La commission des lois désire étendre la portée du contrôle afin de ne pas entraver la vérification des interceptions de sécurité décidées par le Premier ministre[166]. Le gouvernement n'est pas opposé à cette initiative, mais rappelle qu'il ne faut pas aller au-delà du contrôle de légalité envisagé dans le texte du projet de loi[167]. Les amendements sont adoptés, mais le texte définitif reprendra le texte initial. Ce dernier est en revanche complété par un sous-amendement[168] présenté par le gouvernement et qui est adopté sans difficultés. Il reprend l'ancien article 16. En cas de violation de la loi, la commission demande au Premier ministre de faire interrompre l'interception de sécurité.
Le régime particulier des réclamations :

---

[162] François Massot : « La commission a estimé que l'amendement était incompatible avec les exigences de la défense nationale et de la sécurité publique », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

[163] Jean-Marie Daillet : « A partir du moment où une personne est mise en cause, comment, pour des raisons dites de défense nationale, pourrait-on lui refuser le droit de savoir ce qu'il en a été ? Un tel droit fait partie des droits de l'homme », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

[164] Gérard Gaizes : « Je ne peux croire que M.Daillet accepte qu'un responsable de la mafia puisse ainsi demander des explications sur des écoutes dont il aurait fait l'objet sur sa ligne personnelle », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

[165] Jean-Marie Daillet : « Même un responsable de la mafia a le droit, comme tout citoyen, de savoir pour quelles raisons il est interrogé. Il ne s'agit pas de défendre ici la mafia ou les criminels », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

[166] L'amendement n° 18 présenté par François Massot est ainsi rédigé : « Après les mots : « procéder à », rédiger ainsi la fin de l'article 15 : « Tout contrôle nécessaire à la vérification du respect des dispositions du présent titre », JOAN, 2ème séance du 13 juin 1991, p 3163, 1ère colonne

[167] Un sous-amendement n° 81 (amendement n° 18) est présenté par le gouvernement : « Dans l'amendement n° 18, substituer au mot «du respect », les mots « de la légalité d'une décision d'interception et de ses conditions d'exécution au retard », JOAN, 2ème séance du 13 juin 1991, p 3163, 1ère colonne. Henri Nallet : « Par sous-amendement, le gouvernement précise que le contrôle effectué dans le cadre de l'article 15 est bien un contrôle de légalité, et qu'il s'étend bien évidemment tant à la décision d'interception qu'à ses conditions d'exécution, ainsi que je l'ai indiqué dans mon intervention générale », JOAN, 2ème séance du 13 juin 1991, p 3163, 1ère colonne

[168] Un sous-amendement n° 59 rédigé par le gouvernement, tendant à compléter le texte proposé par l'amendement n° 13 est ainsi rédigé : « Si la commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que celle-ci soit interrompue », JO Sénat, séance du 25 juin 1991, p 2093, 2ème colonne

Certains particuliers supposent qu'ils subissent une interception de sécurité. Dans l'indécision, ils déposent une réclamation auprès de la CNCIS, pour que cette dernière procède à des vérifications. Les intéressés souhaitent évidemment des retours d'information. Ces derniers ne sont pas prévus. La commission est tenue de procéder à des vérifications, comme elle l'aurait fait si elle s'était autosaisie. Elle notifie aux particuliers que le travail a été effectué[169]. Elle ne peut d'ailleurs agir autrement. Une autorité administrative est tenue de répondre au courrier, et notamment à une réclamation.
Cela ne signifie pas que le particulier sera satisfait. Une personne physique, même si elle connaît le droit et la loi, saisit un organisme de contrôle avec l'espoir que sa démarche lui permettra de déterminer si l'écoute supposée a eu effectivement lieu[170]. L'ignorance induit une frustration.
Le législateur, quant à lui, n'est pas préoccupé par des fantasmes. Il doit être le plus précis possible. La CNCIS, si elle constate une infraction, saisira le procureur de la République[171]. Cela est conforme au droit commun et n'exige peut-être pas un rappel[172]. Toutes les autorités publiques saisissent sans délai le procureur de la République, lorsqu'elles constatent une infraction : cela correspond au code de procédure pénale[173]. Un ajout peut paraître inutile. Au demeurant, la question s'est déjà posée de savoir si un alinéa de référence au droit commun devait être conservé : à l'occasion des articles 2 et 12, la commission des lois a proposé le retrait d'un texte élaboré par le gouvernement. Ce dernier a suivi les recommandations de la commission des lois. Dans le cas présent, le contexte n'est pas le même. Il s'agit d'un rappel. Cet amendement valorise les libertés individuelles. Parce que la CNCIS est un organisme de contrôle garant des libertés individuelles, l'adjonction de la phrase se référençant au code de procédure pénale est une répétition tacite, mais aussi une métaphore : elle démontre, à titre symbolique, que si l'organisme de contrôle ne perd jamais de vue l'intérêt général, l'ordre public [174] ne sacrifie pas les droits de l'homme sur l'autel des efforts demandés par l'Etat. Ce dernier a besoin de se défendre, y compris par la prévention : les interceptions de sécurité font partie des moyens mis à sa disposition pour cette finalité. Les citoyens ne sont cependant pas oubliés. Par un contrôle diligent du régime des autorisations et des interceptions de sécurité, la CNCIS parviendra à concilier les aspirations explicites et diffuses de l'Etat et des défenseurs des droits de l'homme. Elle se crédibilise ainsi dès sa création. Le droit commun s'applique à tous[175]. Si la loi n'est pas respectée, la CNCIS se fait un devoir de saisir le Parquer qui remplit sa mission.
Les rapports :

---

[169] Article 17 : « Lorsque la commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires », JOAN, 2ème séance du 13 juin 1991, p 3163, 2ème colonne

[170] Même si cela n'est pas pertinent, et comme cela a été traduit par l'amendement du groupe communiste, la plupart des particuliers sont convaincus qu'ils sont en droit de savoir s'ils sont interceptés et pourquoi. Au vide juridique succéderait une transparence lumineuse. Cette idée qui relève du fantasme dans le domaine des écoutes de sécurité, a préoccupé bien des esprits.

[171] L'amendement n° 17, présenté par François Massot, est ainsi rédigé : « Compléter l'article 17 par l'alinéa suivant : « Conformément au deuxième alinéa de l'article 40 du code de procédure pénale, la commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contexte visé en application de l'article 15 », JOAN, 2ème séance du 13 juin 1991, p 3163, 2ème colonne

[172] Le ministre délégué à la justice : « cela va sans dire ». Le garde des Sceaux : « je ne sais pas si cela va mieux sans le dire ou en le disant, JOAN, 2ème séance du 13 juin 1991, p 3163, 1ère colonne

[173] Deuxième alinéa de l'article 40 du code de procédure pénale

[174] L'ordre public est représenté par l'interception de sécurité, exception au secret des correspondances

[175] Principe d'égalité : en droit, équilibre entre individus et biens.

Par leur caractère public, ils permettent aux corps constitués, aux autorités publiques, à la société civile, de se forger une opinion sur le travail du Premier ministre et la réalité tangible des activités initialisées et exécutées par la CNCIS.
Cette pratique des rapports repose en France sur une historicité. Par ailleurs, le rapport apporte une lumière sur des questions souvent laissées dans l'ombre. Ainsi, le rapport de la Cour des comptes, qui fait l'objet de nombreux commentaires, est médiatisé. Détourné de sa finalité par certains journalistes, il est aussi un instrument de dénonciation d'une prétendue gabegie du service public. Les rapports de la CNIL[176]constituent un support obligé pour les juristes spécialisés dans le droit de l'informatique, du multimedia et pour tous ceux qui s'intéressent à l'éventuelle dilution des libertés individuelles dans l'extension des fichiers informatisés. Plus récemment, l'ART, puis l'ARCEP, organisme de contrôle mais aussi autorité de régulation, a rendu publics des rapports[177] qui permettent d'envisager l'évolution des télécommunications, puis des communications électroniques.
Le rapport de la CNCIS[178] revêt un caractère d'annualité, comme tous les autres rapports précédemment mentionnés. Il est remis au Premier ministre, mais aussi présenté au président de l'Assemblée nationale et au président du Sénat qui, tous deux, nomment un membre de la commission, peuvent prendre connaissance du travail réalisé et se voient rappeler une responsabilité éminente. Ce rapport est accompagné d'une lettre qui en résume les grands axes et donne la tonalité générale des impressions et des données rassemblées. Chaque mot est longuement soupesé par les services du CNCIS.
Les recommandations, à défaut d'infractions, traduisent la volonté de faire respecter la loi en cas de dérive momentanée. Le nombre des recommandations apparaîtra dans le rapport[179]. Il convient de renforcer la portée de la recommandation[180] puisqu'elle n'est pas obligatoirement suivie d'effets. Les observations complètent les recommandations[181]. Leur importance se doit d'être reconnue par la loi[182]. Les amendements sont adoptés par l'Assemblée nationale. Le texte définitif retient la mention faite aux observations. Ces dernières sont aussi utiles que les recommandations. Le rapport est accessible au public[183] qui peut ainsi se tenir au courant, par une source directe, et non indirecte, de la trajectoire des interceptions de sécurité.
Les moyens de la CNCIS
Ils sont relativement modestes.
Le personnel

[176] Ce rapport de la CNIL a été créé par la loi du 6 janvier 1978
[177] Le rapport de l'ART a été institué par la loi du 26 juillet 1996. Sa première publication a eu lieu en juin 1998
[178] Projet d'article 19 : « La commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité. Ce rapport est rendu public », JOAN, 2ème séance du 13 juin 1991, p 3104, 1ère colonne
[179] Un amendement n° 21 de François Massot est ainsi rédigé : « Compléter la première phrase de l'article 19 par les mots « qui précise notamment le nombre de recommandations qu'elle a adressées au Premier ministre et les suites qui leur ont été données », JOAN, 2ème séance du 13 juin 1991, p 3164, 1ère colonne
[180] François Massot : « La commission des lois a pensé qu'il fallait préciser le contenu du rapport. La commission nationale de contrôle adresse, chaque année, au Premier ministre un rapport pour donner plus de portée au pouvoir de recommandation qui lui est reconnu par la loi », JOAN, 2ème séance du 13 juin 1991, p 3164, 2ème colonne
[181] Amendement n° 22, présenté par François Massot, Gérard Gaizes, Jean-Pierre Michel : « Compléter l'article 19 par l'alinéa suivant : « Elle adresse, à tout moment, au Premier ministre, les observations qu'elle juge utiles », JOAN, 2ème séance du 13 juin 1991, p 3164, 2ème colonne
[182] François Massot : « Dans le droit fil du précédent amendement, nous avons estimé que le rapport annuel prévu à l'article 19 ne devait pas être le seul moyen offert à la commission de contrôle de saisir le Premier ministre des conditions dans lesquelles elle exerce son activité. Nous proposons donc qu'elle puisse, à tout moment, lui adresser les observations qu'elle juge utiles », JOAN, 2ème séance du 13 juin 1991, p 3164, 2ème colonne
[183] Le rapport, publié par la Documentation française, peut être acheté au Journal Officiel

L'article 16 précise que les ministres, les autorités publiques, les agents publics, doivent prendre toutes mesures pour faciliter l'action de la commission. Il n'est pas précisé cependant quelles sanctions administratives seraient prévues en cas d'entrave. Ce choix est volontaire. L'administration ne doit pas rester opaque devant les initiatives de la CNCIS. D'entité administrative à entité administrative, les rapports sont, sinon harmonieux, du moins conformes à la légalité.

Le budget

Un organisme de contrôle a besoin de moyens financiers pour fonctionner efficacement. Des crédits sont donc affectés au budget des services du Premier ministre. C'est le président de la commission qui est ordonnateur. Le Premier ministre n'intervient pas[184].

Un amendement rédactionnel est proposé et accepté[185]. Le texte initial envisageait : « Les recettes et les dépenses ». S'il est opportun de mentionner les dépenses, les recettes sont supprimées. En effet, la CNCIS ne dispose d'aucune ressource en dehors des crédits affectés. Le terme « recettes »[186] n'a aucune raison d'être.

La CNCIS doit prouver qu'elle est un véritable organisme de contrôle.

3) Le travail de la CNCIS, son organisation, sa mission de concepteur

La loi de 1991 gagne en précision grâce au travail de la CNCIS

a) La CNCIS : nouvelle autorité administrative indépendante

L'organisation de la CNCIS

Le principe de représentation de l'opposition est confirmé dans la pratique :

Après les élections sénatoriales de septembre 1992, le président du Sénat désigne Jacques Golliet, universitaire, sénateur de Haute-Savoie.

A la suite des élections législatives de mars 1993, les présidents des deux assemblées appartenaient à la majorité. A l'Occasion, Paul Bouchet rappelle par courrier à Philippe Séguin la notion de parité qui n'avait pas été mise à l'épreuve des faits. La Cour européenne des droits de l'homme avait retenu la représentation de l'opposition comme critère du caractère démocratique des organes de contrôle. Le président de l'Assemblée nationale, se conformant au vœu de 1991, désigne Bernard Derosier (PS), député du Nord, ancien instituteur, membre de la commission des lois. Bernard Derosier s'est fait connaître dans la lutte contre les sectes[187].

Après le renouvellement sénatorial de 1995, Jean-Paul Amoudry, de formation juridique, sénateur de Haute-Savoie (UDF-UC) comme son prédécesseur Jacques Golliet, devient membre de la CNCIS. Il travaille à la commission des lois, s'intéresse aux libertés publiques et aux droits de l'homme. Jean-Paul Amoudry participe activement aux débats concernant la création de la commission consultative du secret défense.

Après la dissolution de 1997, Laurent Fabius retrouve son poste de président de l'Assemblée nationale et il désigne Jean-Michel Boucheron (PS), député breton. Jean-Michel Boucheron est un universitaire, un économiste. Il est aussi un spécialiste des questions de défense, du Conseil de l'Europe, de l'UEO. A la suite du renouvellement

---

[184] Projet d'article 18 : « Les crédits nécessaires à la commission nationale de contrôle des interceptions de sécurité pour l'accomplissement de sa mission sont inclus au budget des services du Premier ministre. Le président est ordonnateur des recettes et des dépenses de la commission », JOAN, 2ème séance du 13 juin 1991, p 3164, 1ère colonne

[185] Un amendement n° 20, présenté par François Massot, est ainsi rédigé : « Dans le deuxième alinéa de l'article 18, supprimer les mots : « des recettes et », JOAN, 2ème séance du 13 juin 1991, p 3164, 1ère colonne.

[186] François Massot : « Le projet de loi prévoit que le président de la commission de contrôle est ordonnateur des recettes et des dépenses ; qu'il soit ordonnateur des dépenses, on le comprend. Mais qu'il soit ordonnateur des recettes, alors qu'il n'a pas d'autres ressources que les crédits budgétaires, cela nous a semblé étonnant », JOAN, 2ème séance du 15 juin 1991, p 3164, 1ère colonne

[187] Il est l'auteur d'une proposition de loi sur les sectes et membre de la commission d'enquête sur les sectes

partiel du Sénat, Pierre Fauchon, sénateur du Loir-et-Cher (UDR-UC), avocat, succède à Jean-Paul Amoudry.

Les derniers membres nommés de la CNCIS ne sont pas tous spécialisés dans les questions juridiques ; ils sont parfois plus jeunes que leurs prédécesseurs. D'ores et déjà, ils entrent dans un organisme qui a appris à bien fonctionner.

Isabelle Chaussade n'avait pas le titre de déléguée. Elle ne pouvait donc remplacer le Président. Elle fut cependant son adjointe directe. Ancien conseiller référendaire à la Cour de cassation, détachée aux Affaires étrangères, elle avait représenté les affaires étrangères à la Commission consultative des droits de l'homme. Ensuite, Mireille Imbert Quaretta, ancien magistrat, président du tribunal de grande instance de Melun est nommée par Paul Bouchet au poste de déléguée général à compter du 14 juillet 1994. En 1994, la CNCIS avait fait ses preuves. Il était possible de créer un poste de délégué général habilité à remplacer le président los de ses déplacements et de ses congés. Jacques-Hugues Gay est chargé de mission du 6 septembre 1996 jusqu'au 31 décembre 1998.

Après le départ de Mireille Imbert Quaretta pour le cabinet du garde des Sceaux, Michèle Salvat devient déléguée générale à partir du 19 septembre 1997.

Les séances, non publiques, peuvent se tenir sur tout lieu du territoire national. L'ordre du jour est établi par le président. Les agents de la commission, sur désignation du président, peuvent assister aux séances. Le délégué général assure le secrétariat et dresse le procès-verbal.

b) La CNCIS, sa mission de concepteur

La CNCIS est garante des libertés individuelles.

L'appréciation des motifs, l'extrême-urgence, le renouvellement des autorisations.

La CNCIS précise son interprétation des motifs, auxquels l'organisme de contrôle se réfère, quand elle examine la conformité de l'autorisation délivrée par le Premier ministre.

La sécurité nationale est mieux comprise au vu des dispositions du code pénal de 1992. La sécurité figure parmi les intérêts fondamentaux de la nation, de même que l'intégrité du territoire, la forme républicaine des institutions, les moyens de défense. C'est un élargissement de la notion précédente de « sûreté de l'Etat ». Le concept ne doit pas induire de banalisation, et doit comprendre les atteintes à la sécurité des personnes et des biens.

La crainte générale d'un trouble à l'ordre public ne sera pas davantage retenue. Une mesure particulière et grave contre la sécurité nationale peut seule justifier le recours aux interceptions de sécurité. La sauvegarde des éléments essentiels du potentiel scientifique et économique de la France[188] n'englobe pas les risques habituels que rencontre une société concurrentielle, ou la volonté de protéger des intérêts exclusivement privés. Les interceptions de sécurité ne sont relatives qu'à « la criminalité et à la délinquance organisées », non aux infractions individuelles, quel qu'en soit le degré de gravité. La prévention ne s'applique pas aux délits ou aux crimes commis par des particuliers isolés.

La commission Schmelck, dans sa tentative de définition de la criminalité et de la délinquance organisées, s'était référée aux infractions qui avaient justifié la création d'offices spécialisés. Cette définition a été reprise dans l'exposé des motifs de la loi de 1991[189].

---

[188] Article 410.1 du code pénal

[189] Les offices étaient les suivants :

L'Office central pour la répression du banditisme

L'Office central pour la répression de la traite des êtres humains

L'Office central pour la répression du trafic illicite des stupéfiants

L'Office central pour la répression du faux monnayage

L'Office central pour la répression du trafic des armes, des munitions, des produits explosifs et des matières nucléaires biologiques et chimiques

Le code pénal caractérise la bande organisée[190]. Il indique aussi pour quels crimes et délits est retenue la circonstance aggravante de bande organisée[191].

.

Le bon déroulement d'une interception de sécurité

Les demandes sont régulières. Il s'agit de contrôler si les signatures qui interviennent dans la procédure d'autorisation sont celles des personnes habilitées en vertu de la loi de 1991 :

- Pour proposition, celle des ministres responsables des services demandeurs[192]ou de leur délégué ;
- Pour autorisation, celle du Premier ministre ou d'un de ses délégués
- Pour exécution, celle du ministre en charge des télécommunications[193]

La commission a encouragé les ministres à user avec prudence des délégations de signature. Cet avis est d'autant plus nécessaire que les délégations ne sont pas publiées[194].

La commission est informée par le secrétaire général du gouvernement des diverses délégations de signature. Des retards sont susceptibles d'intervenir. La commission note les éventuels retards et insiste pour que ce dysfonctionnement cesse. En 1993, la délégation de la signature du ministre des télécommunications a été enregistrée ; elle a donné lieu à régularisation après observation de la CNCIS.

En 1995, dans l'attente des arrêtés de délégation, le Premier ministre et les ministres ont personnellement signé les documents. Aucune observation n'a été émise en 1996 et 1997.

Par ailleurs, la commission considère[195] qu'une délégation de signature peut être communiquée par les ministres en cas d'absence ou d'empêchement du délégataire spécial[196].

Le respect du délai légal a été obtenu grâce à un suivi diligent de la CNCIS. En 1991 et 1992, la commission a constaté que des interceptions de sécurité avaient été maintenues alors que le délai légal des quatre mois était expiré et que la demande de renouvellement prévue par la loi n'avait pas eu lieu[197].

Le 28 mai 1993, le président de la commission informe le Premier ministre de cet état de fait. Dès le 8 juin, le Premier ministre fait savoir qu'il a pris les mesures permettant d'assurer l'application de la loi[198].

---

[190] Article 132.71 du code pénal. La bande organisée est « tout groupement formé ou toute entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions »

[191] Code pénal : trafic de stupéfiants : article 222-35
- Enlèvement et séquestration (article 224.8)
- Proxénétisme (article 225.8)
- Vol (article 311.9)
- Extorsion (article 312.6)
- Escroquerie (article 313.1)
- Recel (article 321.2)
- Attentat aux biens mettant en danger les personnes (article 322.8)
- La fausse monnaie (article 442.2)

[192] Ministère de la Défense pour la DPSD et pour la DPSE, ministère de l'Intérieur pour la DST et les RG, ministère du Budget pour les Douanes

[193] Cf : article 11 de la loi de 1991

[194] Alors que la publication des arrêtés de délégation avait été envisagée lors des débats parlementaires, ces arrêtés ne donnent plus lieu à publication, pour des raisons de confidentialité

[195] Cette position a été arrêtée en 1991 ; elle est réaffirmée en 1997, Rapport d'activité de la CNCIS 1997, La Documentation française, 1998

[196] Cf : article 4 de la loi de 1991

[197] La commission a effectué des visites

[198] Le Premier ministre rappelle aux ministres de l'Intérieur et de la Défense les dispositions des lois ; il s'assure que les interceptions administratives dont l'autorisation était arrivée à expiration ont cessé, Rapport d'activité de la CNCIS 1993, La Documentation française, 1994

Le GIC a reçu des instructions précises. Le président de la commission, lors des visites suivantes au GIC, remarque que lesdites instructions ont été appliquées[199]. Un échéancier est établi chaque semaine par le GIC : son double est communiqué à la commission de contrôle. Grâce à cet échéancier, le GIC interrompt toute interception arrivée à son terme légal. Ce formalisme est une condition de régularité et de légalité. Il n'est pas vite entré dans les mœurs. Pendant l'année 1995, le GIC a procédé à 216 interruptions d'office. En 1996, le GIC a procédé à 217 interruptions d'office[200], au niveau des services, voire des ministres. La situation ne s'est pas vraiment améliorée. Plusieurs centaines d'interceptions irrégulières par le GIC prouvent que les services demandeurs et leurs ministres responsables n'ont pas compris que l'interception n'avait pas de base légale sans autorisation, et que cette autorisation n'était pas indéfinie. Le rappel de la loi par le Premier ministre aux ministres de l'Intérieur et de la Défense n'a pas porté tous ses fruits : ces ministres, s'ils avaient été conscients de la non-applicabilité de la loi, avaient le devoir et le pouvoir non seulement d'adopter des circulaires (visant à expliciter les dispositions légales auprès des services concernés) mais d'appliquer des mesures disciplinaires aux agents s'étant rendus coupables de manquement à la loi précitée et mentionnée. De telles mesures, très dissuasives, n'auraient pas manqué d'avoir des conséquences manifestes quant au suivi effectué par le GIC. Elles paraissent d'autant plus nécessaires que l'ignorance des services tend à s'institutionnaliser.

En 1997, le GIC a procédé à 304 d'interruptions d'office : cette augmentation est significative, puisqu'elle concerne 6, 45% des écoutes administratives, contre 4,69 % en 1996. L'interruption par le GIC pour cause de dépassement est un palliatif qui peut s'avérer dangereux. La commission de contrôle fait remarquer en 1998 que l'interruption peut générer une relative insouciance de la part des services qui feraient supporter le coût de leurs erreurs par le GIC[201]. Le gain de coût réalisé à la marge par les services des ministères de l'Intérieur, de la Défense, serait supporté par un autre service administratif. Surtout, les principaux services consommateurs d'écoutes pourraient s'habituer à cette situation, et perdre de vue que leurs prérogatives exceptionnelles sont soumises à des conditions légales[202]. Ils s'habitueraient à vivre dans l'illicéité, dans la mesure même où ils n'auraient pas à supporter les conséquences de leur comportement dommageable. La commission, en 1998, semble assez pessimiste. Elle est évidemment convaincue qu'une tendance s'est affirmée et qu'il sera bien difficile d'infléchir cette trajectoire[203].

Les enregistrements sont effacés

La commission, en 1992, indiquait que le contrôle de la destruction des enregistrements dans le délai légal de dix jours serait facile à assumer[204].

Tous les enregistrements sont effectués sur un matériel fabriqué par le GIC, sur des cassettes numérotées, avec indications de la date de mise en service et de la date d'effacement : ces dates sont transcrites sur des registres qui sont mis à la disposition de la commission et qui peuvent être consultés à tout moment par l'organisme de contrôle.

---

[199] 83 interruptions d'office sont effectuées par le GIC entre le 4 et le 21 juin 1993 ; 72 effectuées sur demande de l'Intérieur, 5 sur demande de la Défense, 6 sur demande des Douanes, en Ile de France comme en province

[200] Rapport d'activité de la CNCIS 1996, La Documentation française, 1997, p 18

[201] « Cette augmentation, significative en 1997, amène à se demander si le caractère systématique de l'interruption de l'interception au terme de la durée légale n'induit pas une baisse de vigilance de la part des services utilisateurs », Rapport d'activité de la CNCIS 1997, La Documentation française, 1998, p 18

[202] « Un rappel doit être formulé pour que cette tendance ne s'accentue pas et, si possible, s'inverse », Rapport d'activité de la CNCIS 1997, La Documentation française, 1998, p 18

[203] Nous ne possédons pas de données sur les interruptions d'office par services, ce qui faciliterait un travail de recherche non seulement technologique, juridique mais sociologique sur les entités les plus enclines à ne pas suivre les dispositions légales

[204] Rapport d'activité de la CNCIS 1993, La Documentation française, 1994, p 17

Le point de vue de la commission s'est affiné et affirmé. Les contrôles ont permis de détecter un décalage entre les indications qui apparaissent sur les notes du « bureau lignes » du GIC[205]et la réalisation des opérations de branchement qui permettent l'interception.

En 1995, la commission relève que les indications font désormais apparaître les jours et heures des branchements et coupures de lignes. Chaque responsable territorial du GIC, chaque correspondant local, est tenu de faire remonter ces informations au GIC dans les quarante-huit heures.

Ainsi, les dates de branchements, et non plus seulement d'autorisations, sont connues avec exactitude. Les modalités de calcul de durée des interceptions sont claires ; aucune contestation n'est possible à ce sujet. La durée est calculée à partir de la date de branchement sans lequel le processus d'interception serait impossible[206].

La commission a relevé que les pratiques étaient très diversifiées, ce qui rendait toute analyse problématique, toute conclusion défectueuse. Elle a souhaité une unification du modèle des registres conçus et utilisés par les services dans la relève des dates et heures d'enregistrements et d'effacement.

A la demande de la commission, le GIC a établi un modèle unique de registre, où sont listées les opérations d'exécution des écoutes. La commission a recommandé qu'un inventaire des matériels d'enregistrement, de lecture, d'effacement, soit conservé aux différents niveaux[207] pour faciliter la localisation des matériels. La tenue diligente d'un tel inventaire, adjointe au système de numérotation des cassettes d'enregistrement, n'annihile pas la possibilité d'un détournement de matériels. Le risque est cependant limité, et une utilisation à d'autres fins que celles d'interceptions légales n'est guère envisageable.

Les recommandations ont fait l'objet d'avis au Premier ministre[208]. Le deuxième avis du 8 décembre 1994 porte sur les mesures de renforcement de contrôle. La première des mesures est destinée à améliorer l'exercice et les modalités de contrôle. La deuxième mesure est afférente à l'unification des registres portant relevé des opérations de branchement, enregistrement, transcription, selon un modèle établi après accord entre la CNCIS et le GIC[209]. La troisième mesure est relative à l'établissement d'un inventaire des appareils d'enregistrement mis à disposition de chaque service, selon le modèle élaboré sous la houlette du GIC par le responsable GIC ou le correspondant local, dans les quarante-huit heures du branchement par fax adressé au « bureau lignes ».

Approuvées, les recommandations ont été portées à la connaissance des responsables des services le 22 décembre 1994, en présence du président de l'organisme de contrôle, sous la présidence du préfet, délégué du Premier ministre au titre de la sécurité et conseiller aux affaires intérieures. Elles sont entrées en application.

Le registre de type unique, demandé par la commission, est généralisé : il intéresse les trois quarts des sites fin 1995[210], l'intégralité du territoire fin 1996[211]. Le dispositif de contrôle se trouve soit au siège du GIC, soit sur site.

---

[205] Ces indications étaient un reflet fidèle des dates d'autorisations administratives

1. [206] Les services demandeurs ne peuvent pas se prévaloir de leur retard à effectuer l'enregistrement, IIIème Rapport d'activité de la CNCIS, La Documentation française, 1995, p 23

[207] Au niveau central, au niveau local

[208] Avis de la commission au Premier ministre :

- avis du 27 septembre 1994 sur les contrôles
- Premier avis du 8 décembre 1994 sur les conditions des visites de contrôle

[209] Le GIC adresse directement à chaque service les registres conformes à ce modèle, paraphés par le commandant du GIC

[210] IVème Rapport d'activité de la CNCIS, 1995, La Documentation française, 1996, p 17

[211] Vème rapport d'activité de la CNCIS, 1996, La Documentation française, 1997, p 18

Selon les vérifications, l'effacement des enregistrements est effectué, dans la majorité des cas, bien avant la date butoir des dix jours. Les cassettes sont ensuite réemployées. Le délai des dix jours est souvent atteint quand la communication interceptée nécessite une traduction

L'établissement et la destruction des transcriptions

Dès sa mise en place, la CNCIS a estimé que la destruction des procès-verbaux de transcription posait problème : le système envisagé est insuffisamment protecteur contre les risques de duplication, de report sur fiche, de non-respect de la confidentialité. L'utilisation d'un papier spécial s'autodétruisant en cas de photocopie, après étude micro-économique, est apparue d'un coût trop élevé, sans garantie contre la copie manuelle. La commission insiste sur le fait que la garantie contre une conservation illégale des transcriptions dépend d'une organisation rigoureuse des services destinataires[212]. Un rappel constant de la responsabilité pénale encourue par les agents ne respectant pas les prescriptions légales est un bon facteur de discipline.

En matière de télécopie, le GIC a élaboré, pendant l'année 1993, un appareil qui rend possible la lecture optique des télécopies dont l'interception est autorisée, par visualisation sur écran, ce qui limite la transcription aux seuls éléments en rapport avec l'objet de l'interception. Des exemplaires de cet appareil ont été mis en service en 1993 ; la généralisation du procédé prend effet en 1994[213].

Le contrôle du contenu des procès-verbaux de transcription est effectué chaque semaine par le président de la commission lors de ses visites au GIC. Les registres font apparaître, pour toute opération, le nom de l'agent habilité, suivi de sa signature pour émargement.

La destruction des transcriptions induit des difficultés dont la commission est tout à fait consciente : les transcriptions ne restent pas dans les lieux où elles ont été effectuées. Une dispersion[214]se produit.

Les transcriptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation de l'objectif légal. Ce dernier est insuffisamment garanti par la commission malgré sa volonté de faire appliquer le droit. Il est malaisé de savoir si le contenu d'une transcription, surtout si la transcription est codée, entre dans le champ d'application de l'article sept. Dans la mesure où l'établissement et la destruction des transcriptions s'opèrent sous l'autorité du Premier ministre, la commission attire l'attention des chefs de gouvernement sur ce sujet sensible.

En effet, la destruction[215], contrairement à ce qui se passe pour les enregistrements, n'intervient pas dans un délai impératif : un critère d'opportunité[216]se prête malaisément à un examen ou à une critique.

De plus, même si la transcription originale a fait l'objet d'un procès-verbal de destruction, il est matériellement impossible d'empêcher une reproduction, un report sur fiche qui serait conservé dans les arcanes de l'administration, dont le Premier ministre est le chef, mais un chef qui délègue à de multiples chefs de services la responsabilité du bon fonctionnement[217]. La responsabilisation accrue des personnels dirigeants et intermédiaires évite toute dérive intempestive.

---

[212] Système organisationnel et sécurité Cf : « Le monde du renseignement », 1994

[213] Cf : IIème rapport d'activité de la CNCIS, La Documentation française, 1994, p 23

[214] Les procédures ont été mises au point à la demande de la CNCIS. Les transmission sont assez souvent codées. IVème Rapport d'activité, 1995, La Documentation française, 1996, p 18

[215] Dispersion au lieu de transcription. Dispersion au lieu de conservation

[216] Article 12 de la loi de 1991. La destruction intervient lorsque la conservation n'est plus indispensable à la réalisation de l'objectif. Rappel dans le IVème rapport d'activité de la CNCIS, 1995, La Documentation française, 1996, p 18

[217] « Les constatations sont d'autant plus préoccupantes que les opérations de destruction des interceptions et d'établissement des procès-verbaux en faisant foi sont effectuées, d'après la loi, « sous l'autorité du Premier

Quant au GIC, il a initialisé un processus de contrôle. Il procède à la vérification, tous les quatre mois, de date à date[218], de la destruction de l'ensemble des transcriptions. Le service communique les procès-verbaux de destruction des documents et réalise un état des transcriptions concernées : la procédure est renouvelée tous les quatre mois, jusqu'à la destruction des preuves.

Le système s'applique à la majorité des interceptions, mais n'est pas généralisé. La création des « régions GIC », dont la mise en place devait être terminée en 1999, est un instrument de contrôle interne et externe.

Les conservations ne sont pas exceptionnelles[219]. Dans le cas du contrôle du délai, le GIC pouvait agir impérativement, ce qui générait quelques abus dans certaines administrations. Dans le cas de la conservation des transcriptions, un climat de confiance est souhaitable entre le service destinataire et le GIC. Il n'en demeure pas moins que personne ne peut déterminer si les parties prenantes se plient aux règles juridiques.

La commission demande un renforcement de l'effort déployé par le GIC et appelle de ses vœux une grande rigueur dans l'application de la loi par les services administratifs concernés. Il est évident que la destruction des transcriptions pose des questions qui sont demeurées en partie insolubles. Cela signifie-t-il que la loi devrait être modifiée ? La commission n'émet aucune observation en la matière : elle doit appliquer les textes, peut-être les faire évoluer, non les modifier.

c) La CNCIS garante d'une relative transparence

En raison du caractère secret, indissociable des interceptions, la transparence ne peut être un objectif officiel ; elle est cependant recherchée avec prudence et circonspection, à l'occasion des visites et lors des avis.

Les visites de contrôle de la CNCIS

La CNCIS a la liberté d'effectuer, sans avis préalable, des contrôles inopinés dans tous les lieux où seraient effectuées des interceptions de sécurité[220]. Ces lieux sont multiples, et un membre de la commission peut être habilité, pour le compte de la CNCIS, à examiner les conditions dans lesquelles sont réalisées les écoutes administratives ; ce membre de la commission serait susceptible de se déplacer fréquemment en province. Le travail correspondrait à une mission et non à une fonction. Cette mission impliquerait des vérifications sur les spécificités des locaux préposés aux écoutes et sur leur conformité aux exigences d'un environnement pleinement sécurisé. Elle dénombrerait et caractériserait les appareils d'écoutes utilisés, ou mis en service le jour du contrôle. Enfin, le membre de la commission procéderait à un contrôle de la tenue des registres, de l'élaboration des transcriptions, des conditions de destruction des enregistrements et des transcriptions.

Fin 1994, un avis a fixé avec davantage de précision les conditions des visites de contrôle[221]. La commission arrête à chacune de ses séances le calendrier des visites qui lui paraissent opportunes au bon accomplissement de ses fonctions. Elle décide si la visite se fera en formation plénière, ce qui implique le déplacement des trois membres de la commission (ce qui est rare) [222]ou si un seul membre est chargé de la mission[223], ce qui est

---

ministre », alors qu'il n'existe pas actuellement de dispositif permettant de centraliser l'ensemble des renseignements nécessaires », IVème Rapport d'activité de la CNCIS, 1995, La Documentation française, 1996, p 19

[218] Le GIC agit en la matière sous l'autorité directe du Premier ministre.

[219] Auprès des services destinataires

[220] Avis du 27 novembre 1994

[221] Avis du 8 décembre 1994

[222] La visite en formation plénière a un caractère solennel mais peu pratique. Cependant, dès 1993, la commission avait effectué de telles visites à Lyon et Marseille

plus fréquent. Dans ce cas, le président remet au membre désigné une lettre de mission indiquant le lieu, la date, l'objet de la vérification.

Le président de la commission peut s'autocommettre ; aucun service administratif ne peut lui refuser l'entrée des lieux où s'effectue une interception de sécurité. Voilà pourquoi il est le seul membre de la commission à accéder aux données nominatives protégées par le secret défense.

Quel que soit le mode de contrôle, les missions donnent lieu à un rapport. Au vu de ce rapport, la commission décide s'il convient d'adresser des recommandations au Premier ministre afin de pallier des irrégularités ou des dysfonctionnements. En 1994, des vérifications ont eu lieu tant en métropole[224] que dans les DOM[225].

Cette politique de contrôle ne pouvait revêtir un aspect systématique : la CNCIS n'en avait pas les moyens. Elle effectuait des sondages non pas représentatifs mais révélateurs, qui ont nourri la réflexion de la commission et ont abouti à des recommandations. Enfin, la commission n'a pas manqué de dénoncer les interceptions illégales[226] et de saisir le procureur de la République si elle en avait connaissance. Elle a élaboré une œuvre utile qui a permis une interprétation des textes légaux.

Les avis de la CNCIS

Les avis sont un instrument de l'équilibre instauré entre le Premier ministre et l'organisme de contrôle.

En 1993, la commission a différé son avis dans une vingtaine de cas et demandé aux services concernés des précisions complémentaires. Pour une autre vingtaine de cas, la CNCIS a décidé que la demande n'était susceptible d'acceptation que sous réserve de vérification du contenu de la production pendant une période probatoire de quinze jours.

La plupart des difficultés ont été résolues par le recours aux procédures : soit le service n'a pas persisté dans sa demande, soit le Premier ministre[227] s'est conformé à l'avis négatif de la commission.

En 1994, le nombre de cas litigieux s'était amoindri : les notices d'accompagnement étaient plus détaillées ; les justifications complémentaires étaient précises. La commission a rendu treize avis négatifs, qui ont été suivis dans huit cas. Le Premier ministre[228] a passé outre dans cinq cas. En 1995, la commission a rendu 43 avis défavorables[229]. Le Premier ministre a passé outre dans trois cas. En 1996, la commission a émis 26 avis défavorables qui ont été suivis pour la plupart des affaires. Dans deux cas, l'interception n'a été autorisée que pour une durée de quinze jours. Le Premier ministre a passé outre dans deux cas[230].

---

[223] Comme cela a été mentionné plus haut. L'avis du 8 décembre 1994 a été adopté à la suite d'une difficulté survenue lors d'un contrôle effectué par un membre d'origine parlementaire. Cf : IIIème Rapport d'activité de la CNCIS, 1994, La Documentation française, 1995, p 24

[224] Lille, Poitiers

[225] Guyane, Martinique, Guadeloupe, Saint-Martin

[226] Conformément à l'article 17 de la loi du 10 juillet 1991

[227] Autrement dit, le préfet délégué à la sécurité

[228] Une étude sémantique des rapports d'activité de la CNCIS permet de constater qu'en 1993 et 1994, le « passer outre » est imputé au délégué, le « suivi » est mis à l'actif du Premier ministre. En 1995, la dénomination « Premier ministre » est utilisée pour le « suivi » comme pour le « passer outre ». En 1996, la formulation évite (souvent par l'usage du passif) la mise en cause du Premier ministre ou du délégué. En 1997, le vocabulaire est précis, les données sont significatives mais ne sont pas exploitables scientifiquement. Il est probable que, dans ses premières années d'existence, la CNCIS a fait preuve de beaucoup de diplomatie à l'égard du chef de gouvernement

[229] Ils concernent des demandes nouvelles, et des renouvellements.

[230] La CNCIS n'est pas avare de détails : « Il s'agit de deux cas présentés pour motif de sécurité nationale (l'un par la DST, l'autre par les PIG), d'un cas présenté par les PIG au motif de délinquance organisée, et d'un cas

En 1997, dans 33 cas, l'avis défavorable de la CNCIS a conduit à un retrait de la demande, ou à ce que l'écoute soit refusée par le Premier ministre. En 1998, 37 cas ont abouti à des avis défavorables ou à des retraits après demandes de renseignements supplémentaires.

Ces chiffres permettent de parvenir à deux conclusions :

- La CNCIS, conformément à l'esprit qui a présidé à sa création, cherche à éviter les conflits. Elle n'en fait pas moins preuve de fermeté. Les avis défavorables ne sont pas nombreux[231] mais ils ne présentent pas un caractère de rareté.
- Le Premier ministre passe rarement outre à un avis défavorable de la commission, mais il use néanmoins de ses prérogatives.

Le bilan est cependant positif : le travail d'analyse de la CNCIS est examiné avec attention, pris en considération. Le Premier ministre passe outre quand l'impératif d'ordre public lui paraît plus important qu'une éventuelle distorsion en matière de conformité aux motifs[232]. L'organisme de contrôle a démontré qu'il était pris au sérieux par les acteurs principaux, et, notamment, par le Premier ministre qui tient par ailleurs souvent compte des recommandations et des observations.

La CNCIS est crédible. Les rapports reproduisent des sources étrangères et européennes, des arrêts de jurisprudence, des questions de parlementaires. Ils ne rendent pas seulement compte des activités de l'organisme de contrôle ; ils constituent un instrument de travail pour le juriste. Ils renvoient parfois à des recherches académiques, à des articles de presse.

La distinction entre conception autoritaire et conception de conseil établie par M.Pradel[233]à propos du choix du législateur au moment de la création de la CNCIS est judicieuse. Cependant, la conception du conseil peut générer une dérive : le conseil est parfois trop dépendant à l'égard du Prince pour bien remplir sa fonction. Beaucoup d'observateurs avaient prêté des desseins machiavéliques au législateur. Il existe une autre conception du conseil, qui allie la prudence et la fermeté, le sens du devoir et le goût de la diplomatie, la discrétion et la visibilité. La commission a opté pour cette dernière forme de conseil, qu'elle souhaite renforcer et approfondir. Une personne, physique ou morale, se jauge sur ses actes. Les actes de la commission ont contribué à affiner la loi.

La CNCIS a démontré qu'un pouvoir de recommandation avait la faculté d'être efficace[234], en s'intéressant aux libertés individuelles.

4) Les contrôles effectués à la demande des particuliers

Les libertés individuelles continuent à interpeller la loi de 1991, notamment dans le domaine sensible de la vérification des plaintes par les particuliers.

---

présenté par la DST au motif de protection des éléments essentiels du potentiel économique de la France », Vème Rapport d'activité de la CNCIS, 1996, La Documentation française, 1997, p 14

[231] Moins d'un dixième en moyenne, sur la période 1993-1997

[232] Quand le Premier ministre passe outre à l'avis défavorable, il veut rester fidèle à la lettre et à l'esprit de la loi. Des discussions ont lieu entre la CNCIS et le Premier ministre (son délégué) sur la légalité du motif. Quand un compromis n'est pas trouvé, le Premier ministre semble considérer que « son » point de vue est le meilleur, même s'il ne met pas en cause le sérieux et la pertinence du travail de la commission. Cf Rapports d'activité de la CNCIS, 1993, 1994, 1995, 1996, 1997, 1998, 1999, La Documentation française, 1994, 1995, 1996, 1997, 1998, 1999, 2000

[233] Jean Pradel : « Un exemple de restauration de la légalité criminelle. Le régime des interceptions de correspondances émises par la voie des télécommunications » (commentaire de la loi n° 91-646 du 10 juillet 1991). Recueil Dalloz Sirey, 1992, 6ème cahier, chronique, p 49-59. Distinction entre « conception autoriaire » et « conception de conseil », p 58

[234] Par référence au commentaire de Jean Pradel (référence 1). « Au contraire, la seconde ne lui aurait confié qu'un pouvoir de recommandations, sans grande portée » Recueil Dalloz Sirey, 1992, 6ème cahier, chronique, p 58, 2ème colonne

Lors de la discussion du projet de loi, des parlementaires[235]ont demandé que la commission ne se borne pas à notifier aux requérants que des contrôles ont été effectués, mais qu'elle informe le requérant de l'existence d'une interception à son égard. La commission des lois de l'Assemblée nationale et le gouvernement se sont opposés à cette disposition incompatible avec les contraintes de la Défense nationale et de la sécurité publique. La problématique est large ; elle englobe non seulement les interceptions mais aussi les traitements de données informatisées à caractère nominatif[236]. Au niveau international, aucun consensus n'est réalisé.

a) La CEDH rappelle que l'intérêt supérieur de l'Etat prime sur les intérêts particuliers

L'arrêt Klass

Dans l'arrêt Klass, la CEDH a insisté sur la nécessité d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble. Cet intérêt public justifie que la personne écoutée ne soit pas informée des mesures de surveillance auxquelles elle a été soumise et qu'elle ne soit pas habilitée à saisir les tribunaux quand les mesures sont levées. La Cour s'est interrogée sur la possibilité d'exiger une notification ultérieure. Sa réponse a été négative. Selon la CEDH, les dangers que les mesures de surveillance cherchent à combattre subsistent parfois pendant des années après la fin des interceptions. Une notification ultérieure aux individus touchés par une mesure levée compromettrait dans certains cas le but qui induirait la surveillance. Sur ce point, la CEDH est en plein accord avec la position de la Cour constitutionnelle fédérale[237]. L'article huit sur la protection de la vie privée n'est pas incompatible avec la non-information des personnes intéressées[238]. Au demeurant, en RFA, à cette époque, l'intéressé devait être avisé après la levée des mesures de surveillance dès que la notification pouvait être donnée sans compromettre le but de la restriction[239].

La décision NS et PC c/ Suisse[240]

La requête a été jugée irrecevable parce que les plaignants se fondaient sur l'absence de notification ultérieure. La commission a rappelé la position arrêtée par la Cour à l'occasion de l'arrêt Klass[241].

b) Certains droits nationaux en Europe

L'Allemagne

Elle a réaffirmé ses réserves en matière de notification ultérieure, lors de la révision de la loi du 13 août 1968 par la loi de 1989[242]. L'information peut être exclue totalement si la menace ne disparaît pas après cinq ans[243].

---

[235] Cf : M.Daillet et le groupe communiste

[236] Article 39 de la loi du 6 janvier 1978

[237] « La Cour constitutionnelle fédérale l'a fait remarquer à juste titre, pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignements, leurs champ d'observation et m^me, le cas échéant, l'identité de leurs agents », CEDH, arrêt Klass c/RFA, 6 septembre 1978

[238] De l'avis de la Cour, dès lors que l'ingérence, résultant de la législation contestée, se justifie en principe au regard de l'article huit paragraphe deux, il ne saurait être incompatible avec cette disposition de ne pas informer l'intéressé dès la fin de la surveillance, car c'est précisément cette observation qui assure l'efficacité de l'ingérence. CEDH, arrêt Klass c/RFA, 6 septembre 1978

[239] En vertu de l'arrêt du 15 décembre 1979 de la Cour constitutionnelle fédérale

[240] CEDH, NS et PC c/ Suisse, 14 octobre 1985

[241] « La Cour a déclaré qu'il ne saurait être incompatible avec l'article huit, paragraphe deux de ne pas informer l'intéressé dès la fin de la surveillance, car c'est précisément cette abstention qui mesure l'efficacité de l'ingérence », CEDH, arrêt Klass c/RFA, 6 septembre 1978

[242] Loi du 1er juillet 1989

[243] « Après la suspension des mesures limitatives, les personnes concernées en sont informées, si cela ne menace pas l'objet de la limitation. Si cette condition n'est pas réalisée à ce moment là, l'information des intéressés se fera dès que sera disparue ladite menace. Il n' y aura pas d'information des intéressés, si la menace n'a pas disparu après cinq ans », loi du 13 août 1968, modifiée par la loi du 1er juillet 1989

En avril 1993, dans la revue « Questions parlementaires », Claus Arndt, membre de la commission de contrôle allemande G10, souligne que les libertés individuelles sont bien respectées, compte tenu des exigences de sécurité. Quand une mesure de surveillance est activée, le ministre informe les personnes intéressées, sauf si la finalité de l'action est mise en péril[244]. Dès que l'information est divulguée, la personne intéressée peut porter plainte si le droit lui semble violé. Des demandes de dommages-intérêts devant les tribunaux civils peuvent être sollicitées. En pratique, très peu de personnes ont fait usage de ce droit. En 1993, une seule plainte déposée a été couronnée de succès[245].

Le Royaume-Uni

Les personnes qui désirent se plaindre d'une interception peuvent s'adresser à un tribunal indépendant, composé de cinq membres.

Si le tribunal, à l'issue de l'enquête, conclut que la loi a été respectée, il informe le requérant qu'aucune violation des articles 2 à 6 de l' « Interception of Communication Act » n'a été constatée. Il ne prévient pas le plaignant de l'existence d'une mesure d'écoute à son égard[246].

En 1991, année où la loi française a été adoptée, cinquante-huit plaintes ont été déposées. Le tribunal n'a jamais conclu à la violation des articles 2 à 6 de la loi.

c) Les vérifications sur réclamation des particuliers

Elles n'ont pas connu un grand succès en France ; la CNCIS a tenté d'améliorer modestement la situation.

L'application de la loi par la CNCIS[247]

Toute personne ayant un intérêt direct ou personnel peut demander à la commission de procéder au contrôle d'une interception de sécurité afin de vérifier si elle est effectuée conformément aux dispositions législatives. La possibilité est restée méconnue, ou a été perçue comme illusoire.

En 1992, quinze requérants saisissent la commission d'une demande de vérification. En 1993, quarante-deux requêtes sont présentées. En 1994, 1995, 1996, le nombre de requêtes augmente[248]. En 1997, le contrôle a procédé à cinquante-sept contrôles à la requête des particuliers. Le nombre de particuliers qui recourent à cette possibilité ne dépasse pas plusieurs dizaines. Aucune information n'est divulguée sur l'origine des requérants : la CNCIS respecte son obligation de confidentialité. Le choix du législateur est quasi identique à celui qui fut réalisé en 1978 au moment de l'adoption du texte « Informatique et libertés ». Dans les deux contextes, et en conformité avec les arrêts de la CEDH, l'exécutif et le législatif ont évité de révéler à des personnes soupçonnées la mesure de surveillance qui s'exerçait sur elles. Cette position avait été justifiée par le rapport de François Massot, devant l'Assemblée nationale ; lors du débat parlementaire, les échanges avaient été assez vifs. M.Millet et les membres de son groupe avaient déposé un amendement[249]. A l'Assemblée nationale, le droit

[244] Dans ce cas, le ministre en parlera à la commission, et la décision expresse sera prise par cette dernière

[245] Cet insuccès peut dissuader d'autres personnes de porter plainte

[246] Les décisions du tribunal ne sont susceptibles d'aucun recours

[247] « La question reste posée des moyens d'amélioration présente en matière de notification et de recours, qui reste insatisfaisante pour les requérants de bonne foi », Rapport d'activité de la CNCIS, 1993, p 20. Les rapports d'activité des années suivantes 1994, 1995, 1996 ne mentionnent cependant aucun chiffre

[248] « On comprendra aisément au vu de ces différentes hypothèses que la commission nationale n'a d'autres possibilités que d'adresser la même notification à l'auteur d'une réclamation quelle que soit la situation relevée par les opérations de contrôle, et que toute autre disposition conduirait, directement ou indirectement, la commission à divulguer des informations par nature confidentielle » (Rapport Massot, 1991, p 64)

[249] Amendement n°31 : « Nonobstant toute disposition contraire, toute personne a un droit d'accès direct aux informations nominatives recueillies à son nom par voie d'écoutes téléphoniques par tous les services de l'Etat », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne

d'accès aux informations nominatives recueillies par voie d'écoutes téléphoniques[250]est repoussé au nom des exigences de la Défense nationale et de la sécurité publique[251]. Les tenants de l'amendement se fondent sur le concept de droits de l'homme et sur le risque d'arbitraire[252]. Le président de la commission des lois, Gérard Gouzes, rappelle que les écoutes de sécurité se situent au niveau de la prévention et non de l'information : c'est au stade de l'information que la personne mise en examen dispose d'un droit à être informée de ce dont elle est accusée. Les arguments invoqués sont inspirés des considérations de la CEDH. Les adversaires de la raison d'Etat font valoir la défense des libertés individuelles. Certaines opinions émises par les requérants avant le classement de l'affaire NS et PC c/Suisse auraient pu être reprises par Jean-Marie Daillet. La classe politique, dans sa grande majorité, est convaincue que les interceptions de sécurité ne connaîtront une pleine efficacité que si les personnes soupçonnées ou/et soupçonneuses demeurent dans l'ignorance.
La CNCIS rappelle que la disposition légale tend à protéger l'Etat. Si les personnes soupçonnées à bon droit de constituer un danger pour la sécurité sont écoutées, il ne convient pas de révéler cette information aux intéressés.
La CNCIS fait preuve de diligence ; les vérifications demandées sont réalisées dans un délai d'une semaine. La notification est toujours écrite. La commission est consciente de la frustration des requérants et juge utile d'en faire état dès le deuxième rapport d'activité[253]. Il est probable qu'une réflexion s'est engagée à la CNCIS sur les moyens de concilier le secret de l'Etat et les libertés individuelles de citoyens de bonne foi. La commission indique qu'elle est attentive à toutes les études menées à l'étranger sur ce thème. Il est probable que cette préoccupation ne corresponde pas à une simple curiosité, ou à une volonté d'exhaustivité documentaire.
Les palliatifs de la CNCIS
La requête, moyen de faire respecter la légalité
La CNCIS, devant l'insatisfaction des requérants[254], ne demeure pas passive. Elle décide de procéder à un travail d'information : le demandeur doit comprendre que l'organisme de contrôle ne peut pas l'informer. Elle joint à la notification écrite l'extrait du rapport 1993 concernant les vérifications sur réclamations de particuliers.
Dans la notification, et toujours dans un souci d'explication, la commission fait savoir que si elle constate une infraction aux dispositions de la loi, elle saisit le procureur de la République. Ainsi, les citoyens déçus comprendront que leur démarche n'a pas été vaine. La réclamation déclenche le contrôle de la CNCIS ; si la transparence n'est pas possible, la CNCIS n'en remplit pas moins un rôle protecteur : en cas de défaillance, le procureur de la République est

[250] La formulation s'inspire volontairement des termes de la loi « Informatique et libertés ». Une comparaison est ainsi tacitement établie entre l'interception des télécommunications et la collecte de données informatisées nominatives
[251] Cf François Massot, rapporteur : « Cet amendement est incompatible avec les exigences de la Défense nationale et de sécurité publique », JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne
[252] Les droits de l'homme : « A partir du moment où une personne est mise en cause, comment, pour des raisons dites de Défense nationale, pourrait-on lui refuser le droit de savoir ce qu'il en a été ? Un tel droit fait partie des droits de l'homme » ? Jean-Marie Daillet, JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne. Le risque d'arbitraire : « La disposition est très insuffisante pour protéger contre tout risque d'arbitraire », George Hage, JOAN, 2ème séance du 13 juin 1991, p 3162, 2ème colonne
[253] « Il est nécessaire de souligner que la plupart des requérants demeurent insatisfaits, car une telle notification ne leur permet pas de savoir s'ils font réellement l'objet d'une mesure d'interception, ce qui est évidemment le but de leur demande », IIème Rapport d'activité de la CNCIS, 1993, La Documentation française, 1994, p 18
[254] « Mais comme il a été longuement développé dans le rapport 1993, les requérants demeurent le plus souvent insatisfaits dès lors que cette notification leur indique seulement « qu'il a été procédé aux vérifications nécessaires », sans pouvoir leur en donner le résultat », IIIème Rapport d'activité de la CNCIS, 1994, La Documentation française, 1995, p 25

avisé ; il se livrera à une enquête, ce qui aboutira peut-être à une instruction si un délit a été commis[255]. Le système ne lèse pas les citoyens, même si le secret est de mise.
De plus, et bien que cela ne soit pas indiqué aux requérants, cette possibilité de requête individuelle complète utilement l'arsenal de mesures dont dispose la CNCIS[256]. Loin de l'opinion publique, la CNCIS peut adresser une recommandation demandant l'interruption d'une interception qui ne répondrait pas aux critères de légalité. En cours d'exécution, la commission examine les transcriptions produites : ainsi la CNCIS peut-elle procéder à une comparaison entre le motif initialement invoqué et le motif réel[257]. Si un décalage est constaté, la commission intervient. Elle peut aussi déterminer si la cible de l'opération est celle qui avait été désignée par les services demandeurs. Avec les contrôles sur site, la vérification opérée à la demande des particuliers correspond à une modalité de contrôle sélectif a posteriori. La commission réalise aussi des sondages aléatoires et elle peut constater le bon fonctionnement de la loi, telle qu'elle est comprise et appliquée, notamment aux ministères de l'Intérieur et de la Défense.
Malgré les explicitations, l'insatisfaction des particuliers demeure. Les requérants connaissent mieux la loi et manifestent une défiance évidente à l'égard de la fiabilité de la protection du secret des correspondances[258]. La CNCIS insiste sur l'intensité de l'insatisfaction dont elle est témoin : les termes « non-satisfaction », « insatisfaction », reviennent à plusieurs reprises en quelques lignes[259].
Elle explique par la frustration le comportement d'un requérant qui, en 1995, a saisi la CNCIS sur le fondement de la loi de 1978[260]afférente à la liberté d'accès aux documents administratifs d'une demande de communication des documents administratifs intéressant une écoute dont il serait l'objet. La CNCIS notifie au particulier qu'elle a procédé aux vérifications nécessaires, tout en remarquant que les atteintes au secret des correspondances émises par voie de télécommunications sont régies par la loi du 10 juillet 1991 et non par la loi de 1978. Devant cette réponse, le particulier, réactif passe d'une autorité administrative indépendante à une autre autorité administrative indépendante. Il saisit la CADA[261]pour avis. Il est ainsi susceptible d'établir une comparaison entre les réponses données par la CNCIS et la CADA. La CNCIS est appelée à présenter son argumentation devant la CADA. Elle se contente de rappeler ses obligations légales ; ses membres sont tenus au respect des secrets[262] ; l'article 17 de la loi de 1991 ne permet pas d'informer les requérants après contrôle. Après délibération, la CADA avise le requérant de son incompétence. L'avis est court, mais circonstancié[263].

---

[255] Le procureur représente les intérêts de la société et les citoyens. En matière pénale, une instruction est ouverte après dépôt de plainte par une partie civile, ou à la demande du procureur

[256] « Cette possibilité de vérification a posteriori complète utilement les pouvoirs de la commission », IVème Rapport d'activité, 1995, La Documentation française, 1996, p 19

[257] « Elle peut permettre, par exemple, de s'assurer… que le motif initialement invoqué correspond bien à l'objectif réellement poursuivi », IVème Rapport d'activité, 1995, La Documentation française, 1996, p 19

[258] « Traduisant tout à la fois une meilleure connaissance de l'existence de la législation, concernant les écoutes téléphoniques et une méfiance certaine quant à l'effectivité de la protection du secret des correspondances », IVème Rapport d'activité, 1995, La Documentation française, 1996, p 19

[259] Cf : IVème Rapport d'activité de la CNCIS, 1995, La Documentation française, 1996, p 19 et 20

[260] Loi du 17 juillet 1978 relative à la liberté d'accès aux documents administratifs

[261] CADA : Commission d'accès aux documents administratifs

[262] Secrets protégés par les articles 75 et 378 du code pénal pour les faits, actes ou renseignements dont les membres de la CNCIS ont pu connaître dans le cadre de leurs fonctions

[263] « La commission d'accès aux documents administratifs a examiné dans sa séance du 30 mars 1995 la demande dont vous l'avez saisie par lettre à son secrétariat le 14 mars 1995, à la suite du refus opposé à votre demande de communication des documents relatifs aux interceptions téléphoniques pratiquées depuis 1987 sur vos lignes.
« La commission a constaté que les articles 13 et 17 de la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications établissaient un régime particulier d'information de

Malgré les efforts qu'il a déployés, le particulier en quête d'éclaircissements n'a pas obtenu la moindre information. Les deux autorités administratives indépendantes n'ont pu que procéder à la même approche de la loi. La loi du 10 juillet 1991 déroge aux dispositions générales de la loi du 17 juillet 1978. La marge d'appréciation est réduite. En 1995, la CNCIS, continuant à développer un raisonnement qu'elle mène depuis 1992 et 1993, constate l'existence d'un dysfonctionnement. Le suivi textuel de l'article 17 de la loi de 1991 induit un mécontentement grandissant chez les requérants qui veulent recourir à un contrôle a posteriori. Si la CNCIS, dans son rapport d'activité de 1995, narre par le menu l'incident de la double saisine par un particulier de la CNCIS et de la CADA, elle le fait intentionnellement. L'affaire CNCIS/CADA a induit des frais de gestion importants, a entraîné la multiplication des démarches. Elle a donné une mauvaise image des autorités administratives indépendantes, qui, malgré leur compétence et leur sérieux, sont entrées dans la logique de l'absurde. Seule la multiplication des détails peut faire apparaître cet aspect à des lecteurs qui n'ont pas eu connaissance du cas. Si la CNCIS n'occulte pas ce mauvais effet d'image qui aurait pu rester confidentiel, c'est parce qu'elle veut en tirer les conséquences. Après la reproduction de l'avis de la CADA, la CNCIS répète qu'elle est consciente de l'insatisfaction des requérants[264]. Le mot « insatisfaction » est aussi un euphémisme ; si l'exaspération émotionnelle des requérants à l'occasion de leurs démarches est prise en considération, le terme « insatisfaction » est générique et il véhicule la tension de l'opinion publique, perçue à travers l'exemplarité des dizaines de réclamations de particuliers, qui sont convaincus d'être écoutés, et n'acquièrent aucune certitude. La loi de 1991, si elle voulait avant tout donner un cadre légal aux interceptions de télécommunications, aspirait aussi[265]à rassurer l'opinion publique méfiante à l'égard des écoutes de sécurité. Le contexte de 1994-1995 n'est pas favorable aux autorités décisionnaires en matière d'interceptions de sécurité. La révélation de scandales par la presse à gros tirage, l'exploitation commerciale des affaires ont attiré l'attention du grand public sur l'éventuelle illicéité de certaines écoutes téléphoniques[266]. L'opinion de la société civile est réservée. De cela, les autorités administratives indépendantes sont obligées de tenir compte. Elles doivent faire en sorte que la loi qu'elles appliquent et contrôlent ne perde aucune parcelle de légitimité. Une modification des règles s'avère indispensable.

Le changement du libellé de la notification

C'est une interprétation prudente de l'article 17. Jusqu'en 1995, la commission reprenait textuellement les termes de l'article 17[267]. Désormais, il est précisé si les vérifications ont ou n'ont pas fait apparaître une interception qui serait contraire aux dispositions légales. Cette précision a des conséquences juridiques ; au cas où une interception illégale aurait été constatée par la CNCIS, le requérant pourrait porter plainte. L'ouverture d'une instruction ne dépend plus du seul procureur. Le pouvoir d'ester en justice, de déclencher une procédure, est restitué au citoyen qui était privé de cette faculté en raison de la non-information résultant d'une application textuelle de l'article 17. Grâce à cette souplesse d'interprétation[268], le

---

l'auteur d'une réclamation, dérogeant aux dispositions générales de la loi du 17 juillet 1978. La commission n'a pu, pour ce motif, que se déclarer incompétente pour statuer sur votre demande. Elle en a informé le Président de la CNCIS ». Cité dans le IVème Rapport d'activité de la CNCIS, 1995, La Documentation française, 1996, p 20-21

[264] Cette répétition a évidemment une signification, puisque la CNCIS est « consciente » des effets de la sémantique et qu'elle soupèse tous ses mots

[265] Cela s'est exprimé dans les rapports, dans la discussion générale, cf JOAN, séance du 13 juin 1991 ; JO Sénat, séance du 25 juin 1991

[266] Cf : « Le monde », « Le Figaro », « Libération » des années 1994 et 1995 ; médiatisation de l'affaire Schuller-Maréchal

[267] Avec la formule « il a été procédé aux vérifications nécessaires », qui n'entraînait pas l'adhésion des requérants

[268] Dans le cadre légal

citoyen recouvre la maîtrise de ses droits contre lesquels une atteinte aurait eu lieu. L'opinion publique n'a pratiquement pas eu connaissance de cette précision. Elle n'en a pas moins joué un rôle essentiel dans le changement intervenu.
La CNCIS est également saisie de demandes à caractère général. Par exemple, la CNCIS a été interrogée sur la légalité de l'enregistrement électronique des communications téléphoniques pratiqué par des intermédiaires financiers. La situation n'entre pas dans le champ de compétence de la commission : seule, l'autorité judiciaire, en cas de litige, est habilitée à se prononcer sur la validité de cette mesure.
Néanmoins, la CNCIS a signalé ces demandes à la Commission des opérations de bourse[269]. Dans sa réponse, le président de la COB précise qu'il connaît cette pratique[270]. La COB estime que l'enregistrement, s'il est pratiqué conformément aux critères de licéité, c'est-à-dire au su des salariés et de leurs correspondants, contribue à la moralisation des activités financières. L'interception, qui est un manquement au secret des correspondances, réaffirmé à l'occasion de la loi du 10 juillet 1991, peut être considérée avec faveur par le responsable de la COB[271].
Les consultations générales résultent de la notoriété grandissante de la CNCIS. Quant à la vérification des demandes des particuliers, elle demeure un point sensible ; la loi a privilégié l'intérêt supérieur de l'Etat, au détriment d'individus qui s'estiment lésés, ou, comme la CNCIS ne cesse de l'indiquer avec diplomatie, « insatisfaits ».

5) Les opérateurs et la CNCIS : dans son sixième Rapport, la CNCIS redoute « qu'une[272] insuffisante coopération institutionnelle avec les opérateurs de télécommunications et les industriels, conduise à la multiplication d'initiatives en marge de la légalité ». La CNCIS a jugé opportun de retirer en début d'année 1998 à certaines sociétés, l'habilitation dont elles disposaient pour réaliser des interceptions, en raison du non-respect de la loi. Elle a aussi regretté que des poursuites ne soient pas engagées à l'encontre de ceux qui ont violé la législation en vigueur. Aucun service de l'Etat ne vérifie si les opérateurs de communications électroniques ne réalisent pas des interceptions illégales pour leur propre compte. En avril 1998, une réunion de la CNCIS se tient en présence du président de l'époque, Dieudonné Mandelkern et des deux autres membres de la CNCIS, le député socialiste Jean-Michel Boucheron, le sénateur centriste Pierre Fauchon. La sécurité n'est pas toujours strictement observée par les opérateurs.

   En ce qui concerne France Télécom, la mise en application du programme E02 avec des suppressions de sites, de personnel, de services qui, pourtant étaient rentables, et une augmentation importante de la sous-traitance a généré de nombreuses failles dans la sécurité de l'opérateur historique. N'importe qui est susceptible d'intervenir sur les installations. La réalisation des badges dans certaines filiales est sous-traitée. La

[269] COB
[270] « La commission des opérations de bourse, qui a connaissance de cette pratique, n'en est cependant pas à l'origine et n'a pris aucune initiative réglementaire en ce domaine ». Cité dans le Vème Rapport d'activité de la CNCIS, 1996, La Documentation française, 1997, p 30
[271] « Cette pratique, issue de l'usage, de plus en plus répandu, du téléphone dans la passation des ordres de bourse, est destinée à prévenir les contestations susceptibles de naître au sujet de la prise en compte ou de l'exécution de ces ordres. Indirectement, elle permet aussi aux intermédiaires de s'assurer du respect, par leurs salariés, de la déontologie en vigueur au sein de l'entreprise et contribue ainsi à prévenir la circulation ou l'utilisation d'informations privilégiées ». Pour cette raison, la commission estime que l'enregistrement de telles conversations, qui se situe dans un contexte exclusivement professionnel où les atteintes à la vie privée ne sont à priori pas à redouter, est un facteur de moralisation des activités financières, et n'appelle aucune réserve dès l'instant que (ce qui paraît être la règle) les salariés et leurs correspondants sont informés de l'enregistrement auquel il est procédé ». Cité dans Vème Rapport d'activité de la CNCIS, 1996, La Documentation française, 1997, p 30
[272] 1998

technologie des badges ISO, à piste magnétique, est la moins sûre, en raison des dispositifs de copie des pistes magnétiques. Par ailleurs, les responsables de services demandent aux responsables de la sécurité et des systèmes de contrôle d'accès un grand nombre de badges pour les visiteurs, sans les réclamer systématiquement au départ des dits visiteurs. La gestion induit certains dysfonctionnements. Lorsque des rapports sont rédigés pour pallier les dérives, ils ne sont pas fréquemment suivis d'effets. On ne peut s'étonner que des cambriolages aient lieu. Le 3 mars 2000, les clés d'un responsable de France Télécom avaient disparu après le passage de visiteurs. Dans la mesure où aucun vol ne s'était produit, la gendarmerie et autres services d'investigation n'avaient pas été alertés. Le 24 avril 2000, la direction de la téléphonie mobile à Montrouge[273] a été victime d'un cambriolage et un coffre fort de 50 kg a disparu. Ce coffre fort contenait des fiches téléphoniques classées Secret Défense, un listing de demande d'interceptions en cours et 200 fiches d'écoutes précédentes de mi-décembre 1999, qui auraient dû être détruites et ne l'avaient pas été. Ces fiches étaient afférentes à des écoutes de téléphones portables dont les demandes émanaient de la PJ, de la DST, de la DGSE, de la gendarmerie, des douanes, de la DPSD. Ce cambriolage a visiblement monté par des professionnels qui connaissaient les lieux. La sécurité de l'immeuble était assurée par deux sociétés, dont une de télésurveillance. Ce cambriolage, passablement médiatisé, a fait l'objet de questions devant l'Assemblée nationale. La problématique du contrôle est posée : « C'est avec stupéfaction[274] et avec une grande tristesse que nous avons appris par la presse, qu'un coffre contenant 450 fiches d'écoutes classées « Secret défense » avait été dérobé au siège d'une filiale de France Télécom. Je n'ai nul besoin d'insister sur la gravité de cet acte au regard de la défense de l'Etat, à l'intérieur comme à l'extérieur, de la protection des libertés individuelles et de multiples chantages que cette disparition scandaleuse peut susciter. Nous n'en sommes, je le crains, qu'au prologue d'un dramatique roman-feuilleton. Je m'adresse aujourd'hui au ministre de l'industrie, tuteur de France Télécom et j'attends de lui qu'il ne s'abrite pas derrière le secret de l'enquête judiciaire puisque mes questions porteront essentiellement sur la matérialité des faits. Trouvez-vous légitime qu'une activité régalienne de l'Etat soit ainsi confiée à une société privatisée ou à l'une de ses filiales sans que l'Etat exerce sur elles un contrôle très rigoureux ? Trouvez-vous normal qu'aucune règle du « secret défense n'ait été respectée : choix d'un coffre au lieu d'une chambre forte, vidéo défaillante ? Trouvez-vous normal, alors que les premières constatations conditionnent toujours le résultat d'une enquête, que les responsables de la sécurité de cette société aient prévenu la brigade de gendarmerie des Hauts-de-Seine et non le service spécialisé dans la protection du « secret défense » ?...Quelles décisions conservatoires avez-vous prises et quelles sanctions envisagez-vous de prendre ? ». Le secrétaire d'Etat à l'industrie de l'époque[275] répond : « …Le coffre-fort volé contenait 160 cartons correspondant à des interceptions en cours et 200 correspondant à des interceptions anciennes qui auraient dû être détruits. Ces documents indiquent le service demandeur de l'interception et le numéro devant être écouté. S'agissant de la responsabilité, la société France Télécom Mobiles ne semble pas avoir pris les mesures de sécurité indispensables pour la bonne conservation des documents classés « secret défense »…les opérateurs sont en effet tenus par la loi du 10 juillet 1991 de prendre les mesures appropriées pour protéger la confidentialité des procédures relatives aux interceptions de sécurité et des observations sévères vont leur être adressées à cet égard. J'ai par ailleurs demandé au

[273] Hauts de Seine
[274] Robert Pandraud
[275] Christian Pierret

haut fonctionnaire de Défense du ministère de l'économie, des finances et de l'industrie d'examiner les mesures prises pour la protection des documents classifiés et de me remettre un rapport sur les moyens concrets à mettre en œuvre rapidement pour mieux l'assurer ». Le contrôle des opérateurs dans leur mission d'interception semble insuffisant.

De plus, les opérateurs ne sont pas toujours des partenaires fiables. Techniquement, les opérateurs sont en mesure de se livrer à des interceptions illégales. La CNCIS n'est pas compétente pour intervenir. Il n'existe au demeurant aucune commission de contrôle pour vérifier les agissements des opérateurs, pour déterminer si ces sociétés commerciales ne se livrent pas à des interceptions illégales pour leur propre compte. Depuis 1995, il a été imposé que les opérateurs prennent les dispositions nécessaires, pour permettre les écoutes sur les mobiles. Progressivement, il a été possible de constater qu'il y avait davantage d'interceptions sur les portables que sur les fixes. A la fin du vingtième siècle. Les juges antiterroristes se sont plaints du travail des opérateurs de mobiles. Ces derniers sont accusés d'entrave au bon fonctionnement de la justice. Ainsi, le juge Gilbert Thiel a expédié à France Télécom un courrier en recommandé avec accusé de réception le 17 avril 2000 et exprimait son mécontentement : « Les lenteurs de vos services, par les entraves au fonctionnement de la justice qu'elles entraînent, contribue soit à obérer les chances de succès des enquêtes judiciaires qui nous sont confiées, soit encore à différer la date d'arrestation des auteurs de crimes et délits particulièrement graves qui font courir des risques conséquents à la population compte tenu de leur mode opératoire ». Le 19 avril 2000, une bombe explosait, tuant une serveuse à Quévert en Bretagne. Le juge a fait savoir à la famille de la victime qu'il rencontrait des difficultés à France Télécom. Des courriers semblables ont été envoyés par la suite à Bouygues et SFR. L'association SOS-Attentats s'est constituée partie civile. Des policiers ont insisté sur les délais qui leur sont imposés, qui, parfois rendent caduque l'information qu'ils obtenaient, et donc inexploitable. Bouygues Télécom a eu en avril 2000 au moins 6000 demandes judiciaires, ce qui permet de faire une projection quant au chiffre d'affaires que peut faire un opérateur avec le ministère de la justice. D'une façon générale, pour justifier les délais, les opérateurs font remarquer que le nombre important de demandes provoque une saturation de leurs réseaux. Les dépenses sont très difficiles à supporter pour le ministère de la justice, que la chancellerie a émis une circulaire pour inciter les services à limiter leurs demandes. La négociation entre le ministère de la justice et les opérateurs a abouti à une convention qui favorise excessivement les opérateurs. Les demandes ne justifient guère les coûts, surtout lorsqu'une recherche informatique ne nécessite normalement que quelques minutes, excepté pour une localisation. SOS-Attentats est favorable à la gratuité totale de ces demandes pour la justice. Ce souhait est incompatible avec la législation actuelle, et avec le statut des opérateurs, qui recherchent le profit. Cependant, certains, au ministère de la justice pensent que les demandes pourraient être facturées au prix coûtant. A la fin du vingtième siècle, cette préoccupation était une source de réflexion en France et à l'étranger, pour le législateur et pour les organismes de contrôle

DEUXIEME SOUS-PARTIE : LES ORGANISMES DE CONTROLE A LA FIN DU VINGTIEME SIECLE ET AU DEBUT DU VINGT-ET-UNIEME SIECLE

Le courant sécuritaire se développe. Avec l'essor des moyens sophistiqués et globalisés de communication et d'information, les principales personnes morales publiques, et notamment (mais pas seulement) les Etats veulent s'assurer d'une sécurité toujours plus prégnante. Les

attentats qui ont lieu aux USA, c'est-à-dire dans la seule puissance disposant d'un rayonnement géo-politique mondial, sont largement médiatisés et semblent justifier, aux yeux de l'opinion publique, une lutte sans merci contre le terrorisme, mais aussi contre toute forme d'anti-conformisme. Les règles internationales, régionales, nationales, sont modifiées. Dans ce contexte, le souci de combattre les dysfonctionnements à l'occasion des interceptions, ne sont plus une priorité. Les organismes de contrôle, à quelques exceptions, sont moins influents, plus prudents.

A) Les USA :

Rappelons que la CALEA[276] avait été adoptée par le Congrès américain. Le Patriot Act[277]
A été votée par le Congrès et signée par George W.Bush le 26 octobre 2001. Le 6 août 2007, le FISA[278] est modifié.

1) Le Patriot Act et les interceptions de télécommunications :

Aux Etats-Unis, il existait plusieurs paliers de protection de la vie privée relativement à la surveillance électronique avant la promulgation du Patriot Act. Il fallait généralement obtenir une autorisation judiciaire, ou du moins un mandat ou une assignation à témoigner, avant de procéder à une interception, mais la rigueur des critères d'obtention de ces documents variait selon le type d'information à recueillir, le degré de confidentialité que l'on pouvait raisonnablement attribuer à l'information et le motif pour lequel les agents de la paix ou les fonctionnaires du gouvernement demandaient l'autorisation[279].

Le Patriot Act a apporté des modifications au droit américain pour augmenter la capacité qu'ont les agents de police d'obtenir certains types de mandats des tribunaux afin d'intercepter les communications, et pour accroître les catégories d'informations que ces mandats permettent d'obtenir dans certaines circonstances.

L'Article 206 du Patriot Act autorise la délivrance de mandats généraux[280] aux termes de la FISA[281]. Ces mandats sont demandés au tribunal de la FISA et n'exigent pas que soient identifiés de façon précise l'instrument, l'installation ou l'endroit visés par la surveillance. Plutôt que d'exiger que les agents obtiennent un mandat distinct en vertu de la FISA pour chaque téléphone ou appareil qu'ils désirent mettre sur table d'écoute, cette disposition leur permet d'obtenir un mandat général les autorisant à le faire pour plusieurs appareils appartenant à un individu, c'est-à-dire à cibler une personne plutôt qu'un téléphone en particulier. Afin d'obtenir un tel mandat aux termes de l'article 206, il faut convaincre le tribunal que la cible est un pouvoir étranger, au sens de la définition qui apparaît dans l'article 1801, titre 50 du U.S.C[282] et que les actions de la cible peuvent contrecarrer la surveillance.

L'article 218 du Patriot Act permet aux agents fédéraux de demander un mandat en vertu de la FISA lorsque l'obtention du renseignement étranger constitue une raison importante, et non la raison, comme c'était le cas avant l'entrée en vigueur du Patriot Act, de se procurer ce mandat. On pourrait soutenir que les mandats délivrés aux termes de la FISA seraient susceptibles de servir au cours d'enquêtes criminelles, pourvu que ces enquêtes comportent un volet relatif au renseignement étranger. Cela n'est pas convaincant dans la mesure où les conditions à remplir pour obtenir un tel mandat sont généralement moins rigoureuses que les conditions à remplir pour obtenir un mandat aux termes du titre III.

Concrètement, cette loi autorise le FBI à brancher le système Carnivore sur le réseau d'un fournisseur d'accès à Internet pour surveiller la circulation des messages électroniques et

[276] Communications Assistance for Law Enforcement Act
[277] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
[278] Foreign Intelligence Surveillance Act
[279] Généralement pour un renseignement étranger
[280] Roving orders
[281] Foreign Intelligence Surveillance Act
[282] 50 U.S.C. 1805©(2)(D)et 1805(d)

conserver les traces de la navigation sur le web d'une personne suspectée de contact avec une puissance étrangère. Pour cela, seul, l'aval d'une juridiction spéciale est nécessaire.
Les dérives craintes par les défenseurs des libertés individuelles ont eu lieu. Au printemps 2002, l'organisation américaine Electronic Privacy Information Center[283] a fini par obtenir le droit d'accéder à des dossiers afférents à Carnivore. Ses spécialistes ont découvert que les courriers électroniques de citoyens qui ne pouvaient être soupçonnés d'avoir commis des infractions avaient été interceptés et espionnés « par erreur »[284].
Quant aux logiciels de cryptographie, ils sont mis à mal par le programme « Magic Lantern » du FBI. Envoyé par mél, ce virus enregistre à leur insu les touches sur lesquelles frappent les internautes. Ainsi permet-il au FBI d'identifier la clé de chiffrement des utilisateurs de logiciels de cryptographie et de récupérer les messages rédigés par l'utilisateur de l'ordinateur.
2)Le décret-loi de 2002
En certaines occurrences, il n'est plus nécessaire aux USA de demander et d'obtenir une autorisation judiciaire pour faire des interceptions. En 2002, le président Bush a signé un décret-loi secret autorisant la National Security Agency[285], l'organisme chargé de l'interception de renseignements étrangers d'origine électromagnétique aux USA, à surveiller et à intercepter les appels téléphoniques effectués et les courriels internationaux transmis par des personnes aux Etats-Unis à des personnes à l'extérieur des USA ou inversement, sans avoir à solliciter une autorisation judiciaire préalable du tribunal de la FISA[286]. L'existence de ce décret a été révélée par le New York Times dans un article du 16 décembre 2005. Le président Bush a confirmé qu'il avait en effet signé ce décret-loi. Ses conseillers lui ont indiqué que le président avait le pouvoir requis pour prendre ce décret-loi en vertu de la compétence que lui confère l'article II [287]de la Constitution américaine et conformément à une résolution mixte des deux chambres du Congrès, issue du Sénat[288] , portant le titre Authorization for Use of Military Force[289]. La résolution AUMF autorise le président à utiliser toute la force nécessaire et appropriée contre les Etats, organisations ou personnes qui, d'après lui, ont planifié, autorisé, commis ou aidé les attentats du 11 septembre 2001 ou ont hébergé ceux qui ont commis ces actions, afin de prévenir les éventuels et futurs actes terroristes contre les USA par ces Etats, organisations ou personnes.
Néanmoins, certaines personnes et certains groupes se sont demandé si le président disposait bien du pouvoir constitutionnel ou l'autorité conférée par le Congrès nécessaires pour prendre le décret-loi de 2002. Ils se sont notamment demandé si la surveillance électronique exercée sans mandat par la NSA en application du décret-loi pouvait constituer une violation des droits des Américains en vertu du quatrième amendement[290]. Des études ont été menées à ce sujet[291]. Par ailleurs, certains observateurs ont remis en question l'affirmation du gouvernement selon laquelle le décret-loi était indispensable parce que des périodes de surveillance sans mandat plus longues que celles autorisées par la FISA s'imposent pour

[283] EPIC
[284] Les « erreurs seraient de mauvaises manipulations techniques
[285] NSA
[286] E.Lichtblau et J.Risen « Bush Lets US Spy on Callers Without Courts », The New York Times, 18 décembre 2005, p 1.
[287] Cet article spécifie quels sont les pouvoirs exécutifs du Président, y compris ses pouvoirs en tant que commandant en chef des forces armées américaines
[288] SJ.Res 23
[289] AUMF-autorisation du recours à la force militaire, promulguée par le Président Bush le 18 septembre 2001
[290] Protection contre la fouille et la saisie déraisonnables
[291] Voir le mémoire d'Elizabeth Bazan et Jennifer Elsea, « Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information » ; voir aussi M.H.Halperin « A Legal Analysis of the NSA Warrantless Surveillance Program », 5 janvier 2006

prévenir et combattre les activités terroristes. En effet, bien que les organismes gouvernementaux doivent généralement obtenir une autorisation du tribunal de la FISA avant d'effectuer une surveillance sans mandat, la FISA prévoit des exceptions à cette obligation. Par exemple, le procureur général des USA peut ordonner la surveillance électronique de certaines puissances étrangères sans mandat judiciaire pendant une période maximale d'un an[292].Est possible la surveillance électronique sans mandat judiciaire dans des situations d'urgence pour une durée maximale de 72 heures, pendant qu'un mandat autorisant ce type de surveillance est demandé au tribunal de la FISA[293]et la surveillance électronique sans mandat judiciaire pendant 15 jours suivant une déclaration de guerre par le Congrès[294]. Ces questions, ces débats ont incité certains organismes de défense des libertés individuelles à saisir les tribunaux. Le 17 janvier 2006, deux poursuites distinctes ont été déposées contre le programme de surveillance sans mandat de la NSA, la première par un groupement d'organismes de protection des libertés individuelles dirigée par l'ACLU[295]contre la NSA, la deuxième par le Center for Constitutional Rights (CCR) contre le président Bush, la NSA, et le Federal Bureau of Investigation (FBI)[296]. Selon le groupement dirigé par l'ACLU, le programme de la NSA violerait le premier amendement [297]et le quatrième amendement de la Constitution, les principes constitutionnels de séparation des pouvoirs régissant le président et le Congrès. Le groupement demande que le programme soit déclaré inconstitutionnel et qu'une injonction interdise à la NSA de poursuivre le programme[298]. La poursuite intentée par le CCR affirme que des renseignements protégés par la relation avocat/ client ont été interceptés dans le cadre du programme de surveillance sans mandat de la NSA et reprend les allégations formulées dans la poursuite de l'ACLU afférentes aux violations constitutionnelles. Comme l'ACLU, le CCR réclame une déclaration d'inconstitutionnalité et une injonction interdisant la poursuite du programme[299].

La société civile a évolué. Une majorité d'Américains est hostile à l'interception des conversations téléphoniques et des méls des citoyens, selon un sondage publié par USA Today/Gallup en mai 2006. Les sondés désapprouvent à 51%[300]le programme par lequel l'Agence de la sécurité nationale (NSA) a enregistré des communications sur trois des plus grandes compagnies de télécommunications après les attentats du 11 septembre 2001. Les zélateurs du programme donnent la priorité à la sécurité. En effet, ils reconnaissent que le programme viole certaines libertés civiles, mais ils sont convaincus que « enquêter sur le terrorisme est un but plus important ».

L'enquête démontre que les deux tiers des personnes interrogées se disent inquiètes que le gouvernement fédéral puisse actuellement récolter d'autres informations privées, comme des données bancaires ou des statistiques sur l'utilisation d'internet, ou continuer d'écouter des conversations téléphoniques à l'intérieur du pays sans avoir de mandat.

Les deux tiers des sondés sont inquiets que le programme soit susceptible d'identifier des Américains innocents comme des terroristes potentiels. De son côté, la Maison Blanche maintient qu'elle ne commet aucune illégalité.

Le débat concerne également les milieux parlementaires. Quand l'information sur le programme de surveillance sans mandat de la NSA et le décret-loi l'autorisant a été rendue

[292] 50 USC.1802
[293] 50 USC 1805(f)
[294] 50 USC1811
[295] Tribunal fédéral de district de Detroit
[296] Tribunal fédéral de district de Manhattan
[297] Liberté d'expression
[298] Voir ACLU : « ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law », communiqué du 17 janvier 2006
[299] Voir CCR » CCR Files Suit over NSA Domestic Spying Program », communiqué du 17 janvier 2006
[300] Contre 43% d'avis favorables

publique, divers comités du Congrès se sont prononcés en faveur d'une enquête sur le programme et le pouvoir qu'avait ou non le président, selon la Constitution américaine ou la résolution AUMF, d'autoriser la NSA à effectuer de la surveillance sans mandat, alors qu'aucune loi n'avait modifié la FISA. Le 15 janvier 2006, le président du Senate Committee of the Judiciary[301], Arlen Specter, a déclaré que son comité tiendrait des audiences relatives à ces questions. Néanmoins, Arlen Specter a refusé de préciser la portée de l'enquête du comité et d'indiquer le nombre des audiences qui pourraient avoir lieu, la qualité des témoins qui sont susceptibles d'être convoqués.

Depuis les déclarations du sénateur Specter, le SCJ a effectivement mené une enquête. Il est tout particulièrement intéressé par la légalité du programme. Le 6 février 2006, le comité a entendu le procureur général Gonzales : ce dernier a soutenu la position de l'Exécutif. Le président est bien habilité à autoriser le programme de surveillance sans mandat de la NSA ; le président a le pouvoir requis en vertu de ses attributions de commandant en chef, en application de l'article deux de la Constitution américaine et de la résolution AUMF. Le SCJ a ensuite tenu deux audiences additionnelles sur le pouvoir exécutif en temps de guerre et le pouvoir de surveillance de la NSA, les 28 février et 28 mars 2006.

Enfin, la justice s'est prononcée deux fois. En août 2006, la juge fédérale Anna Diggs Taylor, siégeant à Chicago, avait validé une plainte déposée par des avocats, des enseignants, des journalistes, qui se trouvaient en contact fréquent avec le Proche-Orient et qui estimaient que leurs communications étaient l'objet d'une surveillance. Considérant que le président George W. Bush avait outrepassé ses pouvoirs en autorisant le programme, elle avait exigé sa fin immédiate. Un appel a été déposé et la décision de la juge Diggs Taylor a été suspendue en attendant que la Cour d'appel se prononce. En juillet 2007, l'ordre d'arrêter les interceptions « antiterroristes » aux USA sans mandat d'un juge a été annulé par une Cour d'appel fédérale. Cette décision revient à laisser le président libre de poursuivre les interceptions sans mandat d'un juge.

En conséquence, la justice américaine n'a pas exercé de contrôle sur les interceptions sans mandat.

3)La réforme de la FISA

Une loi promulguée le 5 août 2007 réforme la FISA. La Chambre des Représentants a voté une loi facilitant les interceptions de télécommunications (coups de fil téléphoniques et courriels). Le président des USA s'est engagé à la ratifier « dès qu'elle arrivera sur son bureau » bien que les organisations de défense des droits civils considèrent qu'elle ne va pas dans le bon sens. Le gouvernement américain pouvait déjà espionner les communications purement étrangères ne transitant pas par les USA. Désormais, l'Agence de sécurité nationale-NSA- peut intercepter sans mandat les appels téléphoniques et les méls des ressortissants étrangers transmis au moyen des équipements américains.

Georges Bush est persuadé de la nécessité de cette mesure pour lutter contre le terrorisme. Certains opposants font remarquer qu'il y a un danger de dérive, qu'il est désormais possible d'intercepter des Américains communiquant avec des personnes à l'étranger, sans intention délictueuse ou criminelle. Une majorité du parti démocrate a voté contre cette loi adoptée par la Chambre des Représentants par 227 voix contre 183. La loi, l'amendement à la FISA expire au bout de six mois, sauf si le Congrès les renouvelle. Autre garantie : si un Américain devient la cible principale des interceptions, un mandat devient obligatoire pour poursuivre la surveillance. Les organisations de défense des droits civils se sont prononcées contre cette loi. Ainsi le directeur de l'ACLU, American Civil Liberties Union a condamné le vote et fait la déclaration suivante « Nous sommes profondément déçus que les tactiques d'intimidation du président contraignent une fois le Congrès à la soumission » en 2007 aux USA. Il est clair

[301] SCJ, comité sénatorial des affaires judiciaires

qu'au-delà du président, la majorité de la classe politique est favorable au courant sécuritaire. Les démocrates souhaitaient que la loi mentionne clairement la nécessité de saisir la justice pour autoriser les interceptions lorsqu'un ressortissant américain est impliqué. La présidence de son côté jugeait qu'une saisie est suffisante après les faits. Le Sénat comme la Chambre des Représentants se sont inclinés, bien que le rapport de forces soit favorable aux Démocrates. Si la loi n'est pas renouvelée au bout de six mois, la NSA aura plusieurs choix : demander l'arrêt de la surveillance, solliciter une autorisation auprès du tribunal de la FISA afin de poursuivre la surveillance. La loi amendant la FISA sera peut-être renouvelée début 2008. Tout dépendra de l'évolution idéologique au sein de la classe politique.
La FISA Court, le tribunal de la FISA ne joue plus de rôle actuellement. Le contrôle par un organisme indépendant du gouvernement a vécu. Les organismes de défense des droits civils ne sont pas en mesure de se faire entendre.
Cependant, les USA étant la première puissance mondiale, la première puissance militaire, intervenant dans plusieurs pays étrangers, la reconduction de la loi d'août 2007, la mission dévolue au tribunal interne de la FISA dépendra du contexte géo-politique qui prévaudra dans les années à venir.

4) La loi de 2008 : compte-tenu des discussions qui étaient apparues avec le programme permettant les interceptions sans mandat, une loi a été déposée devant la Chambre des représentants et devant le Sénat. Le président George W.Bush a salué l'adoption par le Sénat de la nouvelle mouture d'une loi autorisant le Renseignement américain à pratiquer sans autorisation préalable des interceptions de télécommunications à l'étranger, dans les affaires d'espionnage ou de terrorisme. Le texte permet d'obtenir un mandat d'un an pour des interceptions de groupes et d'individus étrangers. Un Américain peut, quant à lui, être intercepté si la communication concerne l'étranger. Les autorités disposent à présent d'une semaine, et non de 72h pour obtenir un mandat. Elles doivent obtenir l'aval du tribunal spécial instauré par la loi pour intercepter les conversations d'un Américain à l'étranger, alors qu'avant l'approbation du ministre de la justice suffisait.

Il s'agit de remettre à jour le Titre 50, Chapitre 36 de l'US Code, en effectuant les modifications suivantes :
Interdiction pour les états individuels de mener des enquêtes ou sanctions en utilisant des télécommunications
Permettre au gouvernement de supprimer les enregistrements relatifs aux recherches, et de détruire les enregistrements existants
Protéger les entreprises de télécommunications qui ont coopéré ou qui seront amenées à coopérer avec l'Etat fédéral.
Retirer les descriptions relatives à la nature de l'information recherchée
Augmenter le temps autorisé des surveillances non mandatées
Demander à la cour FISA pour intercepter ou enregistrer des conversations électroniques d'Américains à l'étranger.
Donner trente jours à la cour FISA pour analyser les contrats de surveillance arrivés à terme avant de les renouveler

« Le Sénat a adopté un bon projet de loi autorisant le Renseignement à écouter en temps opportun les conversations des terroristes étrangers afin de défendre la liberté des USA » peut-on lire dans une déclaration diffusée par le service de presse de la Maison Blanche.
Cette version du projet de loi, soutenue par l'administration Bush a été adoptée à une grande majorité par 68 voix pour et 29 contre par le Sénat. La loi a été adoptée définitivement par la Chambre des Représentants le 20 juin 2008 et par le Sénat le 10 juillet 2008 par 69 voix (dont celle de M.Obama) contre 28.

La loi accorde l'immunité juridique aux opérateurs de télécommunications américains accusés par la justice américaine de collaborer avec le gouvernement et les services secrets afin de pratiquer des interceptions illégales.
En 2008, malgré l'arrêt de la Cour d'appel fédérale mentionné ci-dessus, une quarantaine de requêtes en recouvrement de plusieurs milliards de dollars ont été engagées dans le cadre d'écoutes téléphoniques aux USA.
Le projet initial ne mentionnait pas l'immunité juridique. Cette dernière semble essentielle à l'Exécutif et aux compagnies de télécommunications.
Devant la Chambre des Représentants, le débat a commencé. Le président Bush a fait savoir qu'il n'attendrait pas la fin des débats pour autoriser la surveillance des communications[302] des présumés terroristes. Pour justifier cette attitude, le président invoque les menaces contre la sécurité nationale « Des terroristes planifient de nouveaux attentats contre notre pays…. qui rendront le 11 septembre pâle en comparaison ». De plus ce texte « vital permettra à nos professionnels de la sécurité nationale de surveiller de manière rapide et efficace les projets des terroristes se trouvant en dehors des Etats-Unis, tout en respectant les libertés des Américains ». Le parlementaire Lamar Smith, représentant le 21ème district du Texas surenchérit : « Dans les trente années qui ont suivi l'adoption de la loi Foreign Intelligence Surveillance Act par le Congrès, les technologies de télécommunications ont radicalement changé…Par conséquent, les organismes de renseignement sont freinés dans leur processus de collecte d'informations vitales sur les terroristes nécessaires à la prévention des attaques dirigées contre l'Amérique. Le Congrès doit moderniser la loi FISA pour résoudre ce problème »
En conséquence, les opérateurs de télécommunications ne doivent pas avoir à payer des dommages-intérêts aux personnes qui accusent ces sociétés de violer leur vie privée : « Pour pouvoir découvrir… les plans de l'ennemi, nous avons besoin de la coopération des entreprises de télécommunications… Si ces compagnies font l'objet de poursuites qui pourraient leur coûter des milliards de dollars, elles ne participeront pas. Elles ne nous aideront pas. Elles n'aideront pas à protéger l'Amérique. » Une fois la loi adoptée, l'hypothétique contrôle par la justice est hors de portée pour tous les citoyens.
Le Centre américain du PEN International s'est joint à l'ACLU, American Civil Liberties Union, à Human Rights Watch pour contester la constitutionnalité de la nouvelle loi. Selon ces organismes, la loi modifiant la FISA donne à l'administration américaine le pouvoir de poursuivre et d'étendre les activités d'interceptions auxquelles elle se livre depuis 2001. D'après les groupes de défense des droits, le gouvernement des USA peut mener une surveillance « extrêmement étendue et virtuellement non réglementée » des communications internationales de ses résidents et de ses citoyens, sans identifier d'individus en particulier ni obtenir de mandat précis aux termes de la FISA. L'ACLU veut en outre savoir ce qui survient aux renseignements que le gouvernement conserve, quand les dits renseignements sont jugés non pertinents dans une affaire. Plusieurs amendements de la Constitution seraient violés.
Le quatrième amendement déclare notamment que « le droit qu'ont les citoyens de jouir de la sûreté de leur personne, de leur domicile, de leurs papiers et effets, à l'abri des recherches et saisies déraisonnables, ne pourra être violé ; aucun mandat ne sera émis, si ce n'est d'après des présomptions sérieuses, corroborées par le serment ou l'affirmation ; et ces mandats devront contenir la désignation spéciale du lieu où les perquisitions devront être faites et des personnes ou objets à saisir ». L'article 218 amende le FISA Act afin que le FBI puisse secrètement conduire des recherches physiques ou sur écoutes afin de prouver l'existence d'un crime et ce même sans urgence. Cette disposition s'applique même aux citoyens américains. L'article 215 autorise les agents du FBI à obtenir un ordre d'une cours FISA ou

[302] Conversations téléphoniques et échanges de méls

de tout autre juge fédéral leur permettant d'obtenir des informations en rapport avec la lutte contre le terrorisme. Des informations très sensibles peuvent ainsi être collectées, telles que le dossier médical, les documents financiers, les vidéos louées, les empreintes, des échantillons ADN, des contrats de travail, des données relatives à l'immigration.

La parlementaire Zoe Logfren, représentant le 16ème district de Californie craint la violation du quatrième amendement. Ce dernier interroge la loi FISA 2008 sur plusieurs points :

-Le problème de cibles, souvent non identifiées : les organismes procédant aux interceptions ne sont en effet pas tenues d'avoir procédé à l'identification de leur cible. En ce sens, le gouvernement peut intercepter des conversations sans lien avec une activité terroriste

-La situation géographique : le gouvernement peut intercepter la communication d'un étranger. Il est possible d'effectuer la surveillance en dehors du territoire dans la mesure où les informations récoltées s'inscrivent dans la lutte contre le terrorisme

-Les surveillances effectuées par le gouvernement ne connaissent guère de limites. Ces limites sont afférentes à l'utilisation, la rétention, la divulgation des informations récoltées

-Des communications « domestiques » risquent d'être interceptées.

Hormis le quatrième amendement, le premier amendement[303] et le cinquième amendement[304]sont mis en cause par la loi de 2008

Pour sa part, le PEN, qui estime que ses communications avec des écrivains et des défenseurs des droits de l'homme situés outre-mer sont vulnérables devant la surveillance prévue dans le cadre de cette loi qualifie celle-ci de violation inutile des protections présentées par la constitution contre les fouilles et saisies abusives : « Le fait de savoir que ces échanges peuvent être surveillés par le gouvernement des USA mine la confiance nécessaire pour rassembler des renseignements vitaux et servir en leur nom de défenseurs crédibles et efficaces » affirme le PEN. Il en va de même pour les journalistes : « Cette loi menace leur aptitude à rassembler des renseignements de nature vitale » précise le rédacteur en chef du magazine « The Nation ».

Selon le PEN, la loi sape en outre les droits de tous les citoyens des USA d'avoir des conversations privées au téléphone et sur Internet sans craindre que le Gouvernement ne soit en train d'écouter : « le peuple américain pourrait ne jamais apprendre l'étendue du programme et comment il est utilisé »

B) Le Royaume-Uni

En Octobre 2000, entre en vigueur la Regulation of Investigatory Powers Act[305], qui se substitue à l'Interceptions of Communications Act 1985. La RIPA englobe les diverses technologies de télécommunications, dans le présent et dans le futur.

Il s'agit de réaliser un équilibre entre les pouvoirs d'enquête des organisations habilitées, opérateurs et fournisseurs, et le souci de protection des droits de l'homme, en particulier la vie privée. Les mandats pour intercepter une communication sont délivrés par le secrétaire d'Etat à l'Intérieur, ou, en cas d'urgence, par un cadre supérieur du gouvernement et soumis à la surveillance d'un « Interception of Communications Commissioner ».

1) Les interceptions :

Les articles 12 à 14 de la RIPA sont afférentes à la capacité technique d'interception des communications. Ils ont été violemment critiqués et débattus par les FSI qui considéraient que les coûts d'implantation risquaient d'être sous-évalués[306]. L'analyse fouillée des consultations diligentées par le gouvernement a démontré que les exigences techniques imposées par la loi ne devaient pas être excessives, pour ne pas compromettre le commerce.

---

[303] Liberté de parole, de réunion et de presse

[304] « Nul individu ne peut être privé de sa vie, de sa liberté, de ses biens sans un procès équitable »

[305] RIPA

[306] Gabrielle Garton Grimwood et Christopher Barclay, « The Regulation of Investigatory Powers Bill », House of Commons Library, Research Paper 0025, 3 mars 2000, pp 32 et 33

Par ailleurs, l'autre préoccupation concerne la vie privée. Le Data Protection Commissioner, le commissaire à la protection de la vie privée a souligné que les nouvelles dispositions, que les obligations ne devaient pas contraindre les opérateurs à empiéter sur la vie privée de leurs usagers.[307] La RIPA est néanmoins une loi sécuritaire, qui montre la voie à beaucoup d'autres lois sécuritaires dans différents pays occidentaux. L'équilibre penche délibérément en faveur de la sécurité et peut faire naître des craintes sur les libertés individuelles et la vie privée. Les fournisseurs de services de communications publics peuvent être forcés de maintenir une capacité d'interception assez conséquente[308], imposée par le Secrétaire à l'Intérieur. Une injonction peut être adressée à un fournisseur de services de communications qui ne respecte pas les obligations[309]. Ces dernières visent les services postaux et les services de télécommunications[310]. Le secrétaire de l'Intérieur peut couvrir, si cela s'avère indispensable, les frais des fournisseurs de services de communication publics[311]. Un régime de cryptage est mis en place pour qu'une organisation d'application de la loi, munie d'une autorisation judiciaire, puisse obliger toute personne à lui fournir l'accès en clair aux renseignements ou à lui procurer la clé du traitement utilisé[312].
Afin de protéger les droits fondamentaux, certaines dispositions sont adoptées : une ordonnance du secrétaire de l'Intérieur qui impose une capacité d'interception doit être présentée au Parlement et approuvée par les deux chambres[313]. Un fournisseur de services de communication est en droit de contester l'obligation relative à la capacité d'interception devant un tribunal spécialisé[314]. A cette occasion, le Technical Advisory Board se penche sur les normes techniques proposées et les répercussions financières quant aux activités du fournisseur.

2) Les abonnés

Le Royaume-Uni permet aux fournisseurs de services de communications de collecter et de conserver systématiquement les données de transmission[315]. Ces dernières englobent une importante gamme d'informations et peuvent être conservées pendant un temps déterminé :

- Les renseignements sur l'abonné[316] peuvent être conservés pendant douze mois.
- Les renseignements téléphoniques[317]peuvent être conservés pendant douze mois

[307] Trade and Industry Select Committee, « Building confidence in Electronic Commerce : The Government's proposals », HC 187 de 1998-1999, mai 1999
[308] Article 12 de la RIPA
[309] Paragraphe 12(7) de la RIPA
[310] Paragraphe 12(1) de la RIPA
[311] Article 14 de la RIPA
[312] Paragraphes 49(2) et 50(2)
[313] Paragraphe 12(10)
[314] Paragraphe 12(5) et (6)
[315] Anti-Terrorism Crime and Security Act 2001, ch.24, partie 11 ; Code of Practice for Voluntary Retention of Communication Data.
Voir Edgar A.Whitley et Ian Hosein « Policy discourse and data retention : The technology politics of surveillance in the United Kindom », Telecommunications Policy, vol 29, 2005.
Par ailleurs, le Conseil de l'Union européenne a approuvé, le 21 février 2006, une directive sur la rétention des données relatives au trafic, malgré l'opposition de l'Irlande et de la Slovaquie. Les opérateurs et fournisseurs doivent conserver les données pour une période de six mois à deux ans. A partir de l'entrée en vigueur de la directive, les Etats-membres disposeront de 18 mois pour se conformer aux nouvelles règles.
[316] Le nom, la date de naissance, le numéro de téléphone, l'adresse de facturation, l'adresse mél, l'adresse IP, la méthode de paiement, les identifiants de la carte de crédit
[317] Numéros de téléphone fixe ou mobile, l'identificateur unique, la date de la communication, l'heure et la durée de l'appel, l'emplacement de l'interlocuteur

- Les renseignements sur les courriels envoyés et reçus [318]peuvent être conservés pendant six mois.
- Les renseignements sur les activités Internet[319]peuvent être conservés pendant quatre jours[320]

La problématique du stockage des données de transmission a une dimension internationale. La Convention sur la cybercriminalité du Conseil de l'Europe permet de conserver les données de transmission. Le débat a ensuite été relayé par l'Union européenne[321]. Les organisations de défense des libertés individuelles dans les différents Etats se sont élevées contre la conservation des données de transmission.

Au Royaume-Uni, le législateur a cherché à combiner les exigences sécuritaires et les garanties exigées précédemment par la CEDH.

Les articles 21 à 25 de la RIPA créent un système qui permet aux organisations d'application de la loi d'accéder aux données de transmission. La demande est faite par une personne désignée et ne nécessite pas l'autorisation par un juge[322]. Elle est prévue essentiellement à des finalités d'enquête criminelle, de sécurité nationale ou de protection du public[323]. Elle doit pouvoir être retracée[324]. Le secrétaire de l'Intérieur prévoit une compensation financière couvrant les frais occasionnés aux fournisseurs de services de communication publics[325].

Des protections existent : tout d'abord, le principe de proportionnalité s'applique au données de transmission ; la proportionnalité existe entre l'information souhaitée et le but de la demande prévu par la RIPA[326]. Par ailleurs, des garanties ont été introduites dans la RIPA : un commissaire (Interception of Communications Commissioner) surveille l'exercice des pouvoirs conférés aux personnes désignées[327]. De plus, un tribunal[328] est chargé de recevoir les plaintes du public.

Un premier bilan laisse planer des craintes quant à une bonne application de la RIPA. Les renseignements recollés dans le cadre des données de transmission[329]sont très nombreux. Les plaintes déposées par le public sont, par contre, fort rares. Enfin, la révision de la RIPA[330] permet aux services secrets de contrôler tout le trafic du réseau.

3) Le « Anti-Terrorism, Crime and Security Act »

Cette loi britannique adoptée mi-décembre 2001, a porté la durée de conservation des données de connexion des internautes par les fournisseurs d'accès à un an au moins. Le ministère de l'Intérieur a également fait savoir qu'il entendait « avoir un droit de regard sur les transactions financières en ligne, ou contrôler les méls privés ». En vertu de la nouvelle loi, le contrôle tend à disparaître : la police est dispensée en de nombreuses occurrences de l'autorisation préalable d'un juge pour agir. Il suffit d'obtenir l'accord du ministre de l'Intérieur ou de l'un de ses hauts fonctionnaires pour le faire. Ces mesures ont

[318] Les adresses IP, les adresses courriel, la date, l'heure

[319] La date et l'heure, les adresses IP, les adresses URL visitées. Dans ce dernier cas, l'adresse URL conservée comprend uniquement le nom de domaine. Si des caractères suivent le nom de domaine, ce sont des données afférentes au contenu. Elles ne sont pas susceptibles d'être conservées systématiquement.

[320] Home Office, Retention of Communications Data under Part 11 : Antiterrorism, Crime and Security Act 2001, Voluntary Code of Practice, annexe un

[321] Voir directive de 2006

[322] Paragraphes 22(4) et 25(2)

[323] Paragraphe 22(2)

[324] Paragraphe 23(1)

[325] Article 24 de la RIPA

[326] Paragraphe 22(5)

[327] Article 57 de la RIPA

[328] Articles 65 et suivants de la RIPA

[329] Paragraphe 21(4) de la RIPA

[330] Projet de révision proposé en juin 2002

été très critiquées par les organisations de défense des libertés individuelles et par la majorité des fournisseurs d'accès, qui ont fait savoir qu'ils envisageaient la délocalisation de leurs serveurs informatiques hors de Grande-Bretagne.
Elizabeth France, commissaire à l'Information en Grande-Bretagne a déclaré début août 2002 que ces deux textes (RIPA révisée et « Anti-Terrorism, Crime and Security Act ») « entrent en conflit » et que certaines mesures sont anticonstitutionnelles. Les services font savoir que « la loi antiterroriste précise que les données de connexion peuvent être retenues pendant une période plus longue que ne le réclament les besoins des opérateurs, mais seulement si ces données sont nécessaires à des enquêtes impliquant la sécurité nationale ». Le Ripa, lui, autorise un grand nombre d'instances, sans mandat judiciaire, à accéder à ces données, alors même que la plupart de ces instances n'ont pas pour objectif de protéger la « sécurité nationale ». Cela contredit donc les normes régissant la vie privée et les droits de l'homme. Le contrôle est réduit.
Au début du vingt-et-unième siècle, le GTAC[331], Centre d'Assistance Technique Gouvernementale, s'est installé dans les locaux du quartier général du M15 à Londres. Ce centre contrôle le trafic électronique entrant et sortant en Grande-Bretagne.
Au Royaume-Uni, la surveillance s'est renforcée au cours des dernières années. Selon Lord West, la Grande-Bretagne serait « à l'avant-garde de tous les pays du monde sur le front de la protection ». La durée maximale de garde à vue est passée de quatre jours à vingt jours et peut même, dans certaines circonstances, aller jusqu'à huit semaines.
La vidéosurveillance est généralisée. La base de données britannique ADN est la plus grande du monde. Les demandes officielles[332] d'écoutes téléphoniques, d'interception du courrier électronique avoisinent les 30000 par mois. Une loi entrée en vigueur en octobre 2007 stipule que les contacts téléphoniques et les SMS pourront être mis à la disposition d'un grand nombre de services de sécurité. Cette loi se justifie, selon le gouvernement, en raison de la lutte contre les crimes et le terrorisme. Les organisations de défense des droits de l'homme et des libertés civiques de Grande-Bretagne, ont émis des protestations contre « cette nouvelle restriction aux libertés ». Selon Liberty, « Dès lors les Britanniques craindront plus que jamais pour leur vie privée ». Selon un sondage effectué par Liberty, seuls 17% des Britanniques ont estimé que le gouvernement préserverait les renseignements qui les concernent. Pour justifier l'édification de cette société de surveillance, le directeur général du M15[333] déclare que, dans ce pays, il y a trente groupes actifs et deux cent autres représentant 2000 personnes actuellement ou potentiellement impliquées dans le terrorisme. Lord West estime qu'il faudra trente ans pour parvenir à éradiquer le terrorisme. Le volume d'enregistrements téléphoniques et de méls[334] n'a pas seulement pour cibles les 2000 personnes impliquées dans le terrorisme, mais d'autres personnes que l'Etat juge nécessaire de surveiller. Les organismes de contrôle voient leur rôle s'amenuiser progressivement, au nom de la lutte contre le terrorisme.
C) L'Allemagne :
Depuis l'arrêt Klass c/RFA, qui avait permis à la RFA de se sortir avec honneur de l'examen de ses textes (G10 de 1968), la situation a beaucoup évolué. La réunification de la RFA et de la RDA ne s'est pas accompagnée d'une libéralisation de la norme en matière d'interceptions de télécommunications.

[331] Government Technical Assistance Center
[332] Emanant d'environ huit cent organismes y ayant droit
[333] Service, secret, équivalent de la Direction de la Surveillance du territoire français.
[334] Environ 400 000 pendant le dernier trimestre 2006 et l'année 2007

1) La loi sur les télécommunications de juillet 1996 a exigé des fournisseurs d'accès à Internet de rendre possible la consultation des données du trafic Internet[335] par les services secrets.
2) En 2001, la loi G10 a été amendée. Cet amendement imposait des limitations à la politique de protection des communications. Il a été demandé aux opérateurs et aux fournisseurs d'accès de mettre tout en œuvre pour permettre aux services de renseignement de surveiller ou d'intercepter les communications électroniques, nationales et internationales : le champ d'application de la G10 s'est considérablement élargi, au détriment des garanties consenties en matière de droits fondamentaux.
   La médiatisation des attentats du 11 septembre 2001 aux USA a permis au gouvernement, à l'initiative du ministre de l'Intérieur, Otto Schily, de faire voter, fin 2001, une nouvelle loi sur les télécommunications. Cette dernière est entrée en vigueur en janvier 2002. Cette Ordonnance sur l'interception des télécommunications permet notamment aux services de renseignements et à la police d'accéder aux données de télécommunications stockées sur support numérique : informations sur les services utilisés par les clients, accès aux renseignements relatifs aux échanges de méls, accès à toutes les données permettant de localiser les personnes à l'origine des communications ou des courriers électroniques, accès aux données des entreprises de télécommunications. Une vingtaine d'organisations de défense des droits civiques et de la liberté d'expression se sont élevées contre l' « Otto-Katalog », dénomination ironique appliquée à la loi en référence à des mesures jugées liberticides, se sont regroupées dans un collectif pour dénoncer ce contrôle des communications. Ce collectif a permis une réflexion dans la société civile sur les enjeux de la surveillance dans le secteur des communications électroniques. Ces associations, ce collectif considèrent que cette loi, présentée et justifiée comme antiterroriste, est incapable d'établir un véritable rempart contre les activités terroristes et dénoncent les concepts invoqués pour adopter de telles mesures.
   Le 12 mars 2004, le Bundestag examine en troisième lecture un nouveau projet de loi sur les communications électroniques. A l'initiative des groupes « Grünen » et sociaux-démocrates, le texte a été amendé dans un sens qui prend en compte la confidentialité des communications. Il renonce à la conservation généralisée des données de communications-Internet et téléphone. Otto Schily avait fait savoir, en décembre 2003, qu'il voulait contraindre les fournisseurs de service Internet à conserver les données du trafic Internet pendant un an. Il n'a pas été suivi sur ce point par les parlementaires et a du renoncer à ces dispositions. Selon Privacy International, Otto Schily a contribué, sous prétexte de lutte contre le terrorisme, à la restriction des « droits des citoyens en Allemagne et principalement la protection de leurs données personnelles ».
   L'Université de Dresde a mis en place le projet ANON, un système-dit anonymiser-qui permet de protéger la confidentialité des communications sur Internet. ANON a pour objectif de contrecarrer les effets délétères de la loi de 2001. Ce système rend possible la consultation des sites Web de façon anonyme, sans laisser de traces chez les fournisseurs d'accès. Le gouvernement a demandé à ANON, en août 2003, de lui permettre dans certains cas de rompre l'anonymat. Une décision de justice a débouté les autorités allemandes.
3) Le contrôle par les cours constitutionnelles :

[335] Méls, historique de consultation

En février 2007, la Cour fédérale de justice avait refusé à la police le droit de fouiller en secret à distance, via Internet, les disques durs de personnes soupçonnées de terrorisme.

La loi de Nordhein-Westphalen autorisait la police judiciaire[336] à s'introduire secrètement dans des ordinateurs personnels, au moyen de chevaux de Troie, afin d'y effectuer des perquisitions. Les juges de la Cour constitutionnelle de Karlsruhe ont annulé la loi en vigueur sur les perquisitions en ligne. La Cour de Karlsruhe permet les perquisitions en ligne, mais seulement dans certains cas bien circonscrits. La police aura le droit de surveiller à distance la navigation sur Internet des personnes soupçonnées de crime, mais des procédures devront être suivies : premièrement, les perquisitions en ligne devront être autorisées par un juge. Deuxièmement, ces perquisitions en ligne ne sont permises par la Cour Constitutionnelle de Karlsruhe que pour deux motifs : menaces concrètes contre la vie humaine, menaces concrètes contre l'Etat. Troisièmement, les données recueillies lors de ces cyberperquisitions ne pourront pas être utilisées par la justice si elles touchent à la vie privée des suspects. La Cour de Karlsruhe a établi un arrêt essentiel qui touche à la société de l'information et au développement très rapide des technologies de l'information. Selon l'éditorial du Hamburger Abendblatt[337] : « C'est d'une façon impressionnante que les juges ont rempli cette exigence d'équilibre entre liberté et sécurité… Ils ont abordé avec beaucoup de minutie et d'obstination ce sujet compliqué et ont principalement constaté deux choses : aujourd'hui, l'épanouissement de la personnalité de chacun s'effectue avec et via l'ordinateur et doit donc être, là aussi, protégée. Simultanément cependant, on ne peut pas non plus accepter que ces grands espaces de liberté soient utilisés par des criminels mettant en danger notre existence ». En bref, selon Gilles Guglielmi[338], la Cour de Karlsruhe définit un droit fondamental à la protection de la confidentialité et de l'intégrité des systèmes informatiques. Elle s'inscrit en faux contre les positions ultra-sécuritaires du ministre de l'Intérieur de l'époque[339], qui s'était heurté à la ministre de la Justice[340].[341]

Le contrôle en matière d'interceptions est plus limité en Allemagne au début du vingt-et-unième siècle.

D) La Belgique :

1) les interceptions de télécommunications sont régies par les articles 90ter et suivants du Code d'instruction criminelle[342]. Cette loi concerne non seulement les interceptions téléphoniques (fixes et mobiles), mais aussi l'interception de télécopies, de méls.

Elles sont autorisées par le juge d'instruction : c'est sur la base d'un mandat clair délivré par un juge d'instruction que le ou les opérateurs téléphoniques ou internet interceptent les communications visées et envoient celles-ci électroniquement via un système central sécurisé vers les enquêteurs nommément désignés dans le mandat, pour exploitation. L'alinéa deux de l'article 90ter énumère les infractions pour lesquels l'interception est possible, sur la base du principe de proportionnalité. Le

---

[336] BKA

[337] Maike Röttger, 28 février 2008, traduction de Francis Segond

[338] Professeur de droit public à l'Université Panthéon-Assas

[339] Wolfgang Schäuble

[340] Brigitte Zypries

[341] Maike Röttger : « Ce jugement devait pouvoir rassurer beaucoup de ceux qui craignent l'Etat policier et donner en même temps assez de possibilités pour faciliter le travail des enquêteurs. Un arrêt qui montre la voie », die Hamburger Abendblatt, 28 février 2008

[342] Loi du 30 juin 1994 qui insiste sur le principe de respect de la vie privée, qui interdit, sauf cas strictement prévus, la prise de connaissance et l'enregistrement de communications et télécommunications privées, qui prévoit des sanctions pénales en cas d'abus

principe de subsidiarité est aussi pris en compte par l'article 90ter qui s'applique aux personnes et aux lieux ciblés en fonction de leurs liens avec les infractions. La durée est limitée dans le temps : un mois maximum renouvelable avec une durée maximale de six mois.(une durée très inférieure, par exemple, aux quatre mois renouvelables prévue en France). Le système mis en place ne peut en aucun cas avoir un caractère permanent. Par ailleurs, une forme de contrôle existe : un rapport, stipule l'article 90 decies du Code d'instruction criminelle, est transmis chaque année au Parlement au sujet de l'application des dispositions afférentes à l'interception des communications et télécommunications privées.

Les interceptions sur Internet inquiètent les députés. En témoigne la question posée par Mme Zoé Genot[343] lors de la réunion de la Commission de la Justice de la Chambre du 4 mai 2004[344] à la vice-première ministre et ministre de la Justice, Mme Laurette Onkelinx. Mme Genot met en cause des tests concernant l'enregistrement de données sur les lignes ADSL de Belgacom[345]. Ces tests semblaient avoir pour finalité d'expérimenter un logiciel permettant de prendre connaissance des données internet d'une personne physique, afin de lutter plus efficacement contre le terrorisme et la grande criminalité. Selon les informations recueillies par Mme Genot, le système mis en place serait un duplicateur optique qui rendrait possible la déviation d'une copie exacte des données internet de milliers d'utilisateurs vers un ordinateur relié à une centrale. Les logiciels[346] installés sur cet ordinateur devraient permettre de déceler les informations en provenance d'un internaute ciblé. D'après les renseignements utilisés par Mme Genot, contrairement aux écoutes téléphoniques fixes, où c'est une ligne bien identifiée d'un abonné qui est mise sous contrôle, c'est l'ensemble du trafic internet qui serait dévié. Ce n'est que par la suite, par un système d'activation, que l'on va cibler les données venant d'un ordinateur. Mme Genot pose des questions précises : « Quand ces tests ont-ils débuté et combien de temps vont-ils durer ? Il semblerait qu'ils soient achevés, mais quelle est la suite des opérations ? Avez-vous déjà des résultats et quand disposerons-nous d'une analyse détaillée de ceux-ci ? L'installation définitive du système est-elle déjà décidée ? Si oui, pour quand est-elle prévue ? D'autres opérateurs que Belgacom auront-ils l'obligation d'installer ce système ? Qui contrôlera la fiabilité du logiciel? ».Et plus loin : « Pouvez-vous préciser en quoi consiste exactement le mécanisme d'activation qui permet de cibler les données provenant d'un ordinateur spécifique ? Vu la facilité avec laquelle elle peut être mise en œuvre, quelles sont les garanties qui existent, afin d'éviter les risques de dérive, comme l'activation de ce système sans ordonnance du juge d'instruction ? »Et, encore plus loin « Concernant le surfing sur internet, comment les données recueillies pourraient-elles être utilisées contre un suspect à l'encontre duquel le juge d'instruction a autorisé la mesure d'écoute ? En effet, un ordinateur peut être utilisé par un nombre important de personnes et il serait impossible de déterminer si les pages internet ont été effectivement visitées ».

Ces questions sont pointues et participent d'un véritable contrôle parlementaire. En effet, l'article 90 ter du Code d'instruction criminelle n'envisage pas les moyens susceptibles d'identifier les dérives qui peuvent survenir. De plus, les auteurs d'infraction risquent de recourir à des outils de cryptage fiables ou à des outils de déviation qui ne permettent plus d'identifier l'ordinateur d'origine. La réponse de la vice-première ministre n'est pas entièrement convaincante.

[343] Groupe ECOLO
[344] CRIV 51-COM 243
[345] L'opérateur historique belge
[346] Fournis par la société Nicé

En conséquence, il est souhaitable que les parlementaires belges continuent à poser des questions et continuent à collaborer avec les ministères et notamment le ministère de la justice. En effet, dans l'exemple ci-dessus mentionné, selon la ministre, les tests réalisés par la police fédérale l'ont été à partir des lignes internes de la police fédérale avec l'autorisation de leurs utilisateurs. La police fédérale a opté pour des essais en circuit fermé. Un accord ministériel[347]devrait encore intervenir avant la phase opérationnelle : la mise à niveau du matériel utilisé par la police fédérale requiert des investissements de plusieurs million d'euros.

2) Les interceptions de sécurité et le rôle du Comité R

La loi organique du 18 juillet 1991 relative au contrôle des services de police et de renseignement a créé un comité permanent de contrôle des services de renseignement et de sécurité, le comité R. Ses membres ne sont pas des parlementaires, mais ils sont nommés par le Sénat. Les contrôles du comité R portent notamment sur le respect des droits fondamentaux par les services de renseignement, sur leur coordination et leur efficacité. Le Comité R n'est pas donc spécifique au contrôle des interceptions, mais le contrôle des interceptions de sécurité se fait sous la houlette du comité R.

La loi organique du 30 novembre 1998 sur les services de renseignement et de sécurité a donné à ces services une base légale, car ils ne faisaient auparavant l'objet que de textes réglementaires. Les services sont au nombre de deux.

La Sûreté de l'Etat, service de renseignement civil, s'occupe de la sécurité intérieure et extérieure de l'Etat. Elle est placée sous l'autorité du ministère de la justice, mais le ministre de l'intérieur peut y avoir recours pour le maintien de l'ordre public et la protection des personnes.

Le Service général du renseignement et de la sécurité est le service de renseignement des forces armées. Il dépend du ministère de la défense nationale.

La loi de 1991 a été modifiée en 1999 : une commission permanente chargée du suivi du comité R a alors été créée au Sénat. Elle s'est substituée à la commission spéciale qui avait été mise en place auparavant. Le comité R a approuvé en 2001 un projet de loi modifiant l'article 44 de la loi du 30 novembre 1998 qui élargit l'exception créée pour le Service général du renseignement et de la sécurité des forces armées afin de garantir, toujours dans l'optique militaire, la sécurité des troupes et celle de leurs partenaires lors d'opérations à l'étranger et la protection des citoyens belges vivant à l'étranger. Il s'agit de « répondre à l'évolution technique rapide qui permet à des individus et groupes actifs à l'étranger, des groupes cibles des services de renseignement, de ne pas hésiter à recourir aux moyens de communication modernes, tels que les téléphones portables, la correspondance électronique ou la communication par satellites, souvent associés à l'utilisation de moyens cryptographiques puissants »[348].

Ces dispositions législatives ont été adoptées par le Parlement fin 2002.

Quant aux interceptions de sécurité, qui n'avaient aucun fondement juridique, elles sont prises en compte au début du vingt-et-unième siècle dans le cadre de la lutte contre le terrorisme et contre la criminalité organisée.

« La sûreté de l'Etat réclame à nouveau des compétences en matière d'écoute et d'enregistrement des télécommunications privées. Cela ne peut se faire actuellement, dans la phase de réaction, qu'en présence d'un juge d'instruction. La question de l'utilisation proactive des écoutes téléphoniques a de forts relents politiques et doit faire l'objet d'une nouvelle discussion. La mission de sûreté de l'Etat consiste en effet à recueillir et analyser des informations afin de garantir la sécurité de l'Etat. Il faut un

[347] Qui pourrait alors donner lieu à question parlementaire

[348] Chambre, 3ème session de la cinquantième législature, 1er octobre 2001

débat parlementaire où l'on mettrait en balance les libertés garanties essentielles telles que le droit à la vie privée, d'une part, et d'éventuelles atteintes à l'ordre public, d'autre part. Il s'agit d'un problème qui concerne typiquement le parlement. Le ministre de la Justice ne peut décider seul »[349].

Le comité permanent R demande que les services de renseignement soient en mesure de recourir à un outil légal dans ce domaine[350]. Dans le même temps, en novembre 2001, le Conseil des ministres approuve un projet de loi relatif aux techniques policières spéciales de recherche de recherche dans le secteur de la criminalité organisée et se référant au téléphone fixe, au téléphone portable, écoute par microphone. La loi entre en vigueur en 2002. La modification avait pour objectif de répondre « à l'évolution technique rapide qui permet à des individus et des groupes actifs à l'étranger, des groupes cibles des services de renseignement, de ne pas hésiter à recourir aux moyens de communication modernes, tels que les téléphones portables, la correspondance électronique ou la communication par satellites, souvent associés à l'utilisation de moyens cryptographiques puissants »[351]

Par ailleurs[352], le comité R propose des interceptions de sécurité en prenant en compte l'équilibre entre vie privée et ordre public. « La sûreté de l'Etat réclame à nouveau des compétences en matière d'écoute et d'enregistrement des télécommunications privées. Cela ne peut se faire actuellement, dans la phase de réaction, qu'en présence d'un juge d'instruction. La question de l'utilisation proactive des écoutes téléphoniques a de forts relents politiques et doit faire l'objet d'une nouvelle discussion. La mission de la sûreté de l'Etat consiste en effet à recueillir et analyser des informations afin de garantir la sécurité de l'Etat. Il faut un débat parlementaire où l'on mettrait en balance les libertés garanties essentielles telles que le droit à la vie privée, d'une part, et d'éventuelles atteintes à l'ordre public, d'autre part. Il s'agit d'un problème qui concerne typiquement le parlement. Le ministre de la Justice ne peut décider seul »[353] La loi est adoptée. Plusieurs critères sont retenus : la demande d'interception de sécurité, écrite et motivée est adressée par les responsables des services de renseignement et de sécurité au ministre de tutelle du service et au Premier ministre ; l'autorisation écrite est accordée par l'un des ministres ou secrétaires d'Etat concernés, pour une durée limitée renouvelable ; une procédure d'urgence est instituée[354] ; les interceptions de sécurité sont possibles pour des motifs limitativement énumérés, lutte contre le terrorisme et prévention de la criminalité organisée ; les autorisations sont notifiées au comité R ; ce dernier intervient dès le début de la procédure, pendant la procédure et a posteriori, soit sur sa propre initiative ou sur plainte de personnes physiques ou morales ; un rapport périodique est transmis au parlement et aux ministres concernés ; une procédure d'information de la personne sur la base du modèle allemand est instituée ; les interceptions sont effectuées à l'instigation de l'unité globale d'interception.

a) La composition et le fonctionnement de l'instance de contrôle :

Le comité R, instance composée non de parlementaires, mais d'experts choisis par les Sénat contrôle les services de renseignement. Une commission sénatoriale spécifique supervise le fonctionnement du comité R.

[349] Déclaration du ministère de la Justice, le 2 octobre 2001
[350] Cf : rapport d'activité 2000 du comité permanent R, p 56
[351] Chambre, 3ème session de la cinquantième législature, 1er Octobre 2001
[352] Rapport 2001 publié le 17 avril 2002 du comité permanent de contrôle des services de renseignement
[353] Déclaration du ministère de la Justice, le 2 octobre 2001
[354] Compétence des chefs de service avec régularisation de la procédure

Ce dernier est composé de trois membres qui sont nommés par le Sénat pour une durée de cinq ans. Leur mandat est renouvelable deux fois. Le président est un magistrat et les autres membres des juristes expérimentés et compétents dans les questions de police et de renseignement. Seul, le président exerce son activité à temps complet. En même temps que les trois titulaires, le Sénat désigne trois suppléants.
Les membres du comité doivent détenir une habilitation de sécurité du niveau « très secret », c'est-à-dire susceptibles de connaître des informations très confidentielles.
Leur mandat est incompatible avec un mandat public électif et avec certains emplois ou fonctions « qui pourraient mettre en péril l'indépendance ou la dignité de la fonction ». Les membres du comité ne peuvent faire partie ni d'un service de police ni d'un service de renseignement.
Le comité R est susceptible d'agir de sa propre initiative mais, en ce cas, il est tenu de donner des informations au Sénat. Il peut aussi agir sur la demande de l'une des deux assemblées, ou à l'instigation soit du ministre de la justice, soit du ministre de la défense nationale. Il lui arrive également d'être saisi de plaintes émanant de particuliers ou d'être réquisitionné par les autorités judiciaires.
Le comité R travaille avec un service d'enquêtes, qui comprenait cinq membres en l'an 2000. Nommés par le comité R, les membres de ce service d'enquêtes sont en général détachés d'un service de police ou de renseignement.
En résumé, le comité R est une émanation du Parlement, il est un outil d'expertise à la disposition du législateur, qui peut utiliser ses travaux afin de prendre des initiatives législatives ou exercer sa mission de contrôle de l'exécutif.
Le comité R collabore avec la commission du suivi du comité R. Cette commission est présidée par le président du Sénat ; elle comprend en outre quatre sénateurs désignés après chaque renouvellement du Sénat, au scrutin de liste, et ceci pour la durée de la législature. Elle élabore un règlement intérieur, où sont indiquées les modalités de l'organisation de ses travaux et de rédaction des procès-verbaux.
La commission du suivi du comité R tient des réunions au moins une fois par trimestre avec le président ou avec tous les membres du comité R. Elle peut aussi se réunir à la demande de la majorité de ses membres, du président du comité R ou de la majorité des membres du comité R. De plus, elle est susceptible d'être saisie de toute dénonciation de la part d'un membre du comité afférente à la violation par ce dernier de la loi ou de son règlement intérieur.
Les réunions de la commission du suivi du comité R se tiennent à huit clos et les commissaires sont tenus à une obligation de confidentialité, même quand ils n'exercent plus leurs fonctions.
b) Les compétences des organismes de contrôle
La loi de 1991 charge le comité R d'enquêter « sur les activités et les méthodes des services de renseignement, sur leurs règlements et directives internes ». Cela signifie que le comité R, contrairement à la CNCIS françaises n'a pas de compétences spécifiques en matière d'interceptions de télécommunications, mais que les interceptions de télécommunications entrent dans le champ d'activité du comité R.
Le comité R tient autant de réunions qu'il le juge nécessaire, et pour atteindre ses objectifs, il dispose d'importants pouvoirs. Il peut se faire transmettre tout document qu'il juge utile et entendre toutes les personnes dont l'audition lui semble indispensable. Les personnels des services de renseignement ont l'obligation de lui communiquer tous « les secrets dont ils sont dépositaires », sauf ceux qui portent sur les affaires judiciaires en cours. Les personnels ne sont pas en mesure de se retrancher derrière la nécessité de protéger certaines personnes, puisque, dans ces cas, c'est le président du comité R qui statue. Le service d'enquêtes du comité peut également

procéder à des perquisitions et à des saisies sur les lieux où les personnels des services de renseignement exercent leurs fonctions. Il peut collaborer avec des experts.
De leur côté, les services de renseignement sont tenus de transmettre l'ensemble de leurs documents internes au comité.
Chaque enquête débouche sur un rapport, qui est communiqué au ministre compétent et à la commission sénatoriale de suivi. Le ministre informe le comité des mesures qu'il envisage de prendre en réponse aux conclusions du comité. Ce dernier est habilité à questionner les responsables des services de renseignements sur des problèmes ponctuels. Cette forme de contrôle, assez souple, permet au comité de savoir comment les services de renseignement traitent un point donné.
Conformément à la loi, le comité R fait parvenir un rapport annuel d'activité à la commission sénatoriale de suivi. Quand il est chargé d'une enquête par la Chambre des représentants ou par le sénat ou lorsqu'il a constaté que des conclusions qu'il avait fait connaître au ministre n'ont pas été suivies d'effet ou que les mesures prises ne sont pas adéquates, le comité R établit également un rapport.
Le budget des services de renseignement est inclus dans celui du ministère de la justice ou de l'intérieur et le comité R ne dispose d'aucun pouvoir de contrôle, même financier, a priori. Par contre, pendant le déroulement des enquêtes, il peut vérifier l'emploi des crédits. En 1995, le comité R a procédé à une analyse des budgets des deux services de renseignement ; cette étude s'est limitée à une vérification des fonds spéciaux.
C'est le Sénat qui attribue des compétences à la commission du suivi du comité R vis-à-vis du comité R. Cette commission a, entre autres missions la possibilité de charger le comité R[355]de mener des enquêtes, de demander l'avis du comité R sur les projets de textes législatifs et réglementaires. Elle obtient communication des rapports d'enquête diligentés par le comité R et est en mesure de se faire transmettre les dossiers concernés, y compris sur des affaires en cours. La communication des informations ne peut se faire en cas de mise en péril de tiers et entrave au fonctionnement normal et régulier des services de renseignements nationaux et étrangers. Ainsi l'identité des auteurs de dénonciation ne sera pas transmise.
La commission du suivi du comité R siège avec la commission du suivi du comité P afin d'examiner les rapports annuels des deux comités avant publication. Les conclusions des deux commissions sont jointes aux rapports des comités. Les commissions siègent parfois ensemble pour analyser les résultats d'une enquête demandée par la Chambre des représentants au comité R[356] ou pour discuter des informations recueillies.
En 2007, est déposé un projet de loi afférent aux méthodes de recherche pour les services de renseignement : selon les ministres de la Défense André Flahaut et de la Justice Laurette Onkelinx[357], un Collège doit être chargé du contrôle a posteriori de ces méthodes par la Sûreté de l'Etat. Dans ce collège seraient représentés un magistrat, le comité R, la Commission de la vie privée. Un rapport annuel serait transmis au Sénat, qui assure le suivi des activités du Comité R. Une commission de surveillance serait placée sous l'autorité des ministres de la Justice et de la Défense et composée de trois magistrats. Cette commission aurait pour finalité d'exercer un contrôle sur l'application des méthodes spécifiques et exceptionnelles. La présidente du Sénat a émis des critiques sur ce projet de loi dès la rentrée parlementaire, considérant que le

[355] Ainsi que le comité P
[356] Ou par le Sénat au comité P
[357] Déclarations du 8 septembre 2007

parlement ne disposerait plus que d'un contrôle a posteriori. Cela concerne tout particulièrement les interceptions de télécommunications.

« Les rumeurs se multiplient concernant la volonté de saper l'autonomie du comité R. Voilà qui participe également du désir de brider le parlement dans ses prérogatives de contrôle du fonctionnement du pouvoir exécutif » déclare la présidente du Sénat, Anne-Marie Lizin[358].

En 2008, avec le nouveau gouvernement, le texte de Mme Onkelinx demeure la base de travail. Néanmoins, le comité R insiste sur la nécessité de voir son rôle mieux reconnu. Par ailleurs, de nouvelles garanties sont envisagées pour les avocats. L'enjeu est d'améliorer le contrôle à posteriori.

3) Les données de connexion, depuis l'an 2000, sont conservées pour une durée d'un an. A ce sujet, des protestations émanent des organismes de défense des libertés individuelles et collectives.

E) L'Espagne :

La liberté d'expression est garantie dans l'article 20 de la Constitution qui protège le droit « à communiquer ou recevoir librement une information véridique par tout moyen de communication ». Cependant, les interceptions de télécommunications sont pratiquées assez couramment. Le fondement juridique est l'article 55 qui régule l'interception des télécommunications, qui est soumise à certains principes : les règles sont devenues plus contraignantes depuis le début du vingt-et-unième siècle. L'interception implique l'autorisation judiciaire. Elle doit être effectuée de telle manière qu'elle n'affecte pas les contenus des communications. Dès que les personnes habilitées ont pris connaissance du contenu des interceptions, les supports doivent être détruits dans délai ; ils ne peuvent pas être distribués ou stockés. Des règles identiques s'appliquent dans l'interception des réseaux. L'administration dispose du droit d'inspecter, de détecter, de localiser, d'identifier, d'éliminer des interférences préjudiciables, des irrégularités, des perturbations dans les systèmes de télécommunications et d'initier une sanction.

1) La Loi de l'Internet ou LSSICE :

Le 27 juin 2002, le Congrès des députés espagnols a adopté la LSSICE. Cette loi, élaborée par le ministère des Sciences et Technologies, oblige les fournisseurs d'accès à Internet à conserver les données de connexion et de trafic de leurs clients pendant au moins un an. Cependant, grâce à l'introduction d'un amendement par l'opposition, ces dernières ne seront utilisées par les services de police ou de renseignements qu'avec l'aval d'un magistrat. Néanmoins, les parlementaires n'ont pas modifié profondément le projet de loi.

2) Arrêt de la CEDH : Prado Bugallo C.Espagne du 18 mai 2003[359]

José Ramon Prado Bugallo est un ressortissant espagnol né en 1956, domicilié à Cambados. Il se trouvait à la tête d'un important complexe économique composé de plusieurs sociétés d'import-export de tabac ayant leur siège dans la région de Panama, en Galice et à Anvers. M .Bugallo travaillait avec de nombreux collaborateurs.

Dans le cadre d'une enquête judiciaire pour trafic de stupéfiants, le juge central d'instruction n° 5 ordonne, conformément à l'article 579.3 du code de procédure pénale, la mise sur écoute téléphonique de personnes physiques et morales soupçonnées d'appartenir à un réseau de trafic de cocaïne dirigé par M.Bugallo. A l'issue des investigations policières, M.Bugallo et certains de ses collaborateurs sont arrêtés en janvier 1991.

Par un jugement du 26 juin 1993, la chambre pénale de l'Audiencia Nacional reconnaît M.Bugallo coupable des délits de trafic de stupéfiants, de transfert de monnaie non autorisé. M.Bugallo est condamné à vingt ans et trois mois de prison et à un paiement

[358] Déclaration du 24 septembre 2007

[359] N° 58496/00

d'amendes. Le tribunal fonde notamment sa décision sur les enregistrements des écoutes téléphoniques.
Par un arrêt du 31 octobre 1994, le Tribunal suprême rejette le pourvoi formé par le requérant. La légalité des interceptions de télécommunications avait été mise en cause. Le tribunal exerce donc son contrôle sur ce point. Il estime que les tribunaux ont bien pris en compte la jurisprudence du Tribunal constitutionnel et de la Cour européenne des droits de l'homme. Le requérant forme un recours d'amparo devant le Tribunal constitutionnel qui fut rejeté par un arrêt du 20 décembre 1999 : le tribunal constitutionnel estime en effet que les écoutes téléphoniques avaient respecté les exigences de contrôle juridictionnel, de légalité et de proportionnalité requises.
Le requérant soutenait que sa mise sur écoute téléphonique avait porté atteinte à son droit au respect de sa vie privée[360].
La cour relève que l'article 579 du code de procédure pénale, modifié par la loi du 25 mai 1988, précise les modalités de contrôle de la mise sur écoutes téléphoniques. Elle estime que les garanties introduites par cette loi n'offrent pas toutes les conditions exigées par la jurisprudence de la Cour pour éviter les abus. Il en va ainsi de la nature des infractions pouvant donner lieu aux écoutes, de la fixation d'une limite à la durée d'exécution de la mesure et des conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées. Ces insuffisances concernent également les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins d'un contrôle éventuel par le juge et par la défense.
La Cour constate qu'en dépit des progrès induits par la loi de 1988, d'importantes lacunes persistaient au moment où les interceptions furent réalisées. Il est vrai que ces lacunes ont été palliées en grande partie par la jurisprudence nationale, notamment du Tribunal suprême. Néanmoins, cette évolution jurisprudentielle, à supposer même qu'elle puisse combler les lacunes de la loi, ne peut pas être prise en compte dans l'affaire Lugallo, car elle est postérieure aux ordonnances de mise sur écoutes téléphoniques du requérant. Par conséquent, la Cour conclut à l'unanimité, à la violation de l'article 8 de la Convention européenne et alloue 7000 euros au requérant pour frais et dépens.
En résumé, la Cour considère que les garanties de la législation espagnole en matière d'interceptions de télécommunications, même après la réforme de 1988 consécutive à la condamnation subie par l'Espagne dans une autre affaire[361] ne répondent pas à toutes les conditions exigées par la jurisprudence de la CEDH, en particulier dans les arrêts Kruslin C.France et Huvig c.France, pour éviter les abus : concrètement, la Cour considère qu'il en est ainsi pour la nature des infractions pouvant donner lieu aux interceptions, pour la fixation d'une limite à la durée d'exécution de la mesure, pour les conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées, tâche qui est laissée à la compétence exclusive du greffier du tribunal. En outre, selon la CEDH, les insuffisances s'appliquent également aux indispensables précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, dans le but d'un contrôle éventuel par le juge et par la défense, puisque la loi espagnole ne contient aucune disposition à cet égard. La CEDH enregistre l'évolution jurisprudentielle en Espagne, dans le secteur du contrôle des interceptions de télécommunications, mais considère qu'elle ne peut combler les lacunes de la loi au sens formel.
F) L'Italie:
Les interceptions de communications électroniques sont de plus en plus utilisées. L'Italie détient un record en la matière. En 2005, le garde des sceaux de l'époque, Roberto Castelli, a admis que le nombre des écoutes téléphoniques, essentiellement sur les

[360] Article huit de la Convention européenne de sauvegarde des droits de l'homme.
[361] CEDH, Valenzuela Contreras c.Espagne , 30 juillet 1998

portables doublait tous les deux ans : 32000 en 2001, 45000 en 2002, 77000 en 2003, plus de 100000 en 2004, et 200000 en 2005, comme M.Catelli l'a reconnu devant une commission parlementaire qui s'inquiétait de la multiplication des interceptions de télécommunications.. En Italie, 72 citoyens sur 100000 font l'objet d'une interception légale. Ce chiffre s'expliquerait par la difficulté de parvenir à la manifestation de la vérité par des moyens plus traditionnels « Si le nombre des écoutes est si élevé chez nous, c'est parce que, dans les affaires les plus graves, il est difficile de trouver des témoins et de les convaincre d'aller au tribunal » déclare Bruti Liberati, président de l'Association nationale des magistrats. Cet essor exponentiel des interceptions de communications électroniques a pour corollaire une saturation du réseau, qui concerne les principaux opérateurs qui se chargent des écoutes téléphoniques, Vodafone, Wind et surtout Tim. Ce dernier fait savoir en 2005 que 5000 lignes sont sous surveillance et qu'il n'est pas techniquement possible d'en écouter davantage simultanément. Depuis lors, Tim est passé à 7000. Une vingtaine ou une trentaine de lignes restent disponibles pour la direction nationale anti-Mafia.. Les interceptions sont bien réglementées et ne peuvent dépasser quinze jours dans la plupart des cas, quarante s'il s'agit de criminalité organisée. Mais la procédure est renouvelable et la renouvelabilité est fréquente. Ces interceptions sont coûteuses mais cependant moins onéreuses que les filatures courantes. En 2004, les « frais de bretelle » atteignaient 300 millions d'euros, contre 165 millions en 2001. « J'admets que l'Italie est parmi les pays qui dépensent le plus pour les interceptions téléphoniques, déclare le procureur adjoint de Milan, Armando Spataro. Mais il est tout aussi vrai que nous sommes au premier rang pour les actes criminels, de la Mafia à la corruption en passant par le terrorisme ». En matière de terrorisme, citons la loi N° 374 du 18 octobre 2001 et le décret de la loi n° 374 du 18 octobre 2001[362]. La section 7 de ce décret, se référant à la section 18 de la loi 152/1975, a appliqué les dispositions de la loi anti-Mafia au terrorisme international. Cette mesure a étendu le champ d'application des mesures préalables et préventives qui comprennent des restrictions sur la liberté personnelle[363]. La loi 374/2001 criminalise le financement d'actes terroristes aussi bien internationaux que locaux. Selon la Section un[364], « quiconque promouvant, instituant, organisant, gérant ou finançant des organisations dont le but est de proposer des actes de violence aux fins du terrorisme, ou pour perturber l'ordre démocratique, est passible d'une peine de prison allant de cinq à quinze ans » et « la poursuite du terrorisme sera également de rigueur lorsque les acte de violence sont dirigés contre un Etat étranger ou bien contre une organisation ou une institution internationale ». La loi 374/2001 considère comme un crime le simple fait de participer à toute activité préparatoire, en association avec d'autres personnes dans le but d'accomplir des actes de terrorisme. En particulier, il étend l'application de ce régime aux écoutes téléphoniques légales, à la fouille de bâtiments ou blocs de bâtiments destinés à couvrir des cas de crimes perpétrés en faveur du terrorisme international[365]. En Italie, si le téléphone d'un parlementaire ne peut être intercepté par la justice, les propos qu'il échange avec une personne faisant l'objet d'une interception légale, deviennent des éléments probatoires. Au demeurant, le secret de l'instruction est levé dès la mise en examen d'un prévenu

A l'occasion de différents scandales[366], le contenu de nombreuses écoutes téléphoniques légales a été publié dans la presse, alors que ces interceptions sont couvertes par le secret

[362] Décret de la loi 374/2001

[363] Y compris les interceptions de télécommunications

[364] « Disposition sur la conspiration liée au terrorisme local ou international »

[365] Section trois de la loi 374/2001

[366] Mise en examen de Victor Emmanuel de Savoie, Juventus de Turin (football), gouverneur de la Banque d'Italie

de l'instruction. A plusieurs reprises, les gouvernements successifs ont envisagé de réformer le régime des interceptions de télécommunications. En 2006, le garde des sceaux étudie un décret-loi pour limiter l'usage des écoutes téléphoniques au terrorisme et à la criminalité organisée. De plus, les sanctions prévues à l'encontre des journaux qui rendent publiques ces interceptions seraient durcies. Précédemment, le gouvernement Berlusconi avait failli adopter le même type de réglementation. Le 25 septembre 2006, un décret sur les écoutes téléphoniques adopté par le Conseil des Ministres est une réponse fiable aux scandales déjà mentionnés. Le texte prévoit la destruction immédiate de tous les documents qui contiennent conversations ou communications téléphoniques récupérés de manière illégale et prévoit de graves sanctions pour qui les publie. Le 17 avril 2007, la Chambre des députés a adopté un projet de loi réglementant la publication par la presse des écoutes administratives. Ce texte prévoit notamment l'obligation de détruire tous les enregistrements cinq ans après la décision d'un juge dans une affaire et l'interdiction de publier ou de diffuser un enregistrement relatif à un dossier si l'enquête est terminée. En juillet 2008, le Parlement italien adopte une loi qui limite à quelques cas spécifiques : terrorisme, pédophilie, mafia des interceptions de télécommunication, et notamment téléphoniques qui sont, comme nous l'avons vu, pléthoriques. Leur divulgation est passible des tribunaux pénaux avec des peines sévères pouvant aller jusqu'à trois ans de prison pour les journalistes et directeurs de journaux qui contreviendraient à ces dispositions. Cette loi a provoqué de vifs débats, au niveau des partis entre le premier ministre Silvio Berlusconi et la Ligue du Nord et au niveau des magistrats. Ces derniers regrettent que soient exclus du champ d'application de la loi les délits de corruption et de concussion politique. « Il faut étendre les écoutes à la corruption et à la concussion. Les en exclure ne serait pas compris par nos électeurs » a déclaré l'un des dirigeants de la Ligue du Nord, le secrétaire d'Etat Roberto Castelli, lui-même garde des Sceaux dans le précédent gouvernement de Silvio Berlusconi. Le ministre de la justice Angelino Alfano a indiqué que le gouvernement n'avait nullement pour objectif de restreindre les enquêtes, d'entraver le pouvoir d'investigation, mais simplement, et conformément aux engagements de l'Italie, de « mettre fin à des intrusions intolérables dans la vie privée ». Les magistrats ont cependant élevé des objections : « l'écoute téléphonique est souvent la seule méthode possible d'investigations » fait valoir leur association ANM. Ils se prononcent néanmoins en faveur d'une « sélection » tendant à éliminer le matériel superflu lors de la clôture de l'enquête. En Italie, le secret de l'instruction est levé quand la mise en examen a été formulée. Chaque personne physique peut alors consulter le dossier d'instruction. En outre, le Conseil des ministres adopte un projet de loi qui institue un système de « personnes protégées », au profit du président de la République, du premier ministre, des présidents des deux chambres pendant la durée de leur mandat..

La quasi-absence de contrôle dans le domaine des interceptions de télécommunications est relevée par la CEDH.[367]. Les juges remarquent que la disposition qui réglementait le contrôle de la correspondance à l'époque, ne pouvait constituer une base légale suffisante au regard de la Convention européenne de sauvegarde des droits de l'homme, en raison de la trop grande latitude laissée aux autorités pénitentiaires pour déterminer l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine.

G)La France :

1) Les membres de la CNCIS
   - Les députés et les sénateurs désignés par le président de l'Assemblée nationale et du Sénat
   - Les députés :

[367] CEDH, Musumeci c/Italie, 11 juin 2005

Henri Cuq, député des Yvelines, 4 juillet 2002 : il est diplômé de l'IEP de Toulouse, de l'Institut d'études internationales et de l'Institut de criminologie de droit de Toulouse. En 1986, il est élu député de l'Ariège, puis devient député des Yvelines sous l'étiquette RPR puis UMP à partir de 2002. Il a été amené à s'intéresser aux questions de sécurité comme secrétaire national du RPR chargé de la sécurité de 1986 à 1997. Par la suite, il sera ministre délégué aux relations avec le Parlement de 2004 à 2007, puis redevient député. Il a donc une bonne formation juridique et une sensibilisation forte aux problèmes de sécurité.

Bernard Derosier succède à Henri Cuq ; il a déjà été membre de la CNCIS. Membre du parti socialiste, c'est un ancien instituteur, membre de la Commission des lois.

Daniel Vaillant succède à Bernard Derosier. Ancien ministre des relations avec le Parlement, ancien ministre de l'intérieur, il est élu parisien (18 ème arrondissement) membre de la Commission des lois.

- Les sénateurs :

Pierre Fauchon est avocat de profession. Avant de travailler à la CNCIS, il est d'abord membre de l'Office parlementaire d'évaluation des politiques publiques, puis membre de la Commission d'accès aux documents administratifs. Il s'est également penché sur les questions de sécurité en tant que membre de la Délégation française à l'Assemblée parlementaire de l'Organisation pour la Sécurité et la Coopération en Europe[368] Ce sénateur de Loir-et-Cher était d'appartenance UDF. Il est désigné à la CNCIS en 1998.

André Dulait, sénateur des Deux Sèvres, d'appartenance UMP, lui succède le 6 novembre 2001. C'est un vétérinaire, qui fut membre de la commission des affaires étrangères, de la défense et des forces armées. Il n'a pas de formation juridique.

Jacques Baudot, sénateur de la Meurthe et Moselle, fut désigné le 26 octobre 2004 et décéda le 21 juin 2007. Chirurgien-dentiste de profession, il n'avait pas reçu de formation juridique. Il était d'appartenance UMP.

Hubert Haenel, sénateur du Haut-Rhin, également UMP prend sa suite en 2007. Maître des Requêtes au Conseil d'Etat, c'est un juriste. Membre de la commission des affaires étrangères, de la défense et des forces armées, il s'intéresse de très près aux questions de sécurité et à l'Union européenne : il est Président de la Délégation pour l'Union européenne[369]. Il exerce des fonctions qui font appel à ses compétences dans le domaine juridique : il est membre de la Cour de Justice de la République et membre de la Haute Cour de Justice.

Depuis le 1er octobre 2003, le Président de la CNCIS est Jean-Louis Dewost. Président de section du Conseil d'Etat, Jean-Louis Dewost est également un acteur de la vie de l'Union européenne. Il a été longtemps directeur juridique de la Commission européenne. L'acculturation européenne apparaît dans les cours qu'il donne à l'Institut d'études politiques de Paris, il porte son enseignement sur l'Union européenne.[370]Il a défendu avec force la Constitution européenne.

2) Les dépenses induites par les interceptions :

Le Ministère de la Justice affirme que la France est l'un des pays européens qui pratique le moins d'interceptions judiciaires : quinze fois moins que l'Italie, douze fois moins que les Pays-Bas et trois fois moins qu'en Allemagne. Cependant, en 2005, les dépenses d'interception se sont élevées à 92 millions d'euros, « ce qui représente 20% des frais de justice », selon Mme Cottin, secrétaire générale adjointe du ministère de la justice en 2005. Il y a environ 20000 écoutes téléphoniques judiciaires par an, qui représentent 30% des

[368] OSCE

[369] Au demeurant, il a été membre titulaire de la Convention chargée de l'élaboration de la Charte des droits fondamentaux

[370] Cf : « Introduction aux études européennes et au droit communautaire »

interceptions globales (Le reste est constitué par la communication des données de connexion liées à Internet).L'augmentation des interceptions judiciaires est significative : elles seraient passées de 5845 en 2001 à 27000 en 2007. Les interceptions de portables sont particulièrement faciles et ne coûtent pas grand-chose aux opérateurs[371]. A ces interceptions judiciaires, il convient d'ajouter les 5985 interceptions administratives[372].
Concernant la tarification des prestations, deux[373] décrets et deux arrêtés[374] ont fixé de nouvelles règles. L'Etat garantit à l'opérateur une juste rémunération des interceptions légales de communications électroniques. La juste rémunération de l'opérateur correspond à la couverture des coûts exposés pour les études, l'ingénierie, la conception, le déploiement des systèmes demandés pour les interceptions, des coûts liés à la maintenance, et, dans certains cas, à la location des moyens permettant le fonctionnement des systèmes demandés pour les interceptions, des coûts induits par le traitement des demandes d'interception. La rémunération de l'opérateur est assurée dans le cadre d'une convention signée avec l'Etat. L'arrêté du 22 octobre 2007 (D.98-7) établit une distinction entre les interceptions des communications de téléphonie fixe et les interceptions de téléphonie mobile. Pour les interceptions des communications de téléphonie fixe, quand les interceptions sont effectuées au moyen d'une liaison louée, les coûts afférents au traitement des demandes d'interception comprennent les coûts d'accès au service : 497 euros hors taxes par interception, sauf si le site d'interception est prééquipé, les coûts liés à la liaison louée de renvoi en fonction de la distance à vol d'oiseau entre les deux extrémités de celle-ci calculés par période de trente jours

- pour les liaisons inférieures ou égales à 10 km :
- 1, 1 x (104,60 euros hors taxex+ 1, 64 euro hors taxes par kilomètre)
- Pour les liaisons supérieures à 10 km :
- 1, 1 x (119, 30 euros hors taxes+ 0, 17 euro hors taxes par kilomètre)

Ces tarifs incluent la fourniture du détail de trafic pour toute la période d'interception.
Pour l'interception des communications de téléphonie mobile, les coûts liés au traitement des demandes d'interception s'élèvent à 88 euros hors taxes par interception. Ces tarifs incluent la fourniture du détail de trafic pour toute la période d'interception. L'arrêté du 22 octobre 2007 (R.213-2) établit également une distinction entre téléphonie fixe et téléphonie mobile. Conformément aux dispositions de l'article R.213-2 du code de procédure pénale, les réquisitions adressées dans les conditions prévues au présent code les interceptions de communications de téléphonie donnent lieu à remboursement aux opérateurs de communications électroniques, sur facture et justificatifs, en appliquant à ces demandes, pour chacune des prestations demandées, le montant hors taxes des tarifs . Pour l'interception des communications de téléphonie fixe, quand les interceptions sont effectuées au moyen d'une liaison louée, les coûts relatifs au traitement des demandes d'interception comprennent :

- les coûts d'accès au service : 497 euros hors taxes par interception, sauf si le site d'interception est prééquipé.

[371] 700 euros à l'opérateur
[372] Chiffre de 2007
[373] Décret n° 2007-1519 du 22 octobre 2007 portant modification du code des postes et des communications électroniques et relatif à la tarification des interceptions de communications électroniques ; décret n° 2007-1520 du 22 octobre 2007 portant modification du code de procédure pénale et relatif à la tarification des interceptions judiciaires
[374] Arrêté du 22 octobre 2007 pris en application de l'article D.98-7 du code des postes et des communications électroniques fixant la tarification applicable aux demandes ayant pour objet les interceptions de communications électroniques
Arrêté du 22 octobre 2007 pris en application de l'article R.213-2 du code de procédure pénale fixant la tarification applicable aux réquisitions ayant pour objet les interceptions de communications électroniques

Les coûts liés à la liaison louée de renvoi en fonction de la distance à vol d'oiseau entre les deux extrémités de celle-ci calculés par période de trente jours :

- pour les liaisons inférieures ou égales à 10 km:
- 1,1 x (104,60 euros hors taxes+ 1, 64 euro hors taxes par kilomètre)
- Pour les liaisons supérieures à 10 km :
- 1, 1 x (119, 30 euros hors taxes +0, 17 euro hors taxes par kilomètre)

Ces tarifs incluent la fourniture du détail de trafic pour toute la période d'interception.
Pour l'interception des communications de téléphonie mobile, les coûts liés au traitement des demandes d'interception s'élèvent à 88 euros hors taxes par interception.
Une plate-forme nationale d'interceptions judiciaires a été instituée en 2007 : cela devrait permettre de réaliser 45 millions d'euros d'économie. Forte d'une trentaine de personnes, cette structure est l'équivalent du GIC, Groupement interministériel de contrôle dédié aux interceptions de sécurité. Elle centralise l'ensemble des demandes émanant dans la plupart des cas des juges d'instruction. Cette plate-forme permet notamment l'écoute de la voix, l'identification des numéros appelants, la géolocalisation de téléphones mobiles, des informations détenues par les opérateurs et qui sont ensuite renvoyées sur les services enquêteurs. Elle est accessible aux magistrats et enquêteurs par les réseaux intranet des administrations. Les procédures de travail sont simplifiées et les possibilités opérationnelles sont améliorées, correctement adaptées aux technologies du moment. Le dispositif autorise la modernisation des différentes procédures financières qui en découlent. Il est appelé Délégation aux interceptions judiciaires[375], placé sous l'autorité d'un magistrat. Ses travaux sont coordonnés par le secrétariat général du ministère de la justice. Pour diligenter ses actions, le délégué est assisté d'un fonctionnaire de la police nationale et d'un officier de la gendarmerie nationale. La mission de préfiguration de la délégation aux interceptions judiciaires a collaboré avec les divers acteurs concernés, administrations, opérateurs, fournisseurs d'accès, loueurs de matériel. Un appel d'offres a été lancé en 2007. Dans l'attente de la structure, une petite plate-forme a été réalisée en 2007 pour l'interception spécifique des SMS.
La DIJ met en place le référentiel des interceptions judiciaires. Ce dernier identifie et qualifie les réquisitions judiciaires courantes en matière de communications électroniques. Il distingue les réquisitions selon trois catégories : informations concernant les abonnés, le trafic des communications électroniques et les documents d'abonnement. Il est complété avec les prestations afférentes aux interceptions, puis Internet, porte sur les demandes relatives à la téléphonie fixe et mobile.
Sur un modèle identique, chaque réquisition est déclinée en fiche. Tarification, code, finalité de la prestation, mise en garde, éventuelle observation constituent les données d'une fiche. Sous la forme d'un guide papier diffusé auprès des magistrats, personnels des régies, enquêteurs et autres acteurs intervenants en matière d'interceptions judiciaires, le référentiel fait l'objet d'un site à accès restreint depuis le réseau ADER. Le site garantit une mise à jour régulière induite par le caractère évolutif du référentiel ; il clarifie les demandes des officiers de police judiciaire et facilite la réponse des opérateurs.
Avec cette plate-forme, le Ministère de la justice considère qu'il a opté pour un système efficace, évolutif, sécurisé, compétitif au niveau tarifaire ; de plus, la plate-forme est placée sous le contrôle de la CNIL.
Néanmoins, le département de recherche sur les menaces criminelles contemporaines, plus connu sous son acronyme[376] estime[377] qu'un système moins concentré et centralisé au niveau des juridictions interrégionales spécialisées[378] aurait été préférable.

[375] Du Secrétariat général du ministère de la justice
[376] DRMCC
[377] Cf : Rapport « Ecoutes et interceptions légales des télécommunications », DRMCC, 2006

3) L'évolution des interceptions de communications électroniques en France :

Le réseau d'interceptions français a fait l'objet d'abondants commentaires. Il est baptisé avec ironie « Frenchelon » par les anglo-saxons. Il a été construit au fil du temps par deux entités du ministère de la Défense : d'une part la DGSE, d'autre part la Direction du renseignement militaire (DRM). Une liste détaillée des bases françaises de ce réseau d'interceptions a été publiée par le Monde. Ces bases sont présentées comme rattachées à la DGSE et à sa direction technique[379]. Ces moyens d'interception, satellitaires ou autres, sont déployés à Alluets-Feucherolles (Yvelines), Agde (Hérault), Domme (Dordogne), Mutzig (Bas-Rhin), Solenzara (Corse du Sud) à Saint-Barthélemy (Antilles), à la Réunion, à Djibouti et à Mayotte. Censé servir à collecter des informations pour la Défense nationale, afin de prévenir les conflits, lutter contre le terrorisme et la prolifération des armes nucléaires, ce réseau d'écoute est soupçonné d'espionnage économique. Les notions d'alliance et d'alliés tendent à se diluer. L'espionnage entre pays entretenant de bonnes relations est pratiqué pour conquérir des parts de marché. Soulignons que les interceptions pratiquées ainsi, notamment par la DGSE ne relèvent pas de la CNCIS. Il n'existe aucun moyen de contrôle. L'élargissement du réseau d'interception satellitaire est un objectif pour la DGSE, comme le mentionnait déjà le rapporteur du budget 2001 de la défense[380]. Une station a été construite sur le plateau d'Albion, une autre sur la base aéronavale de Tontouta, en Nouvelle-Calédonie. Ce réseau, en l'absence de contrôle est une menace pour la vie privée. Quand elles passent par l'un des satellites surveillés par les bases de Domme, de Kourou, de Mayotte, les communications avec l'étranger ou les DOM-TOM peuvent être interceptées, recopiées, diffusées par la DGSE, sans qu'aucun organisme de contrôle puisse intervenir. Les autres pays européens qui sont dotés d'un réseau d'interceptions satellitaires, telle l'Allemagne, ont mis en place un système de contrôle. L'information est-elle par ailleurs fiable, efficace ? Un responsable de la DGSE estime à quelques dizaines les interceptions utiles

Sous l'égide de la commission des Finances de l'Assemblée nationale, le député UMP du Tarn, Bernard Carayon a rendu le 22 octobre 2004 son rapport parlementaire sur le volet renseignement du Budget de la Défense nationale. Il révèle que les interceptions de télécommunications ont progressé de 400% en cinq ans.

Dans le domaine de l'interception, la France disposait au début du vingt-et-unième siècle d'une dizaine de stations d'interception au sol, de deux micro-satellites, dénommés Cerise et Clementine, qui furent mis en orbite au vingtième siècle, en 1995 et 1999. En 2004, le programme Essaim est à l'origine du lancement de quatre satellites supplémentaires « d'écoute des communications en constellation reprochée et en bande basse ». Essaim est le compagnon de guerre de l'information d'Hélios 2[381] ; il a pour mission le recueil du renseignement électromagnétique[382] avec pour but de réaliser une cartographie des émetteurs de télécommunication. Les quatre satellites doivent être exploités jusqu'en 2009.

Ces quatre satellites tendent à servir d' « indice d'alerte dans la gestion des crises, tout en favorisant l'évaluation des dommages » ; leur coût total est évalué à 79, 3 millions d'euros. Par ailleurs, un nouveau démonstrateur[383] est à l'étude, avec mise en orbite en 2008 et un coût voisin des cent millions d'euros. Quatre autres microsatellites de renseignement électromagnétique doivent être lancés fin 2009.

---

[378] JIRS

[379] Ex GCR pour Groupement des contrôles radioélectriques

[380] Jean-Michel Boucheron

[381] Cf : infra

[382] ROEM

[383] Nom des « programmes » dans le secteur des interceptions

Le 13 octobre 2005, la France a aussi lancé Syracuse III, système de radiocommunications utilisant un satellite ; Syracuse III a amélioré le débit des transmissions autorisées par ses précédentes versions, mais aussi la sécurité des communications, tant en terme de chiffrement que de résistance au brouillage et multiplie par six le nombre de stations de réception. Ce système a mis en œuvre une solution large bande ADSL par satellite issue d'un projet du Centre National d'Etudes Spatiales, initié en 2003 et qui tendait à mettre en orbite un satellite à faible coût pour les zones rurales, montagneuses ou désertiques.
Le 28 octobre 2005, Michèle Alliot-Marie avait inauguré le « Dupuy-de-Lôme », navire-espion de la DRM. Selon la ministre de la Défense de l'époque « la protection de la France ne peut pas être efficace si la surveillance se limite au territoire national. Il faut aller de plus en plus loin dans le renseignement et être capable d'intercepter les communications partout dans le monde. Le bateau est autorisé à demeurer dans les eaux internationales et donc dans les régions non couvertes par les stations d'écoute de la DRM et de la DGSE, comme en Océan indien ou dans le Pacifique.
Par ailleurs, la France, en coopération avec l'Italie, a développé le satellite de télécommunications à usage mixte civil/militaire, Athena. D'autres programmes de type CISR ont été également initiés en collaboration avec d'autres pays[384].
« Plus que jamais, l'espace, les communications et le renseignement sont au cœur de la défense des pays développés » a déclaré le rapporteur Yves Fromion qui estime que cette tendance s'est accentuée depuis les attentats du 11 septembre 2001 aux USA. « L'espace représente le même enjeu aujourd'hui que la dissuasion nucléaire dans les années soixante ». Ainsi le satellite Hélios II A, qui, en termes de renseignements par l'image, améliore les capacités françaises, le nombre et la qualité des prises de vue, a été lancé en 2004. Il succède à Hélios I, qui fut un très coûteux[385] satellite d'observation militaire que la France a développé en collaboration avec l'Italie et l'Espagne. La DRM et la DGSE ont exercé leur main-mise sur Hélios I. Selon Jean-Michel Boucheron[386] « Jusqu'à une date récente aucun réseau n'était disponible… Des navettes (véhicules, motards) ont ainsi été organisées quotidiennement entre Creil et le siège de la DGSE dans le XXème arrondissement, où à une fréquence moins élevée entre Creil et le siège de la force aérienne de combat à Metz, ou celui de la brigade de renseignement de l'armée de terre. On peut s'interroger sur la rationalité de ces procédures… . A l'heure de la fibre optique et d'Internet, le coût financier et opérationnel de ces liaisons datant d'un autre âge reste à chiffrer ». Hélios 2, lancé le 18 décembre 2004 permet d'atteindre une très haute résolution, de l'ordre de quelques dizaines de centimètres, de prendre des images de jour comme de nuit et d'identifier la différence entre un char et un tracteur. Malgré des dysfonctionnements, les satellites jouent le rôle prééminent et permettent de fiabiliser davantage les interceptions de télécommunications. Il reste à instituer un bon contrôle pour que la vie privée soit respectée.

4) Le terrorisme et le contrôle des interceptions de communications électroniques : la prévention du terrorisme est un des motifs d'interceptions de sécurité. La loi du 23 janvier 2006[387] est relative à la lutte contre le terrorisme. Elle concerne, entre autres, les interceptions de communications électroniques. Elle se réfère au Code des postes et communications électroniques et à la loi pour la confiance dans l'économie numérique[388]. La CNCIS se voit confier de nouvelles missions.

   4.1) Dans le code des postes et des communications électroniques, est inséré l'article L.34-1-1 après l'article L.34-1. Afin de prévenir les actes de terrorisme, les agents

[384] Notamment de l'Union européenne
[385] 10 milliards pour le programme
[386] Cf : « Les coutumes du renseignement » dans « Renseignement par l'image »
[387] Loi n°2006-64
[388] Loi n°2004-575 du 21 juin 2004

individuellement désignés et dûment habilités des services de police et de gendarmerie nationale spécialement chargés de ces missions peuvent exiger des opérateurs la communication des données conservées et traitées par ces derniers.

Les données qui sont susceptibles de faire l'objet de cette demande sont limitées aux données techniques afférentes 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 donnés techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs font l'objet d'une compensation financière.

Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée, placée auprès du ministre de l'intérieur. Cette personnalité est désignée pour une durée de trois ans renouvelable par la CNCIS sur proposition du ministre de l'intérieur qui présente une liste d'au moins trois noms. Des adjoints suppléants sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport annuel d'activité à l'adresse de la CNCIS. Les demandes, dûment motivées, font l'objet d'un enregistrement et sont communiquées à la CNCIS.

La Commission nationale de contrôle des interceptions de sécurité peut à tout moment procéder à des contrôles relatifs aux opérations de communication des données techniques.

Lorsqu'elle constate un manquement aux règles, une atteinte aux droits et libertés, elle saisit le ministre de l'intérieur d'une recommandation. Le ministre fait connaître dans un délai de quinze jours les mesures qu'il a arrêtées pour pallier les manquements constatés.

4.2) La loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure :

Il s'agit, bien sûr, d'achever la mise en application des dispositions de la loi d'orientation et de programmation relative à la sécurité du 21 janvier 1995. Surtout, parmi les moyens juridiques, il convient de renforcer la lutte contre une éventuelle menace terroriste et de recourir aux technologies de l'information. La loi prend acte du retard en matière d'informatique et entend développer un réseau intranet jusqu'à l'échelon des brigades. L'accroissement des capacités de traitement des traces et indices alimente les fichiers, tels le fichier national automatisé des empreintes génétiques, le fichier automatisé des empreintes digitales. Les nouvelles technologies permettent de développer la lecture automatique des passeports et cartes nationales d'identité, la mise en œuvre des technologies de biométrie aux contrôles transfrontières. Une architecture intégrée des systèmes d'information est installée. « A terme, tous les fonctionnaires et militaires, dans la limite de leur habilitation, doivent avoir accès dans le cadre de leurs missions de sécurité, à tout endroit et dans toutes circonstances, à toutes les applications de sécurité intérieure » (Article Annexe). La France est particulièrement favorable à des accords internationaux dans ce domaine.

4.3) La prévention du terrorisme et la loi du 21 juin 2004 pour la confiance dans l'économie numérique :

Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités soit des services de police soit de gendarmerie nationale spécialement chargés de ces tâches peuvent exiger des fournisseurs la communication des données conservées et traitées.

Les demandes des agents sont motivées et soumises à la décision de la personnalité qualifiée envisagée précédemment dans le Code des Postes et des communications

électroniques selon les modalités vues antérieurement. La Commission nationale de contrôle des interceptions de sécurité exerce là aussi son contrôle.
La loi du 10 juillet 1991 a été modifiée et complétée. Citons notamment l'article 27 : « La Commission nationale de contrôle des interceptions de sécurité exerce les attributions définies à l'article L.34-1-1 du code des postes et des communications électroniques et à l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique en ce qui concerne les demandes de communication de données formulées auprès des opérateurs de communications électroniques et personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n°2004-575 du 21 juin 2004 précitée ».
Cette loi, pour laquelle l'urgence avait été déclarée a été discutée à l'Assemblée nationale du 23 au 29 novembre 2005, puis au Sénat pour une seule lecture par chaque Assemblée. La CNIL a émis des réserves importantes sur ce texte[389] mais l'avis de l'autorité de régulation en matière de vie privée et de protection des données personnelles n'a pas été pris en compte ni en considération par Alain Marsaud, rapporteur du projet de loi à l'Assemblée nationale. La CNIL considère que les objectifs de lutte et de prévention du terrorisme poursuivis par le Gouvernement en s'appuyant notamment sur les possibilités nouvelles induites par l'essor des techniques informatiques sont légitimes. Les dispositifs de prévention du terrorisme, prévus par le projet de loi doivent être perçus comme des mesures exceptionnelles. La CNIL estime que l'ensemble du dispositif retenu par le projet de loi doit être encadré précisément par le législateur afin de garantir les libertés individuelles, notamment la liberté de circulation[390]. En effet, elle constate que les mesures prévues, en venant ajouter au cadre de police judiciaire existant en matière de lutte anti-terroriste un cadre de police administrative[391] permet un accès très large à des fichiers publics et privés. Dès lors, des garanties devraient utiliser l'utilisation de ces moyens. Dans ces conditions, la CNIL définit des priorités :

- L'ensemble des mesures prévues doit être limité dans le temps pour une durée de trois ans
- Les mesures feraient l'objet d'une évaluation, remise au Parlement
- La CNIL exerce sans restriction les pouvoirs de contrôle qui lui sont dévolus, notamment depuis la loi du 6 août 2004
- Pour chaque dispositif, des garanties renforcées sont envisagées et des contrôles sont mis en place pour assurer leur respect.

Le projet de loi élargit considérablement les possibilités offertes en matière d'accès aux informations techniques issues de l'utilisation quotidienne faite par chacun du téléphone et de l'Internet : quiconque propose un accès internet au public devra conserver ces données techniques et les services de police et de gendarmerie en charge de lutter contre le terrorisme pourront avoir accès à ces données. La CNIL ne s'oppose pas aux nouvelles possibilités d'accès à ces données offertes aux services de police et de gendarmerie mais met l'accent sur la diversité et la sensibilité des informations ainsi mises à disposition. Les services de police et de gendarmerie pourront avoir accès à tout moment et sans contrôle du juge à l'ensemble des informations liées à l'utilisation du téléphone, à la connexion à Internet depuis un an. La CNIL prend acte avec satisfaction des garanties apportées par le projet de loi, notamment aux tâches dévolues à la CNCIS. Cette autorité administrative indépendante saura assumer des missions

[389] Examen par la CIL du 10 octobre 2005
[390] Article 13 de la Déclaration universelle des droits de l'homme, protocole quatre de la Convention européenne de sauvegarde des droits de l'homme, article douze du Pacte international des droits civils, article 18 de la Charte européenne des droits fondamentaux
[391] C'est-à-dire en dehors du contrôle a priori du juge

délicates. La CNIL remarque que le projet de loi renvoie à un décret d'application fixant notamment les modalités d'habilitation des agents. Cependant, elle ne se dessaisit pas pour autant de son pouvoir de contrôle et d'investigation.

Le projet de loi prévoit également que les services de police et de gendarmerie pourront accéder à des fichiers administratifs gérés par le ministère de l'intérieur. La CNIL propose que la loi ou les décrets d'application précise

la liste des données accessibles strictement nécessaires à la poursuite des finalités de lutte anti-terroriste

L'UMP et le parti socialiste sont d'accord sur les objectifs. Daniel Vaillant[392] déclare : « La lutte contre le terrorisme ne doit pas être l'objet de polémiques entre les responsables politiques respectueux de la République et de la démocratie. Le sujet est trop grave pour être l'otage de calculs tactiques, d'arrière-pensées ou de préoccupations étrangères à son objet ….c'est pourquoi il serait éminemment souhaitable qu'au terme de cette discussion, la représentation nationale puisse voter ce texte, afin de montrer à nos concitoyens notre détermination commune à mener, dans le respect du droit, une lutte efficace contre le terrorisme ». Deux menues réserves sont avancées : il convient de prendre en compte les observations de la CNIL ; des garanties devraient permettre d'encadrer strictement l'accès des services de police aux fichiers administratifs et aux données recueillies. Par ailleurs, le parti socialiste souhaite l'instauration d'un contrôle parlementaire sur les services d'information et de renseignement. Il ne s'agit pas de bouleverser l'économie de la loi : « Il n'y a donc rien dans ces amendements qui remette en cause la philosophie, les objectifs et l'efficacité des mesures de lutte contre le terrorisme que vous nous proposez d'adopter. Si vous répondez à nos demandes, vous créerez les conditions d'un vote positif de notre part »

Seuls, les députés Verts manifestent leur opposition face à cette « union sacrée ».[393]. Noël Mamère met en cause la référence américaine : « Pourquoi aller chercher votre modèle dans un pays dont le « Patriot Act » tire partie des menaces terroristes pour porter atteinte aux libertés et remettre en cause le pacte fondateur de la société américaine que vantait Tocqueville ? » et insiste sur la violation des droits de l'homme : « Cette loi ne fait que tordre le cou à l'article deux de la Déclaration des droits de l'homme, qui protège l'individu contre l'arbitraire de la puissance publique. Toutes les dispositions que vous proposez constituent de nouvelles atteintes aux libertés fondamentales, comme la liberté d'aller et de venir, le droit à l'intimité de la vie privée et particulièrement le secret de la correspondance ». « …la justice est cantonnée au statut d'auxiliaire et les libertés fondamentales considérées comme subsidiaires ».

En dehors des Verts, et, à un moindre degré, du parti communiste français, l'unanimité se fait sur les finalités de la loi. Seules, des questions techniques, telle la coordination entre services de renseignement sont abordées : ainsi, selon, Gérard Léonard « S'agissant des administrations en charge de la lutte contre le terrorisme, je voudrais souligner la nécessité de la coordination et du discernement dans l'action. Outre la DGSE, qui dépend du ministère de la défense, deux grands services concourent à la collecte et à l'exploitation du renseignement en France : la DST et les Renseignements généraux, dont les personnels relèvent du ministère de l'intérieur. L'efficacité de la DST dans la prévention du terrorisme résulte de nombreux atouts : une longue expérience ; des compétences très particulières, qui associent renseignement et police judiciaire ; l'outil juridique très efficace qu'est

[392] Deuxième séance du 23 novembre 2005

[393] «Mes propos risquent de détonner dans cette atmosphère de consensus. Les députés Verts considèrent en effet que ce projet de loi est dangereux et porte une grave atteinte aux libertés publiques ».Noël Mamère. Deuxième séance du 23 novembre 2005. Assemblée nationale

l'incrimination pour « association de malfaiteurs en relation avec une entreprise terroriste » ; la grande qualité de ses agents et les liens personnels de confiance qu'ils ont su nouer avec leurs collègues étrangers ; enfin, le renforcement des relations avec la direction centrale des Renseignements généraux, engagés depuis trois ans…Les partenariats avec la DST, la DNAT et la sécurité publique..sont autant de facteurs qui ont permis de renforcer l'efficacité de notre dispositif de renseignement…Ce rapprochement doit-il pour autant être le prélude à une fusion des deux directions dans un grand service de renseignements ? Je ne le pense pas, car cela risquerait notamment d'éloigner les renseignements généraux d'autres service comme ceux de la sécurité publique qui peuvent fournir des informations recueillies sur le terrain »[394].

Peu d'amendements sont adoptés. Noël Mamère, au nom des Verts propose un amendement 62 visant à renforcer les pouvoirs de contrôle de la CNIL. Cette dernière a émis un avis sur l'avant-projet de loi que la Commission des lois a partiellement pris en compte. Ses prérogatives, selon les Verts, seraient insuffisamment respectées. Elle a alerté le gouvernement sur le changement « profond » auquel correspond ce dispositif et qui « en venant ajouter au cadre de police judiciaire existant en matière de lutte antiterrorisme un cadre de police administrative, c'est-à-dire hors du contrôle a priori du juge, permet un accès très large à certains fichiers publics et privés et aux renseignements de vidéosurveillance ».

La CNIL suggère de limiter l'application de la loi à une durée de trois ans. Cette limitation est prévue pour l'accès aux données de connexion des opérateurs de communications électroniques et à certains fichiers administratifs par les services de police, mais non pour les autres dispositions. Par ailleurs, la CNIL demande que l'application des mesures fasse l'objet d'une évaluation précise remise au Parlement. La loi sur la sécurité quotidienne contenait une clause identique qui n'a jamais été mise en œuvre. La CNIL exige également de pouvoir exercer pleinement ses pouvoirs de contrôle alors que la présente loi les limite, surtout en cas d'urgence. Le rapporteur de la Commission des lois, Alain Marsaud, émet un avis défavorable[395]. Christian Estrosi[396] fait remarquer que la CNIL a effectivement émis quelques remarques sur certains articles du projet de loi mais oppose à l'avis de la CNIL l'avis de l'Assemblée générale du Conseil d'Etat, « institution qui a quelques titres pour dire le droit et faire respecter les libertés publiques » et qui approuve le projet de loi du Gouvernement « à quelques points près ». Le gouvernement oppose en la matière les avis de deux organismes qui ont des statuts différents, l'un ayant un rôle consultatif tout en étant par ailleurs la juridiction suprême dans l'ordre administratif, l'autre étant une autorité administrative indépendante. Et il est vrai que le gouvernement suit plus fréquemment les avis du Conseil d'Etat que les avis de la CNIL. L'amendement 62 est rejeté devant l'Assemblée nationale.

Jacques Floch présente ensuite, pour le parti socialiste, un amendement n°82 visant à permettre le contrôle du Parlement sur les services de renseignement[397].

---

[394] Gérard Léonard, Assemblée nationale, deuxième séance du 23 novembre 2005

[395] « Cet amendement relève de la tautologie ». Alain Marsaud, Assemblée nationale, première séance du 24 novembre 2005

[396] Alors ministre délégué à l'aménagement du territoire

[397] « Nous sommes un des rares démocratiques où le Parlement ne contrôle pas les services de renseignements. Pourtant, nous légiférons sur eux et nous votons des budgets, lesquels ont d'ailleurs permis que ces services se situent parmi les meilleurs au monde. Considérant qu'il serait normal que les représentants du peuple soient informés de la façon dont ces services travaillent et puissent les évaluer, en même temps que leur apporter un

Ces derniers sont tenus de rendre des comptes au ministre de l'intérieur, au ministre de la défense et au Président de la République, mais ils ne rendent pas de comptes au Parlement alors que c'est une obligation pour presque tous les pays européens, si l'on excepte le Portugal. Un amendement 124 rectifié propose qu'un juste équilibre soit créé entre d'une part, le renforcement des moyens d'action de la puissance publique dans la lutte contre le terrorisme, d'autre part, le strict encadrement juridique des moyens, conformément aux principes fondamentaux du droit français[398]. Enfin, Pierre Lellouche, pour l'UMP, propose un amendement 134. Selon lui, les services de renseignement ne constituent pas un domaine réservé de l'exécutif, puisque le contrôle parlementaire s'applique déjà en matière de défense et que la lutte contre le terrorisme peut être perçue comme un prolongement des missions de défense nationale. Le contrôle serait assuré dans un strict respect de la confidentialité requise et se ferait sans interférence avec les opérations en cours. Toutes les grandes démocraties se sont dotées d'instruments de ce genre. L'amendement 134 implique la création d'une instance composée de trois députés et trois sénateurs, ainsi que de représentants du Conseil d'Etat, de la Cour de cassation et de la Cour des comptes. La commission des lois de l'Assemblée nationale n'a pas examiné l'amendement 82, a repoussé l'amendement 134, a adopté le 124 rectifié. Ce dernier stipule notamment que la commission de contrôle ne serait pas susceptible d'intervenir dans la réalisation d'opérations en cours. Les Verts décident alors de soutenir l'amendement présenté par Jacques Floch. Le ministre de l'intérieur se prononce en faveur d'un contrôle parlementaire sur les services de renseignements[399]. Il suggère de mettre en place un groupe de travail réunissant les représentants des groupes parlementaires et les hauts fonctionnaires des services de renseignement ; ce groupe de travail rendrait ses conclusions en février 2006 et déboucherait sur un projet ou sur une proposition de loi. Néanmoins, certains parlementaires sont toujours favorables à l'adoption d'un contrôle parlementaire sur les services de renseignement. Michel Vaxès déclare : « Le ministre se dit ouvert et n'exclut aucune des trois formules proposées. Or je constate que l'amendement présenté par M.Floch présente toutes les garanties de pluralisme. Rien ne nous empêcherait de l'adopter, quitte à réunir ensuite une commission pour proposer d'éventuelles améliorations ». Jacques Floch renchérit : « ..Je veux obtenir la création d'une commission de contrôle parlementaire. Je veux par ailleurs faire observer que la constitution de la Vème République ne reconnaît aucun domaine réservé au Président de la République : c'est une habitude qui a été prise sous le général de Gaulle et qui a perduré après

---

soutien juridique, je propose, par l'amendement 82, la création d'une délégation, d'un office ou d'une commission, peu importe le nom, qui puisse être le lieu où cette évaluation se fasse », Jacques Floch, Assemblée nationale, première séance du 24 novembre 2005

[398] « Faut-il dans ce cadre doter le parlement d'un organe de contrôle de nos services de renseignement ? Je pense qu'en effet, le moment est venu de le faire, car avec le terrorisme, le débat a changé de nature. Et de même que le Parlement contrôle, en particulier via la commission de la défense, nos militaires, confirmant ainsi que la défense est l'affaire de tous, de même faut-il un contrôle démocratique des services engagés dans la lutte contre le terrorisme, qui est aussi l'affaire de tous », Pierre Lellouche, Assemblée nationale, première séance du 24 novembre 2005

[399] « Dans toutes les démocraties avancées, à de très rares exceptions près, le Parlement exerce une responsabilité de contrôle sur les activités de renseignement….cette exigence démocratique est d'autant plus forte lorsque la loi confie aux services de renseignement de nouveaux instruments, comme c'est le cas avec ce texte, qui facilite l'accès d'agents spécialisés à certains fichiers… Aussi le Gouvernement examine-t-il avec le plus grand intérêt ces tris amendements… »Nicolas Sarkozy ministre de l'intérieur, Assemblée nationale, première séance du 24 novembre 2005

lui. »[400]. A la suite des discussions entre parlementaires, l'amendement 134, puis l'amendement 124 rectifié sont retirés. M.Vaxès, alors représentant de la gauche républicaine[401], reprend l'amendement 82. Il n'est pas suivi par le parti socialiste, tout acquis à l'objectif de consensus : « Je souhaite que nous n'ayons pas à voter sur cet amendement pour ne pas marquer négativement le débat. Cette situation pourrait trouver un débouché si l'engagement était pris devant la représentation nationale et inscrit dans nos documents officiels, que ce dispositif sera pluraliste ». Finalement, le vote a lieu et l'amendement 82 est repoussé. Par la suite, un groupe de travail est bien créé, débouche sur un projet de loi, qui n'a pas été mis à l'ordre du jour.

Le débat afférent à l'article quatre concerne les données et les communications électroniques. Comme l'a souligné dans son avis du 26 septembre 2005 le contrôleur européen des données, les dispositions relatives aux conditions d'accès aux données retenues relèvent de la compétence exclusive des Etats. Les mesures permettant l'accès direct aux données retenues par les opérateurs, en dehors de tout contrôle judiciaire, sont identiques à celles qui autorisent les interceptions de sécurité. L'article quatre élargit la notion d'opérateur de communications électroniques à toute personne qui propose un accès internet au public comme les cybercafés. Le rapporteur indique que seules sont visées les personnes qui offrent une connexion dans le cadre d'une activité professionnelle mais la notion est parfois difficile à cerner. Cependant, il est clair que les nouveaux opérateurs devront conserver certaines données techniques de connexion. L'amendement 69 est présenté. Il vise à définir précisément les personnes qui devront conserver les données techniques de connexion. Il est soutenu par le PCF et les Verts. Le rapporteur reconnaît que le concept d'activité professionnelle est flou mais il revient à la jurisprudence et à l'Exécutif de clarifier la définition. Selon le ministre de l'intérieur Nicolas Sarkozy, ce sont les cybercafés qui sont concernés. Ce sont en effet les cybercafés qui offrent au public une connexion au réseau internet, qui doivent conserver les données techniques de connexion, numéros de terminaux, dates, horaires, durée de communication, indépendamment des données de contenu, comme par exemple le contenu d'un mél. Les mairies, les universités, les bibliothèques, les médiathèques n'entrent pas dans le champ d'application. S'il apparaissait qu'une bibliothèque jouait le rôle de cybercafé, elle pourrait entrer dans le champ des personnes soumises à l'obligation de conservation des données au titre de leur activité accessoire. La définition n'appelle pas de précision par décret. L'argumentation ne convainc pas les défenseurs de l'amendement[402], qui mettent l'accent sur le danger d'insécurité juridique. L'amendement 69 est repoussé.

L'article 5 vise à permettre une exploitation rapide des données techniques générées par les communications électroniques. Les services de police spécialisés dans la lutte contre le terrorisme pourraient ainsi se faire communiquer ces

[400] Michel Vaxès, Jacques Floch, Assemblée nationale, première séance du 24 novembre 2005

[401] Communiste

[402] « Pourquoi ne pas inscrire précisément dans la loi la liste des personnes devant conservet les données relatives à l'utilisation d'internet ? » Noël Mamère. « le ministre a exclu de l'obligation de communication des données les bibliothèques, les universités, les hôtels de ville….Le cas échéant, il ne faudra donc pas leur reprocher a posteriori de ne pas avoir accumulé l'ensemble des éléments d'information nécessaires à une enquête. L'imprécision du texte est dommageable…. » Michel Vaxès, première séance du 24 novembre 2005

données techniques dans un cadre juridique administratif, c'est-à-dire hors de tout cadre judiciaire.

L'amendement 12 codifie les dispositions de cet article 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. Ces deux textes tendent à préciser les obligations à la charge des opérateurs de communications électroniques et des hébergeurs de sites internet. Selon le rapporteur, il est souhaitable que les nouvelles obligations à la charge des opérateurs de communications électroniques et des hébergeurs de sites internet soient codifiées dans un souci d'accessibilité et d'intelligibilité de la loi. Cela correspond à une exigence de sécurité juridique. L'amendement 12 est accepté par le gouvernement et adopté.

L'amendement 110 est présenté par Michel Hunault[403]. Sa finalité est de donner au juge des libertés et de la détention le pouvoir de décision et de contrôle lorsque des agents habilités demandent que soient communiquées les données techniques des communications électroniques. Le rapporteur émet un avis défavorable : le projet est afférent à la police administrative ; il ne convient donc pas de faire intervenir le juge judiciaire ; la justice n'est pas concernée. Au demeurant, si le droit rendait possible cette procédure, les juges des libertés et de la détention seraient surchargés de travail. Mais le droit fait obstacle à la procédure : il ne faut pas confondre les pouvoirs.

L'amendement 110 est repoussé par le gouvernement et n'est pas adopté.

L'amendement 15 a pour objectif de faire nommer la personnalité chargée d'examiner les demandes des agents habilités par la Commission nationale de contrôle des interceptions de sécurité et non par le ministre de l'intérieur. C'est un gage d'impartialité et cela correspond à la première mouture du texte[404]..

Un autre amendement, 92 vise aussi à améliorer l'impartialité de la nomination et propose de demander à la CNIL son avis. Selon le rapporteur,, la CNIL n'a pas vocation à donner cet avis. En conséquence, l'amendement 15 est adopté et l'amendement 92 repoussé.

L'amendement 126 est relatif à la CNCIS et au contrôle exercé par la CNCIS dans le secteur des opérations de communication des données techniques. Il ne convient pas que les recommandations de la CNCIS soient rendues publiques, mais d'envisager un bilan des suites données aux recommandations. L'amendement 126 est adopté.

Au Sénat, le consensus existe également mais les débats sont un peu plus animés.

L'amendement 69 est présenté par Mmes Assassi, Borvo Cohen-Seat, Mathon-Poinat et les membres du groupe Communiste Républicain et Citoyen. Mme Josiane Mathon-Poinat rappelle que l'article 5 du projet de loi tend à permettre, dans le cadre des pouvoirs de police administrative, l'accès des agents individuellement habilités des services de police et de gendarmerie nationale à certaines données de trafic générées par les communications électroniques. « Alors qu'actuellement ces données sont systématiquement communiquées dans un cadre administratif adapté et donc en dehors de tout contrôle du juge judiciaire, nous ne saurions l'accepter ». Mme Mathon s'appuie sur cet extrait de l'avis de la CNIL rendu le 10 octobre 2005[405]. « L'obligation ainsi faite aux opérateurs de

[403] UDF en 2005, réélu Nouveau Centre en 2007

[404] « Je propose donc d'y revenir, même si je fais confiance au ministre de l'intérieur pour faire en sorte que la personnalité qualifiée soit impartiale ». Le rapporteur, Assemblée nationale, première séance du 24 novembre 2005

[405] Mme Mathon-Poinat, Sénat, Séance du 15 décembre 2005

communiquer, dans le cadre des pouvoirs de police administrative et hors contrôle des autorités judiciaires, les traces des connexions qui, par recoupement avec d'autres données, peuvent dévoiler l'identité des utilisateurs d'internet, leur navigation sur le web et, de manière plus générale, l'usage privé que l'on fait du réseau déroge aux principes fondamentaux de protection des libertés individuelles ». Il s'agit de faire respecter le droit à la vie privée. Cette réquisition administrative ne serait pas entourée de garanties suffisantes permettant de préserver les libertés individuelles, dont le droit à la vie privée est l'une des composantes. La limitation dans le temps[406] n'est pas entièrement rassurante[407].
Un amendement n°40 est proposé par Mmes Boumediene-Thiery, Blandin et Voynet et M.Desessard, inspiré par l'inquiétude qu'induit la procédure de réquisition administrative, qui ne respecterait pas le principe de proportionnalité[408].
Les auteurs de l'amendement 40 se félicitent de l'accroissement des compétences dévolues à la Commission nationale de contrôle des interceptions de sécurité mais déplorent que la CNCIS ne dispose pas de davantage de moyens financiers et souhaitent que cette autorité administrative indépendante gagne en autonomie. Ils regrettent enfin que la CNIL n'exerce pas de contrôle.
Néanmoins, le gouvernement et le ses sénateurs sont d'accord pour que la commission nationale de contrôle des interceptions de sécurité soit placée au cœur du dispositif. Les sénateurs socialistes et notamment MM. Peyronnet, Badinter, Boulaud, Mmes Cerisier-ben Guiga, Tasca, MM.Collombat, Frimat et C.Gautier, Mme Khiari, MM.Mermaz, Sueur, Vantomme, Yung, Mme Boumediene-Thiery présentent un amendement 90 ainsi libellé : « Remplacer le quatrième alinéa du texte proposé par le I de cet article pour l'article L.34-1-1 du code des postes et des communications électroniques par un alinéa ainsi rédigé :
Les demandes des agents sont motivées et soumises à la décision de la Commission nationale de contrôle des interceptions de sécurité. Ces demandes, accompagnées de leur motif, font l'objet d'un enregistrement. Cette instance établit un rapport d'activité annuel adressé au ministre de l'intérieur et à la Commission nationale de l'informatique et des libertés… »
M.Jean-Pierre Sueur, appartenant au groupe socialiste évoque le travail de la CNCIS. Cette dernière comprend en son sein des magistrats dont l'autorité est généralement reconnue.
Certes, la Commission nationale de contrôle des interceptions de sécurité est un organisme consultatif. Il n'est pas susceptible d'imposer des décisions au chef de l'administration, mais, et ceci au fil des différents gouvernements, le Premier ministre suit presque toujours les avis de la CNCIS, ce qui prouve la pertinence des avis susenvisagés. Il est possible de faire évoluer les compétences de cette autorité administrative indépendante sur des sujets qui, en matière de respect des libertés publiques, requièrent une vigilance accrue. Le seul contre-argument est celui de l'urgence et de la rapidité. Or, la CNCIS a su faire preuve d'une grande réactivité dans un passé récent.

[406] Jusqu'au 31 décembre 2008
[407] « Rappelons…que des dispositions antiterroristes insérées dans la loi relative à la sécurité quotidienne au lendemain des attentats du 11 septembre, bien qu'initialement limitées dans le temps, ont été cependant prorogées ». Mme Josiane Mathon-Poilat, Sénat, séance du 15 décembre 2005
[408] « Les mesures permettant l'accès direct aux données retenues par les opérateurs, en dehors de tout contrôle judiciaire, sont au fond de même nature que celles qui autorisent les interceptions téléphoniques administratives. Prévoir un dispositif d'autorisation et de contrôle distinct constitue donc une source de complexité injustifiée qui affaiblit l'effectivité des garanties offertes, déjà toutes relatives », Mme Alima Boumediene-Thiery, Sénat, séance du 15 décembre 2005

Jean-Pierre Sueur rappelle qu'en avril 2003, sans modification de la loi de 1991, et en accord avec Jean-Pierre Raffarin, alors premier ministre, le régime d'avis préalable aux demandes d'interceptions a été étendu aux demandes urgentes. Cette réforme a été motivée par l'accroissement du nombre de décisions d'interceptions urgentes. Selon les chiffres communiqués par la CNCIS, cette évolution a été réalisée sans ralentissement, grâce à la disponibilité accrue de la structure permanente de la commission, qui est en mesure de rendre un avis dans un délai maximal d'une heure en cas de saisine urgente, en se fondant sur la jurisprudence de la commission. Ainsi, le délégué général de la commission ou son adjoint, informe systématiquement le président de l'autorité de toute saisine. En effet, l'article premier du règlement intérieur de la CNCIS prévoit que celle-ci se réunit sur l'initiative de son président lorsque celui-ci estime que la légalité d'une autorisation d'interception n'est pas certaine. Le dispositif actuel est fiable et réactif.

« Dans le cas qui nous occupe, ce qui est vraiment incompréhensible, surtout lorsqu'il s'agit d'un problème d'interception de communications, qui a donc trait aux libertés publiques, c'est que vous nous demandiez de vous affranchir des prérogatives de cette commission pour, si j'ai bien compris, mettre en place une personnalité qualifiée. Vous avez même obtenu à l'Assemblée nationale que celle-ci soit nommée par la commission, mais sur proposition du ministre de l'intérieur. Alors, foin d'hypocrisie ! Autant dire que cette personnalité qualifiée est nommée par le ministre de l'intérieur

Dans ce cas précis, c'est d'autant plus incompréhensible que le pouvoir régalien de l'Etat intervient en dehors de toute autorité de justice et même en dehors de la commission mise en place à cet effet ! Pourtant, il a été démontré que cette commission, à laquelle M.Jean-Pierre Raffarin a fait référence, qu'il a lui-même utilisée-et je ne doute pas que M.de Villepin fera de même-peut se prononcer en moins d'une heure ! »

Ce point de vue n'est pas partagé par la majorité mais des sénateurs UMP déposent des amendements pour améliorer la qualité rédactionnelle.

Ainsi, MM.Portelli, Türk, Nogrix, Mme Malovry, MM.Mouly, Sellier, Cambon, Goujon, Lecerf déposent un amendement 54 ainsi rédigé :

« Rédiger comme suit la deuxième phrase du quatrième alinéa du texte proposé par cet article pour l'article L.34-1-1 du code des postes et des communications électroniques :

Cette personnalité est désignée pour une durée de trois ans renouvelable, par la Commission nationale de contrôle des interceptions de sécurité parmi les personnes figurant sur une liste établie par le ministre de l'intérieur et comportant trois noms ». Ainsi, la CNCIS pourra-t-elle établir son choix entre trois noms[409].Par ailleurs, MM.Türk, Portelli, Nogrix, Mme Malovry, MM.Mouly, Sellier, Cambon déposent un amendement 55 rectifié bis ainsi libellé :

« Compléter l'avant-dernière phrase du quatrième alinéa du texte proposé par le I de cet article pour l'article L34-1-1 du code des postes et des communications électroniques par les mots :

Et à la Commission nationale de l'informatique et des libertés »

Lucienne Malovry explique que des garanties complémentaires seraient les bienvenues dans la mesure où le texte prévoit l'accès des services de police aux données de connexion et où certaines informations dont les agents des services de

[409] « Le choix entre plusieurs candidats apportera une plus grande objectivité à la désignation de la personnalité qualifiée par la CNCIS », Lucienne Malovry, Sénat, séance du 15 décembre 2005

police et de gendarmerie nationale ont connaissance sont particulièrement sensibles. Dans ce contexte, l'intervention de la CNIL est justifiée par la nature des données qui relèvent directement de la loi du 6 janvier 1978 modifiée le 6 août 2004. Au demeurant, le ministre de l'intérieur et la personnalité qualifiée conservent leurs compétences ; il s'agit simplement de rendre la CNIL destinataire du rapport annuel établi par la personnalité qualifiée. Au demeurant, cette transmission était prévue dans l'avant-projet de loi.

Le rapporteur[410] se prononce contre l'amendement 69, contre l'amendement 40, parce qu'il vise à supprimer la procédure spéciale selon laquelle seront autorisées les demandes de réquisition administrative des données de connexion. De plus, selon M.Courtois, les auteurs de l'amendement 40 souhaitent que cette procédure afférente aux données de connexion soit confondue avec la procédure applicable aux interceptions administratives. Or, les données de connexion ne sont pas de la même nature que les interceptions de sécurité. Une donnée de connexion ne porte pas sur le contenu des communications. M.Courtois soutient qu'il n'y a pas, en la matière, de danger pour le droit à la vie privée[411]. Sur l'amendement 90, le rapporteur émet aussi un avis défavorable : il ne va pas dans le sens du projet de loi, puisqu'il attribue à la commission nationale de contrôle des interceptions de sécurité les pouvoirs de contrôle des réquisitions administratives des données techniques que le projet de loi a dévolus à une personnalité qualifiée nommée par la CNCIS. Le rapporteur justifie cet échafaudage : le choix de confier à une personnalité qualifiée le contrôle des réquisitions a été guidé par le souci de ne pas alourdir les missions de la CNCIS[412]. De plus, en confiant ce contrôle à une personnalité qualifiée, il est possible de concilier l'objectif de rapidité et l'objectif de sauvegarde des libertés individuelles[413]. La personnalité qualifiée remplit mieux ce rôle que ne pourrait le faire la CNCIS, car il serait très difficile, pour des raisons matérielles qu'elle exerce un contrôle a priori.

Le rapporteur se prononce en faveur de l'amendement n°54 rectifié ter ; la CNCIS pourra choisir entre trois noms présentés par le ministre de l'intérieur[414]. ; sa position est mitigée sur l'amendement 55 rectifié bis. Il n'est pas opposé à l'amendement mais redoute une confusion entre les missions de la CNCIS et celles de la CNIL[415]Il demande donc le retrait de l'amendement 55 rectifié bis, ce qui est fait. Les échanges d'arguments devant le Sénat semblent beaucoup plus pertinents que devant l'Assemblée nationale.

La loi a été adoptée à une large majorité, avec une volonté de consensus de la classe politique. Le texte définitif du projet de loi a été adopté par le Parlement[416], l'Assemblée nationale et le Sénat ayant trouvé un accord sur le texte mis au point par la Commission mixte paritaire Le Conseil constitutionnel, saisi le 23 décembre

[410] Jean-Patrick Courtois

[411] « ….au regard du respect des libertés individuelles, leur réquisition est…beaucoup moins instructive. J'ajoute que, contrairement aux écoutes administratives, la procédure proposée offre des garanties fortes puisqu'il s'agit non pas d'un contrôle a posteriori, mais d'un contrôle a priori » Jean-Patrick Courtois, Sénat, séance du 15 décembre 2005

[412] Commentaire de Jean-Pierre Sueur : « Cela ne tient pas », Sénat, séance du 15 décembre 2005

[413] Commentaire de Jean-Paul Sueur : « Une personnalité qualifiée respecterait mieux les libertés individuelles ! C'est incroyable ! » Sénat, séance du 15 décembre 2005

[414] « Je suis favorable à ce dispositif : de la sorte, la CNCIS ne se verra pas imposer un candidat, elle aura le choix », Jean-Patrick Courtois, Sénat, séance du 15 décembre 2005.

[415] « Je crains qu'il n'engendre un enchevêtrement entre les missions de la CNCIS et celles de la CNIL », Jean-Patrick Courtois, Sénat, séance du

[416] Par l'Assemblée nationale le 29 novembre 2005, par le Sénat, avec modification, le 15 décembre 2005

2005 d'un recours présenté par plus de soixante sénateurs valide l'essentiel de la loi, hormis les articles 6[417] et 19[418] le 19 janvier 2006 Elle est promulguée le 23 janvier 2006, est publiée au Journal officiel le 24 janvier 2006. La .CNIL établit un bilan. Elle se félicite notamment que le respect de la loi Informatique et libertés ait été pris en compte dans le cadre des dispositifs anti-terroristes, à l'exception toutefois de la vidéosurveillance. Elle considère que des précisions utiles ont été apportées quant aux services de police et de gendarmerie accédant aux données pour des finalités anti-terroristes. Les conditions d'habilitation et d'accès aux données sont définies, certains dispositifs sont limités dans le temps, un rapport d'évaluation annuel est remis au Parlement.

Elle regrette l'absence de définition des personnes offrant un accès à internet et chargées de conserver la trace des données de l'ensemble des connexions.

Des organismes de défense des droits de l'homme ont manifesté leur opposition. Il convient de mentionner la Ligue des droits de l'homme[419], le Syndicat de la Magistrature[420], le Syndicat des avocats de France[421], l'intercollectif Droits et libertés face à l'informatisation de la société[422], l'association Imaginons un réseau Internet solidaire[423], la Coordination anti-vidéosurveillance d'Ïle de France[424]. Les intervenants ont mentionné que cette loi constituait un nouveau maillon de la longue chaîne de mesures qui, depuis la loi sur la sécurité quotidienne de novembre 2001, ont porté atteinte aux droits fondamentaux, aux libertés individuelles et collectives, aux garanties de la procédure judiciaire. Selon ces entités, et souvent traduites par des dispositions qui paraissent simplement techniques, ces mesures ont en fait pour objectifs la restriction de l'immigration et la répression de la petite délinquance alors que l'objectif avoué est la lutte contre le terrorisme. Les dispositions légales organisent le contournement des garanties offertes par l'intervention préalable de l'autorité judiciaire ou d'autorités de contrôle indépendantes. En fait, la CNCIS se voit confier des tâches supplémentaires. Ces missions sont-elles en conformité avec la sauvegarde de la vie privée ? Il faut étudier les décrets d'application pour donner une réponse adéquate. C'est le ministre de l'Intérieur qui établit la liste de trois noms où la CNCIS devra faire son choix. Tout dépend des relations instituées entre le ministre de l'Intérieur et la CNCIS. Jusqu'à maintenant, l'interlocuteur privilégié, au sein de l'Exécutif de la CNCIS, était le premier ministre, chef de l'administration.

Selon la Ligue des droits de l'homme, cette loi bat en brèche le principe de finalité[425] qui préside au stockage des fichiers informatiques et de la protection des données personnelles. Les moyens seraient disproportionnés par rapport aux buts poursuivis alors que les autorités de régulation en matière de protection des données se sont prononcées en faveur de la proportionnalité. Il y aurait détournement de finalité, ce qui est strictement interdit par les directives de l'Union européenne du 24 octobre 1995 et 12 juillet 2002, ainsi que par la loi du 6 janvier 1978, révisée et complétée par la loi du 6 août 2004. Les

[417] Censure de la référence à la « répression du terrorisme

[418] Amendement sur la représentation syndicale dans les commissions administratives paritaires compétentes pour les corps de fonctionnaires actifs de la police nationale, qualifié de « cavalier législatif »

[419] LDH

[420] SM

[421] SAF

[422] DELIS

[423] IRIS

[424] Antivideo-IDF

[425] Directive 95/46 du 24 octobre 1995, Article six, b) « Les Etats membres prévoient que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.3

détournements de finalité sont rarement sanctionnés mais les peines d'amende prévues pour cette infraction sont élevées. Sur ce point, l'application de la loi est trop récente pour qu'il soit possible de déterminer si le principe de finalité et celui de proportionnalité sont bien observés.

Les décrets d'application sont minutieusement étudiés même s'ils n'ont pas été médiatisés. Le décret afférent à la conservation des données par les fournisseurs d'accès et les fournisseurs d'hébergement[426]détermine, en application du II de l'article six de la LCEN, la nature des données à conserver par ces intermédiaires techniques ainsi que la durée de cette conservation. Le chapitre 2 porte sur les conditions de fourniture de ces données aux services de police et de gendarmerie, en application du IIbis de ce même article, introduit dans la LCEN par la loi de lutte contre le terrorisme du 23 janvier 2006.

En parfaite cohérence avec le décret du 24 mars 2006 relatif à la rétention des données de communications, introduite par la loi sur la sécurité quotidienne de novembre 2001, le chapitre premier du décret fixe la durée de conservation des données à un an ; cette durée semble normale et légitime au législateur, surtout par référence à Rip Act, trop longue aux yeux des défenseurs des libertés individuelles, qui font valoir en outre que le délai de conservation des données par les hébergeurs prend comme point de départ la moindre modification par l'abonné d'un quelconque contenu hébergé, y compris sa suppression.

Les dispositions relatives au contenu des données sont encore plus débattues. Si elles paraissent légitimes à de nombreux observateurs, elles sont critiquées par les zélateurs des libertés individuelles. Alors que ces données ne sont censées servir qu'à « permettre l'identification de quiconque a contribué à la création du contenu » d'un service, le décret prévoit la conservation de données qui vont bien au-delà de cet objectif, comme par exemple le mot de passe fourni lors de la souscription d'un contrat d'abonnement ou lors de la création d'un compte auprès du prestataire Internet. IRIS, en particulier, s'inquiète à ce sujet[427] :

« A quoi une telle donnée va-t-elle être employée, soit par l'autorité judiciaire en vertu du II de l'article 6, soit par les services de police et de gendarmerie en vertu du IIbis de cet article, c'est-à-dire dans le cadre d'une enquête administrative ? Aucun garde-fou n'est prévu alors que la loi sur la prévention de la délinquance du 5 mars 2007[428]a encore étendu les prérogatives des services de police judiciaire[429]. L'article 35 prévoit en effet que les enquêteurs peuvent participer à des échanges électroniques sous pseudonyme, et peuvent détenir et fournir des contenus illégaux, dans le cadre d'enquêtes sur certaines infractions » Les défenseurs des droits de l'homme craignent qu'un mot de passe ne soit utilisé à mauvais escient, mettant en danger des personnes innocentes. La conservation des informations semble au demeurant excessive et non pertinente, et pas justifiée par la loi que ce décret est censé préciser.

L'article deux du décret fixe les conditions dans lesquelles les services de police et de gendarmerie peuvent demander et traiter les données conservées par les fournisseurs d'accès et d'hébergement ; ce chapitre mentionne que ces données, une fois obtenues, pourront être conservées pendant trois ans « dans des traitements automatisés mis en œuvre par le ministère de l'intérieur et de l'aménagement du territoire et le ministère de la défense ». Toute trace de la demande elle-même aura disparu au bout d'un an. Il s'agit en

[426] Article six de la LCEN

[427] Communiqué de presse d'IRIS, 20 avril 2007 :

[428] Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance a encore étendu les prérogatives des services de police judiciaire

[429] Edrigram,lettre électronique d'EDRI du 14 mars 2007 : Enditorial : French Law On Delinquency : The Thrat To Foe Is Elsewhere

l'occurrence d'enquêtes administratives et non pas judiciaires. Le décret constitue en fait un moyen d'étendre la durée de rétention de données au-delà de ce que permettent les législations française et européenne (respectivement un an et de six à vingt-quatre mois). Ces mesures se situent dans la continuité de lois sécuritaires, comme la loi sur la sécurité quotidienne.

Selon le décret du 24 mars 2006[430], les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales les informations afférentes aux équipements terminaux permettant d'identifier l'utilisateur, les données relatives aux équipements terminaux de communication 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. Pour les activités de téléphonie, l'opérateur conserve les données mentionnées précédemment, celles permettant d'identifier l'origine ou la localisation de la communication ; la durée de conservation des données mentionnées est d'un an à compter du jour de l'enregistrement.. pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois les données permettant d'identifier l'origine de la communication, les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication, les données à caractère technique permettant d'identifier le ou les destinataires de la communication, les données afférentes aux services complémentaires demandés ou utilisés et leurs fournisseurs.

H) L'Union européenne :

L'objectif est toujours de mutualiser un certain nombre de programmes. A l'occasion du lancement des satellites Hélios et Essaim, Michèle Alliot-Marie indiquait que « seule une dynamique européenne permettra de répondre à l'ampleur des besoins… Notre effort de recherche nous permettra de donner une impulsion à cette démarche, qui doit être résolument européenne. La France continuera à jouer un rôle moteur dans ce domaine… afin de bâtir ensemble les programmes dont l'Europe a besoin ». Paul Quilès est plus pessimiste. Il insiste sur « la dissymétrie entre des USA dont la supériorité en matière spatiale militaire est écrasante et une Europe, nouvel acteur encore balbutiant dans ce domaine, est énorme : comment comparer un Etat qui dépense 18,6 milliards de dollars [431] par an au spatial civil et militaire et une union d'Etats qui consacrent, de manière partiellement coordonnée, 1,9 milliard d'euros par an au spatial civil et miliaire-dont 500 millions d'euros dépensés par la France pour le seul spatial militaire ? Comparaison d'autant plus délicate quand on sait que les premiers ont augmenté ces crédits entre 2001 et 2003. Ce qui n'empêche pas la délégation générale pour l'armement (DGA) de travailler sur plus d'une vingtaine de programmes de type CISR ». Le Conseil

a adopté un protocole à la convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, établi par le Conseil conformément à l'article 34 du traité sur l'Union européenne. Ce protocole a été transposé dans le cadre de la loi française du 30 mars 2005. La coopération judiciaire entre les Etats membres de l'Union européenne ne date pas du vingt-et-unième siècle. Elle se base sur les instruments internationaux adoptés sous l'égide du Conseil de l'Europe. Il convient de citer notamment la convention européenne d'entraide judiciaire dans le domaine pénal du 20 avril 1959 et son protocole du 17 mars 1978. Ces textes ont été complétés par la convention d'application de l'Accord de Schengen du 14 juin 1990 et par le traité Benelux d'extradition et d'entraide judiciaire du 27 juin 1962. La suppression des contrôles aux

[430] Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques
[431] Chiffres 2005

frontières entre les Etats membres des accords de Schengen a induit une augmentation importante des flux migratoires, de la circulation des personnes et des marchandises. Des rapports ont mis l'accent entre cette libéralisation et le développement de la délinquance. Le traité de Maastricht a fait entrer les questions judiciaires dans le champ européen mais sur le seul mode intergouvernemental. Quant au traité d'Amsterdam, il étend à la coopération judiciaire le droit d'initiative de la Commission européenne et permet l'entrée en vigueur des conventions lorsqu'elles ont été ratifiées par la moitié des Etats membres. Ces normes s'appliquent également à l'Islande et la Norvège, qui sont associés aux accords de Schengen depuis 1996.

Les experts européens, et ceci depuis le début des années mille neuf cent quatre-vingt dix travaillent sur la surveillance des échanges de méls et les conversations téléphoniques internationales. Il s'agit, dans un monde globalisé au niveau de l'économie, mais aussi des infrastructures de télécommunications, d'étendre la capacité de surveillance. Devant cette option, les réactions sont bien différentes : « Les polices sont en train de nouer des arrangements, en coulisses, pour pouvoir surveiller, sans décision de justice !-le téléphone, Internet ou Iridium » s'inquiète la députée européenne irlandaise Patricia McKenna. « Les plans qui ont filtré jusqu'à nous risquent d'offrir un accès illimité des polices à toutes nos communications ».Un expert français du ministère de l'intérieur justifie : « Notre objectif est simple. Tous les opérateurs de télécommunications-et je ne parle pas que du téléphone-doivent tenir compte des nécessités policières. Les membres de l'Union cherchent à fixer ensemble les normes qu'ils leur imposeront ». Menés sous la houlette du conseil des ministres de l'Union européenne, les travaux ne font l'objet d'aucune publicité. L'opacité menace : « Quelques exigences élémentaires devraient être respectées[432]. Il faut qu'il y ait une certaine maîtrise de ce qui est surveillé et une dose de contrôle parlementaire, européen ou national. Nous n'avons pas d'objection de principe au fait qu'il y ait des écoutes, mais la lutte contre le terrorisme et les filières de blanchiment ne peut servir de prétexte à l'écoute d'Amnesty International ou à l'espionnage économique ». A ce stade, un contrôle est donc envisagé mais les contrôles paraissent assez flous.

La démarche a commencé en décembre 1991, lorsque le groupe de Trevi[433]est créé. Sollicité par le FBI américain, le groupe de Trevi se fixe comme objectif d' « étudier les effets des développements légaux, techniques et du marché…sur les possibilités d'interception, et les actions à entreprendre ». Le FBI a réuni plusieurs Etats membres de l'Union européenne afin de déterminer comment utiliser les nouveaux moyens de télécommunication pour qu'ils puissent être exploités par les agences de sécurité concentrant le renseignement. Il s'agit de savoir comment inciter les industries de la télécommunication à fabriquer des matériels et des logiciels qui permettent l'interception[434]. Il s'agit également de vérifier si les personnes concernées disposent bien du pouvoir juridique de procéder à des interceptions sans restriction. Le groupe de Trevi prend contact avec un certain nombre d'Etats en Europe et à l'international : la Suède, la Finlande, la Norvège, les USA, le Canada, l'Australie, la Nouvelle-Zélande et Hongkong. En juin 1993, un questionnaire, relatif aux différentes législations concernant les interceptions de télécommunication, est transmis aux Etats-membres de l'Union européenne. Un texte de coopération policière est préparé et destiné à étendre la convention européenne d'entraide judiciaire en matière pénale,

[432] Déclaration de Glyn Ford, membre britannique du comité des libertés civiles et des affaires intérieures du Parlement européen

[433] Le groupe de Trevi réunissait les ministres de l'intérieur des douze pays de la Communauté européenne, coopération destinée à lutter contre le terrorisme

[434] Dont l'interception en « temps réel » de plusieurs séries de communications se tenant entre deux pays ou plus

adoptée par le Conseil de l'Europe en 1959 « Mais la convention de 1959 n'est nullement restreinte aux « crimes majeurs » dont parlent les ministres » faisait remarquer Tony Bunyan, chercheur à l'association britannique Statewatch. « Les nouvelles dispositions s'appliqueront donc à toutes les infractions, même mineures ! ». Ces dispositions conviennent surtout aux services de renseignement. La liste des pays impliqués dans les discussions internationales évoquent[435]le réseau Echelon : « Même si le projet euro-américain diffère, dans sa nature, policière et non militaire, ainsi que dans ses objectifs, du réseau Echelon[436], les spécifications formulées représentent, pour les libertés civiles et pour le droit à la vie privée, un danger potentiellement aussi important… Les normes euro-américaines deviendront globales ». Dans le même temps, la cryptologie se libéralise. La question de la démocratie est posée : « Les citoyens doivent toujours essayer de contrôler l'Etat, y compris lorsqu'il s'agit pour celui-ci d'intercepter les communications. Quand le gouvernement est digne de confiance, une bonne loi de régulation devrait suffire. Mais, si la loi autorise les écoutes dans des situations qui ne relèvent ni de la sécurité de l'Etat ni de la lutte contre la criminalité, ou si l'on s'aperçoit qu'il y a des écoutes illégales, les citoyens seront enclins à chercher à se protéger individuellement. La seule réponse est une démocratie bien vivante qui réussisse à instaurer une loi stricte et respectueuse des libertés individuelles »[437].

Une rencontre de 1993 entre plusieurs Etats de l'Union européenne et les USA au quartier général du FBI à Quantico fut dénommée « Séminaire sur l'application du droit international des télécommunications »[438]En octobre 1994, le Congrès des USA adopte un projet de loi inspiré par le FBI qui expose « les exigences nécessaires pour les utilisateurs internationaux[439] » pour procéder à des interceptions de télécommunications. L'Union européenne réagit à ce texte et adopte le document le17 janvier 1995, sans consulter le Parlement européen, sous la forme de la « procédure écrite »[440]. Cette initiative de l'Union européenne n'a été rendue publique qu'en novembre 1996 quand un Memorandum of Understanding fut soumis à la signature des pays hors USA et Union européenne. Les adresses auxquelles les signatures parvenaient étaient soit le Conseil de l'Union européenne à Bruxelles, soit le FBI aux USA, ce qui explique la dénomination : « le système UE-FBI de surveillance des télécommunications.

En septembre 1998, le groupe de travail sur la Coopération policière au sein de l'Union européenne a débattu, puis, dans un deuxième temps approuvé des Requirements ayant pour finalité de couvrir les communications satellites et Internet. Les résultats furent connus sous l'appellation d'ENFOPOL 98 et assez largement médiatisés, ce qui obligea les autorités à retarder la mise en vigueur de cette initiative jusqu'en 2001. Lors du Conseil de l'Union européenne du mois de mai 2001 consacré à la Justice et aux Affaires intérieures, les ministres approuvent un rapport qui explique clairement les conséquences des Requirements au sein de l'Union européenne. Cela aboutit à la mise en place d'ENFOPOL 29 de 2001 qui a en fait incorporé le contenu d'ENFOPOL 98 de 1998. ENFOPOL 29 instaure les mesures

[435] Cf : Australie, Nouvelle-Zélande, Canada
[436] Selon Tony Bunyan
[437] Bert-Jaap Koops, chercheur à l'université de Tilburg, auteur de « The Crypto Controversy. A Key Conflict in the Information Society », Kluwer Law International, La Haye, 1999
[438] ILETS
[439] IURs ou Requirements
[440] Le document, au lieu d'être formellement adopté par le Conseil des ministres a simplement été mis en circulation et approuvé.

encadrant les interceptions ; il doit obtenir un ordre spécifique autorisant l'écoute sur un sujet précis.

Les agents de la Commission en charge de la protection des données étaient conscients des exigences des agences de sécurité, formulées notamment lors de forums internationaux comme dans le sous-groupe du G8 consacré au crime High-Tech afin que les données soient automatiquement conservées et qu'elles soient susceptibles d'être consultées pendant des mois, voire des années. Les demandes présentées par les agences de sécurité de l'Union européenne sont explicitées dans un rapport envoyé par le NICS[441] au Ministère de l'Intérieur en août 1999 et détaillent les mesures envisagées, y compris un éventuel site d'archivage de données. Les fonctionnaires de la Commission en charge de la protection des données s'opposent aux demandes des agences de sécurité de l'Union européenne ; ils sont soutenus par le groupe de travail de l'Union européenne sur la protection des données et par la Commission européenne. La proposition[442] de la Commission européenne sur le traitement des données personnelles et « la protection de la vie privée dans le secteur des communications électroniques »[443] met à jour le droit communautaire. La proposition prend en compte la directive de 1997 sur la protection des données personnelles dans le secteur des télécommunications et la directive cadre d'Octobre 1995. Elle a été soumise au Parlement européen au cours de l'été 2000, puisqu'elle devait selon le principe de codécision, obtenir l'accord non seulement du Conseil et de la Commission, mais aussi du Parlement. Les rapporteurs parlementaires ignoraient jusqu'en avril 2001 que le Conseil souhaitait non seulement adopter ENFOPOL 98/ actuellement ENFOPOL 29 mais discutait aussi d'un ensemble de projets de « Conclusions » appelant la Commission à amender la proposition et les directives de l'Union européenne[444] existantes afin de satisfaire aux exigences des agences de sécurité de l'Union européenne. Par ailleurs, il était convenu d'adopter un projet de « position commune » sur cette proposition avant que cette dernière ne passe en première lecture devant le Parlement européen[445]. Le changement proposé par le Conseil et initié par la Commission est important : il confère aux gouvernements de l'Union européenne et à leurs agences de sécurité tous les pouvoirs dont ils ont besoin pour adopter des lois de mémorisation des données au niveau national ; le dixième alinéa autorise « la conservation des échanges de données et de localisation des données pour une période limitée. Le 7 juin 2001 le Président du Groupe de travail sur la protection des données avait fait connaître son point de vue aux trois institutions européennes, faisant valoir notamment : « une conservation systématique et préventive des communications ou de tout autre moyen de transfert de données des citoyens de l'Union européenne minerait les droits fondamentaux à la vie privée, à la protection des données, à la liberté d'expression, à la liberté et à la présomption d'innocence. La société de l'information pourrait-elle encore se réclamer société démocratique en de telles circonstances ? ». Le 11 juillet 2001, le Comité des droits et libertés des citoyens a adopté son rapport sur ladite proposition par 22 voix contre 12[446]. Ce rapport proposait que l'alinéa 10 fût modifié afin de limiter la conservation de données à des cas individuels spécifiques et mentionnait : « la surveillance électronique à grande

[441] Service britannique du renseignement criminel

[442] Qui devait aboutir à directive du 12 juillet 2002 sur la protection des données personnelles dans le secteur des communications électroniques

[443] COM (2000) 385 final, 12 juillet 2000

[444] Celles de 1995 et 1997

[445] Sous la dénomination « lignes de conduite », elles ont été adoptées au Conseil sur les Télécommunications » le 27 juin 2001

[446] La majorité des eurodéputés socialistes6PSE- votent contre

échelle, exploratoire ou générale, est prohibée ». La directive du 12 juillet 2002 permet de conserver certaines données pendant une durée limitée. Le débat n'est pas clos pour autant. Un projet de décision-cadre[447] sur les données de connexion résulte de l'initiative de la France, du Royaume-Uni, de l'Irlande, de la Suède, sans aboutir à un consensus ; les points les plus litigieux sont relatifs à la nature des données conservées, données déjà détenues par les fournisseurs de service, ou conservation de l'ensemble des données et au délai de conservation des données, relativement courte (trois mois) ou assez longue (quatre ans). Le projet de décision-cadre est rejetée en juin 2005 par le Parlement européen. Il a été vivement critiqué par le groupement 29 qui rassemble les autorités de régulation des divers Etats de l'Union européenne en matière de protection des données personnelles. Après le vote négatif du Parlement, la question qui se pose est la suivante : les idées portées par le projet de décision-cadre doivent-elles être abandonnées ou trouver leur place dans une autre norme ? Le Conseil européen, négligeant le vote du Parlement, continue à travailler sur le projet de décision-cadre. Le 12 octobre 2005, le Conseil des ministres décide de maintenir le projet : les données de connexion dépendent du « troisième pilier » de l'Union européenne. De son côté, la Commission estime que le dossier relève de sa compétence. Le refus du Parlement n'a pas beaucoup d'importance, puisque, dans le cas d'un projet de décision présenté par les Etats, le Parlement n'a qu'un rôle consultatif. Un projet de directive est présenté le 21 septembre 2005. Le projet pose trois questions :

- Le nombre des éléments à conserver : il englobe les données de localisation, les sites web consultés, les adresses IP des personnes contactées par messagerie instantanée, les adresses électroniques des correspondants d'un abonné.
- La durée de conservation : la convention sur la cybercriminalité avait retenu trois mois ; la durée peut être de douze mois ou de trente-six mois.
- Le coût de conservation : selon le rapport de la Commission des Libertés civiles du Parlement européen, la mise en place serait de 175 millions d'euros pour les fournisseurs d'accès et les opérateurs de communications électroniques.

La décision-cadre doit enfin prendre en compte les critiques émises par les associations de défense des droits de l'homme. Il s'agit de répondre aux craintes émises par le G29 et par les ONG pour lesquels il doit exister une distance infranchissable entre les enquêtes dirigées contre des criminels et la surveillance massive à titre préventif de tous les citoyens. En fait, la décision-cadre retient une durée de conservation d'un an, ce qui semble excessif aux associations de défense de droits de l'homme.

L'entraide judiciaire concerne notamment les TIC et les communications électroniques. Dans son champ d'application, la convention prévoit le recours à la vidéoconférence et à la téléconférence. Le titre III est afférent aux interceptions de télécommunications. Il s'agit de combattre la délinquance et la criminalité sur le territoire de l'Union européenne. Cet objectif ne peut être disjoint du contexte international de lutte contre la criminalité et le terrorisme. Dans la plupart des Etats occidentaux, sont adoptés des textes qui limitent les libertés individuelles et autorisent le recours aux technologies de l'information pour empêcher la commission de crimes et de délits.

Un débat s'est instauré à ce sujet. La grande majorité des juristes est favorable à un équilibre entre la sécurité et les libertés individuelles. Cela correspond en particulier

[447] Cf : Claudine Guerrier « Les interceptions de télécommunications, les données de connexion et l'Europe », Communication et commerce électronique, décembre 2005, p 4

aux valeurs exprimées dans la Charte des droits fondamentaux et aux principes qui régissent le Conseil de l'Europe et la Convention de sauvegarde des droits de l'homme. L'entraide européenne correspond au volet sécuritaire et tous les Etats de l'Union européenne sont membres du Conseil de l'Europe. De plus, le rapport de forces géo-politique est favorable au courant sécuritaire.
Si une téléconférence est organisée entre deux Etats membres de l'Union européenne, il faut obtenir le consentement préalable des personnes physiques concernées ; la téléconférence permet l'audition de témoins ou experts originaires de plusieurs Etats de l'Union européenne. Les deux catégories visées par l'article onze de la loi de 2005 ont des significations différentes. Le témoin a assisté à l'infraction ou a connaissance de renseignements permettant de parvenir à la vérité. L'expert est entendu pour faire état de ses connaissances dans un domaine particulier, ayant directement un rapport avec l'affaire considérée. La téléconférence peut être utilisée dans une affaire afférente à des personnes provenant de plusieurs Etats de l'Union européenne. Cela permet des gains de temps appréciables et une amélioration de la procédure, plus souple, plus rigoureuse. La vidéoconférence, quant à elle, est introduite dans l'arsenal juridique français par l'article dix de la loi de 2005. Elle est utilisée quand la comparution est inopportune ou impossible. Lors d'une vidéoconférence, sont entendus, comme lors d'une téléconférence, les témoins et les experts. Une comparution est inopportune si la comparution d'un témoin dans un certain lieu géographique favorise des pressions qui risquent de fausser le témoignage. Elle sera impossible si le témoin ou l'expert ne peut pas se déplacer. L'autorité judiciaire de l'Etat requis est présente : elle se fait représenter lors de la vidéoconférence, ce qui signifie que l'Etat concerné donne son accord à la procédure. L'autorité judiciaire est garante de l'identification de la personne entendue. Elle reconnaît que le témoin ou l'expert sont ce qu'ils prétendent être. L'autorité judiciaire est garante des principes fondamentaux de son droit interne. En effet, il ne peut y avoir de vidéoconférence s'il n'existe pas de prise en compte des principes fondamentaux du droit interne de l'Etat concerné. La personne auditionnée peut invoquer le droit de ne pas témoigner, reconnu soit par le droit de l'Etat requérant, soit par celui de l'Etat requis. Vidéoconférence et téléconférence sont deux instruments privilégiés de l'entraide judiciaire européenne.
Les interceptions de télécommunications jouent aussi un rôle essentiel, au niveau national, dans les procédures judiciaires. Le domaine des interceptions de télécommunications semblait relever des prérogatives des Etats nations. Deux résolutions sont cependant intervenues dans la dernière décennie du vingtième siècle. La première résolution du Conseil de janvier 1995 indique qu'un équilibre doit être trouvé entre l'intérêt de l'Etat et le respect de la vie privée, du secret de la correspondance, de la protection des données personnelles. La résolution du 3 mai 1999 englobe, sur le plan technique, non seulement la téléphonie mais aussi Internet. Les interceptions impliquent une qualité dans l'exécution et une précision dans les modalités. La recherche de la qualité dans l'exécution des interceptions légales se définit par l'accessibilité, la connaissance des données, la sécurité. La précision dans les modalités de mise en œuvre est le corollaire de l'interception légale. Les interceptions sont réalisées dans la discrétion, les missions dévolues à chaque personne concourant à l'interception sont définies. La dimension économique apparaît en filigrane dans le droit de l'Union européenne, surtout dans la résolution de 1999. Les opérateurs et les fournisseurs sont des acteurs privilégiés de l'interception. L'internet est mis en exergue dans la problématique financière. La résolution de 1999 demande aux personnalités habilitées de parvenir à une coordination « dans le but de mettre en pratique, vis-à-vis des opérateurs de réseaux/fournisseurs de service, les

spécifications afférentes aux interceptions ». Elle complète la résolution antérieure, celle de 1995. Elle englobe l'ensemble des technologies[448], est ouverte sur le futur, prévoit de nouvelles atteintes à la sécurité par des technologies qui ne sont pas opérationnelles. Elle reflète les incertitudes qui pèsent sur le droit des interceptions au sein de l'Union européenne. Elle convie les ministres à coopérer. La collaboration en matière d'expérimentations juridiques et techniques est destinée à combler un vide possible. Le groupe « coopération policière » est un aiguillon dans l'application des deux résolutions. Ainsi l'étude des deux résolutions (celle de 1995 et celle de 1999) permet-elle de dégager trois conclusions : le principe de subsidiarité est menacé d'obsolescence par les nouvelles technologies ; la coopération au sein de l'Union européenne est institutionnalisée ; la protection de la vie privée semble reculer devant la prééminence de l'ordre public. Un nouveau jalon apparaît avec le protocole à la convention sur l'entraide judiciaire dans le secteur des interceptions de télécommunications.

1)L'interception de télécommunication avec assistance technique d'un Etat de l'Union européenne : dans certains cas, les demandes d'interceptions de télécommunications impliquent une assistance technique d'un Etat de l'Union européenne. C'est l'autorité compétente d'un Etat membre qui introduit la demande d'interceptions. L'autorité compétente est soit une autorité judiciaire pour les interceptions judiciaires, soit une autorité administrative pour les interceptions de sécurité. La demande d'interceptions induit des indications obligatoires : la confirmation de l'émission d'un ordre ou d'un mandat d'interception sans laquelle l'interception ne pourrait avoir lieu ; les informations qui permettent d'identifier la cible de l'interception, nécessaires pour l'autorité compétente de l'Etat requis ; les précisions sur le comportement délictueux faisant l'objet de l'enquête. Des précisions complémentaires sont exigées : la durée souhaitée pour l'interception ; les données techniques suffisantes, en particulier le numéro pertinent de connexion au réseau. L'autorité compétente de l'Etat membre requérant adresse à l'autorité compétente de l'Etat membre requis une demande en vue d'une interception de télécommunications et d'une transmission immédiate à l'Etat membre requérant ou en vue d'une interception de l'enregistrement et de la transmission ultérieure à l'Etat membre requérant[449].

Des demandes peuvent également être présentées, en ce qui concerne l'utilisation de moyens de télécommunications par la cible de l'interception, si celle-ci se trouve dans l'Etat requérant, lorsque celui-ci a besoin de l'aide de l'Etat requis, dans l'Etat requis, lorsque les communications de la cible peuvent être interceptées dans cet Etat, dans un Etat membre tiers, lorsque l'Etat membre requérant a besoin de l'aide technique de l'Etat membre requis.

Il arrive de plus en plus fréquemment que l'interception de communications électroniques se fasse via un satellite, grâce à l'aide d'un fournisseur de services. Les systèmes de services de télécommunications qui concourent à une interception légale de télécommunications d'une cible présente dans un autre Etat membre que l'Etat requérant et qui ne sont pas directement accessibles sur le territoire de l'Etat requis, sont rendus directement accessibles par l'intermédiaire d'un fournisseur de services présent sur son territoire.

Les autorités compétentes d'un Etat membre peuvent, pour les besoins d'une enquête judiciaire, en se conformant à la législation nationale applicable et si la cible de l'interception[450] est présente dans cet Etat membre, procéder à l'interception par l'intermédiaire d'un fournisseur de services présent sur son territoire, procéder à l'interception via un fournisseur de services sans faire intervenir l'Etat membre sur le territoire duquel se

[448] Téléphonie fixe et mobile, internet

[449] Les Etats membres requérants ont davantage recours à la première qu'à la deuxième solution.

[450] La personne interceptée

trouve la station terrestre une demande d'interception légale de télécommunications, en particulier lorsqu'il n'existe pas d'intermédiaire dans l'Etat membre requérant.

2)L'interception de télécommunications sans l'assistance technique d'un autre Etat membre :

Dans ce cas, les termes changent : il n'est plus question d'Etat requérant et d'Etat requis, mais d'Etat membre interceptant, pour désigner l'Etat où se trouve l'adresse de la cible visée dans l'ordre d'interception. Cela traduit la différence des rôles qui incombent aux Etats membres concernés puisque l'Etat membre notifié n'apporte pas d'assistance technique à l'Etat membre interceptant.

L'Etat membre interceptant et l'Etat membre notifié ont des obligations l'un envers l'autre :

L'Etat membre interceptant a une obligation d'information vis-à-vis de l'Etat membre notifié.

L'Etat membre interceptant informe l'Etat membre notifié de l'interception avant l'interception si l'Etat membre interceptant sait déjà, au moment de procéder à l'interception, que la cible se trouve sur le territoire de l'Etat membre notifié.

L'Etat membre interceptant informe l'Etat membre notifié de l'interception, s'il ignore où se trouve la cible de l'interception, dès qu'il s'aperçoit que la cible de l'interception se trouve sur le territoire de l'Etat membre notifié.

Les informations de l'Etat interceptant sont notamment[451] les suivantes :

- L'indication de l'autorité compétente qui ordonne l'interception
- La confirmation de l'ordre d'interception régulier émis dans le cadre de l'enquête judiciaire
- Les informations relatives à l'identification de la cible de l'interception
- L'indication de l'infraction faisant l'objet de l'enquête
- La durée probable de l'interception

L'Etat membre interceptant et l'Etat membre notifié ont d'autres obligations l'un envers l'autre :

L'Etat membre notifié a un devoir de réponse vis-à-vis de l'Etat membre interceptant.

Dès qu'elle a reçu les informations nécessaires, l'autorité compétente de l'Etat membre notifié répond « sans délai », c'est-à-dire au maximum dans les quatre-vingt-seize heures et donne des indications à l'Etat membre interceptant.

L'Etat membre notifié peut permettre l'exécution de l'interception sans réserves ou donner son consentement sous réserves de conditions à respecter dans une affaire nationale similaire.

L'Etat membre notifié peut refuser l'exécution de l'interception ou exiger l'interruption de l'interception si l'interception est incompatible avec le droit national. Dans cette hypothèse, l'organisme de contrôle national peut être amené à intervenir. La décision est obligatoirement communiquée par écrit.

L'Etat membre notifié peut exiger que les données interceptées ne puissent pas être utilisées ou soient utilisées sous conditions spécifiques. L'Etat membre notifié fait connaître à l'Etat membre interceptant les motifs qui justifient les conditions.

L'Etat membre notifié peut demander, en accord avec l'Etat membre interceptant que le délai initial de quatre-vingt-seize heures soit prolongé d'une période qui ne peut dépasser un butoir de huit jours. L'Etat membre notifié fait alors connaître à l'Etat membre interceptant les raisons pour lesquelles le butoir est prolongé.

Tant que l'Etat notifié n'a pas pris de décision, l'Etat membre interceptant peut poursuivre l'interception ; en revanche, il n'est pas autorisé à utiliser les données interceptées, sauf s'il en a été convenu autrement entre les Etats membres concernés ou pour prendre des mesures urgentes afin de prévenir un danger immédiat et sérieux pour la sécurité publique. L'Etat membre notifié est alors prévenu de l'utilisation des données et des motifs qui la justifient.

[451] La liste n'est pas exhaustive

Ainsi, la coopération concilie-t-elle la prise en compte des droits internes. Un équilibre a été trouvé en la matière.
Les autres points relatifs à la coopération sont traités dans le cadre des relations entre l'Etat membre interceptant et l'Etat membre notifié.
L'Etat membre notifié peut demander un résumé des faits et des informations complémentaires
qui sont indispensables pour décider si l'interception serait autorisée dans une affaire nationale similaire.
Les Etats membres concernés prennent les mesures pour que le délai imparti[452]soit respecté et qu'une décision soit arrêtée. Les Etats membres désignent des points de contact qui fonctionnent vingt-quatre heures sur vingt-quatre.
Lorsque l'Etat membre interceptant considère que les informations à fournir sont sensibles, il peut les transmettre à l'autorité compétente par le biais d'une autorité spécifique.
Les coûts exposés par les exploitants des installations de télécommunications constituent toujours un point d'achoppement en matière d'interceptions. Les frais exposés par les exploitants d'installations de télécommunications ou les fournisseurs de services sont à la charge de l'Etat membre requérant ou interceptant. Cette solution est logique puisqu'elle satisfait les besoins du demandeur.
La loi de 2005 est-elle trop sécuritaire ou correspond-elle à l'équilibre souhaité entre sécurité et libertés individuelles ?
Téléconférence et vidéoconférence ne posent pas problème, sont de simples supports qui facilitent et assouplissent les procédures. La réponse est plus difficile pour les interceptions de télécommunications. Les procédures d'entraide ne sont pas liberticides en elles-mêmes, mais elles peuvent favoriser des dérives, d'autant qu'aucune procédure de contrôle n'est prévue.
Avec la loi du 30 mars 2005 et la loi du 19 mai 2005 portant ratification de la convention sur la cybercriminalité, la France, tant pour le Conseil de l'Europe que pour l'Union européenne, s'est arrimée à des procédures d'entraide pénale qui concernent aussi les technologies de l'information et de la communication.

DEUXIEME PARTIE / ETUDE CROISEE

Plusieurs questions seront envisagées : organismes de contrôle et interceptions judiciaires/interceptions de sécurité ; organismes de contrôle/ Motifs d'interceptions, Interceptions techniques. Cela nous amène à revenir sur certains concepts déjà envisagés, mais dans une optique différente.

PREMIERE SOUS-PARTIE : ORGANISMES DE CONTROLE ET INTERCEPTIONS JUDICIAIRES/INTERCEPTIONS DE SECURITE

A) Pays où cohabitent les interceptions judiciaires et les interceptions de sécurité : ces systèmes impliquent non seulement une procédure d'autorisation préalable mais aussi un contrôle

1) L'Allemagne[453] : le texte de base est, au sein de la RFA, la loi du 13 août 1968 limitant le secret de la correspondance, des envois postaux et de télécommunications, dite « loi G10 », entrée en vigueur le 1er novembre 1968. Les interceptions judiciaires sont ordonnées par le juge d'instruction. En cas d'urgence, le Procureur a la possibilité de décider la mesure, qui doit être confirmée par un juge dans les trois jours.

[452] Les quatre-vingt-seize heures
[453] La réunification est récente. Les lois actuelles sont un héritage de la RFA

Les interceptions de sécurité sont délivrées par des personnalités incarnant le pouvoir exécutif ; l'autorité suprême dans le Land quand la demande émane d'un service chargé au niveau de chacun des Länder de la protection de la Constitution ou des ministres de l'Intérieur et du ministre de la Justice dans les autres cas.

Une commission de contrôle, composée de membres du Bundestag élus dispose de compétences décisionnelles : aucune mesure administrative de surveillance des correspondances ne peut être réalisée sans son autorisation préalable. Néanmoins, dans les cas relevant de l'urgence, l'interception est mise en œuvre à la demande du ministre fédéral de la défense ou de l'Intérieur. Ensuite, elle est soumise sans délai à la commission de contrôle et les décisions négatives de sa part induisent l'interruption immédiate de la mesure d'interception de sécurité.

La loi entrée en vigueur en janvier 2002[454] permet aux services de renseignement et à la police d'accéder aux données de télécommunications stockées sur support numérique : informations sur les services utilisés par les clients, accès aux renseignements relatifs aux échanges de méls, accès à toutes les données permettant de localiser les personnes à l'origine des communications ou des courriers électroniques, accès aux données des entreprises de télécommunications ou de communications électroniques.

Par contre, la commission de contrôle est toujours composée de membres du Bundestag. Deux autres spécificités apparaissent : premièrement, un contrôle est constitué par l'obligation faite au ministre fédéral compétent d'informer toute personne qui a fait l'objet d'une mesure d'interception individuelle. La commission G10 a pourtant la possibilité de dispenser le gouvernement de cette notification ou d'accorder qu'il soit sursis à cette démarche si cette notification est de nature à remettre en cause l'objectif poursuivi par la mesure. Deuxièmement, une autre spécificité réside dans la possibilité pour tout citoyen estimant que ses droits fondamentaux ont été violés de saisir la Cour constitutionnelle allemande.

La dichotomie interceptions judiciaires/interceptions de sécurité demeure mais l'organisme de contrôle garantit moins la protection de la vie privée

2) L'Italie :

Le juge d'instruction et le Procureur de la République du lieu où l'infraction a été commise sont habilités pour délivrer une autorisation d'interception judiciaire. Un registre récapitulant les autorisations dans l'ordre chronologique de leur adoption est tenu par le Procureur de la République[455].

Le ministre de l'Intérieur est compétent pour autoriser les interceptions de sécurité. Le Haut Commissariat de lutte contre la mafia peut également demander des interceptions à titre préventif.

En juin 2008, Sylvio Berlusconi a annoncé son intention de limiter les interceptions de télécommunications aux enquêtes sur le terrorisme et au crime organisé.

Il n'y a quasiment pas de contrôle des interceptions légales, comme cela a été relevé par la CEDH.

3) L'Espagne :

Les interceptions judiciaires ont pour fondement l'article 55 de la constitution. (suspension des garanties et des droits). L'interception implique l'autorisation judiciaire. Elle doit être effectuée de telle manière qu'elle n'affecte pas les contenus des communications. Dès que les personnes habilitées ont pris connaissance du

[454] En 2001, la loi G10 a été amendée. Cet amendement imposait des limitations à la protection des communications. Le champ d'application de la G10 s'est considérablement élargi, au détriment des garanties consenties en matière de droits fondamentaux.

[455] Article 226ter du Code de procédure pénale

contenu des interceptions, les supports sont détruits. Ils ne peuvent pas être distribués ou stockés.

Les interceptions de sécurité :

Elles mettent l'accent sur la lutte anti-terroriste Selon l'article un, paragraphe un de la loi « anti-terroriste »[456], les interceptions administratives ont pour but, en surveillant certaines communications, de prévenir ou de réprimer les activités délictueuses de bandes armées ou d'éléments terroristes. La durée maximale de la première opération de surveillance est fixée à trois mois[457].et peut être renouvelée de trois mois en trois mois. La loi anti-terroriste espagnole prévoit un contrôle mi-judiciaire, mi-administratif. Le résultat de la surveillance doit être communiqué régulièrement au juge, qui a le pouvoir de rapporter la décision à tout moment au vu des productions. L'article sept de la loi stipule que le gouvernement tient informé le congrès des Députés et du Sénat au moins tous les trois mois, voire plus tôt si les groupes parlementaires en font la demande, de l'utilisation qui a été faite des mesures prévues par cette loi et des résultats ainsi obtenus.

4) Les USA :

Les fondements légaux afférents aux interceptions de communications sont deux textes fédéraux. Le premier est le titre III du « Omnibus crime control and safe street act » adopté en 1968[458]. Le second est le Foreign Intelligence Surveillance Act » de 1978.

Le Title III Act est relatif aux dispositions législatives concernant les interceptions au niveau fédéral et au niveau des Etats en ce qui concerne les enquêtes judiciaires ; le FISA Act établit les dispositions juridiques fédérales afférentes aux interceptions réalisées dans l'objectif d'assurer la protection de la sûreté des USA et concernant les opérations d'espionnage et de contre-espionnage diligentées par les services de renseignement américains.

Avec le « Patriot Act », adopté par la quasi-totalité des élus américains du Congrès, les autorités fédérales, depuis 2001 et jusqu'en 2006[459], bénéficient d'une plus grande latitude dans la surveillance des communications électroniques et dans l'étude, l'exploitation des informations ainsi récoltées. Dans ce dispositif figure l'utilisation par les enquêteurs des moyens techniques développés pour le programme Carnivore. Ce système de surveillance[460] mis en place par les USA a d'ailleurs donné lieu à une enquête de la Commission européenne. Les fournisseurs d'accès ont dû rendre leur matériel compatible avec les systèmes de surveillance. AOL, Earthlink, Home, les plus importants des fournisseurs d'accès américains ont recherché dans leurs réseaux des communications qui aurait pu participer aux attentats du 11 septembre 2001. En bref, le « Patriot Act » est le fondement de la surveillance généralisée de l'internet.

Les USA ont opté pour un double système de contrôle. La première garantie réside dans le mode de traitement dévolu aux informations recueillies dans la mise en œuvre du « FISA Act ». En effet, les informations obtenues en cette occurrence constituent, aux USA, un mode légal de preuve susceptible d'être invoqué dans un procès pénal ; la personne mise en cause et son avocat doivent en être informés au préalable afin que les droits de la défense soient respectés. Néanmoins, le principal élément de contrôle implique que la personne mise en cause est en droit de saisir le tribunal fédéral de première instance territorialement compétent afin d'invoquer éventuellement

[456] Article 5.1 de la loi anti-terroriste de 1980
[457] Article 5.1 de la loi anti-terroriste de 1980
[458] Il est connu sous la dénomination Title III Act
[459] Nous avons vu antérieurement qu'une grande partie des mesures avaient été reconduites
[460] Qui concerne notamment l'activité des personnes perçues comme suspectes sur Internet

l'irrecevabilité des preuves recueillies par ces moyens. Ce recours juridictionnel est ouvert afin qu'il soit possible de démontrer que les preuves n'ont pas été rassemblées de manière licite et que les mesures de surveillance étaient contraires à la loi. Le système juridique applicable aux USA est le seul à prévoir la réalisation de rapports dans le domaine des interceptions judiciaires. En effet, dans le cadre du « Tile III Act » et tous les cinq jours pendant la période d'interception, le procureur doit présenter un rapport au magistrat qui a rendu la décision de façon à ce que le dit magistrat puisse déterminer la poursuite ou la cessation des interceptions. Trente jours après que l'autorisation de justice a été accordée, le « Title III Act » a prévu que le juge fasse un rapport sur la mesure d'interception qu'il a ordonnée à l'Administration des tribunaux fédéraux[461]. De plus, l'Attorney General a la responsabilité de réaliser un rapport à cette même administration fédérale[462]. L'Administration des tribunaux fédéraux rend à son tour un rapport annuel relatif à l'ensemble des interceptions réalisées au niveau fédéral comme au niveau des Etats fédérés.

D'autre part, l'Attorney general doit informer les commissions parlementaires permanentes du renseignement , ainsi que la Justice. Dans chaque cas, la justice a l'obligation d'être informée du nom du « Federal officer » chargé d'exécuter la surveillance électronique, de l'étendue de sa mission, de son objectif, de la cible visée, des circonstances qui la justifient et des procédures instaurées.

L'Attorney general fait un rapport annuel « to the administrative office of the US Court » et au Congrès sur le nombre de surveillances effectuées. Le rapport mentionne notamment le nombre total de demandes nouvelles, de renouvellements, de mesures refusées. Chaque semestre, l'Attorney general informe aussi les commissions spéciales du Congrès sur les activités de surveillance. Les commissions parlementaires du renseignement[463] sont en mesure de solliciter tous les éclaircissements, toutes les explications qui lui paraissent indispensables. Depuis le Patriot Act, les contrôles sont moins nombreux. La priorité est donnée au maintien de l'ordre public et à la lutte contre le terrorisme.

5) La Belgique :

   Pendant longtemps, on a classé la Belgique dans les pays où la seule source légale d'interception était judiciaire. Le juge d'instruction ou bien, en situation d'urgence, un magistrat du ministère public pouvaient autoriser une mesure d'interception. Les interceptions de sécurité n'étaient pas autorisées, mais le comité permanent de contrôle des services de renseignement avait recommandé que les services de renseignement puissent disposer d'un outil légal dans le domaine

   Ces interceptions sont devenues des interceptions de sécurité. La loi de 2007 est afférente aux méthodes de recherche pour les services de renseignement : un Collège doit être chargé du contrôle a posteriori. Dans ce Collège, sont représentés un magistrat, le Comité R, la Commission de la vie privée. Un rapport annuel est transmis au Sénat, qui assure le suivi des activités du Comité R. Une commission de surveillance est placée sous l'autorité des ministres de la Justice et de la Défense et composée de trois magistrats.

6) La France : fait cohabiter interceptions judiciaires et interceptions de sécurité. Le texte de base est la loi du 10 juillet 1991[464] adoptée après la condamnation de la France par la CEDH. Cette loi a été modifiée à plusieurs reprises, notamment par la loi du 9 mars 2004, et la loi de lutte anti-terrorisme.

[461] The Administrative Office of the United States Court
[462] Le rapport concerne l'ensemble des interceptions qui ont été réalisées dans l'année
[463] Qui sont au nombre de deux
[464] Loi 91646

6.1) Les interceptions judiciaires :

a) Les interceptions au stade de l'instruction : sont autorisées, sur la base du quantum de la peine (deux ans) par le juge d'instruction[465], pour une durée de quatre mois renouvelable.

Le projet de loi précise que le juge d'instruction ne pourra recourir aux interceptions judiciaires que lorsque les nécessités de l'information l'exigent. De nombreux parlementaires constatent que cette formulation peut se prêter à de multiples interprétations. Il convient de prévoir des garde-fous, des précisions sur les « nécessités de l'information »[466]. Un texte est finalement adopté sous la forme suivante :

-les autres moyens d'investigation ne permettent pas de cerner la vérité

-les écoutes ne constituent pas un artifice déloyal ni une violation des droits de la défense

La décision d'interception est écrite. Elle n'a pas de caractère général et n'est susceptible d'aucun recours ;

Devant le Sénat, d'autres amendements sont proposés lors de la séance du 25 juin 1991[467].

Ces amendements paraissent dangereux au gouvernement. Le juge d'instruction, pour être efficace doit disposer d'une large marge d'appréciation. L'exécutif s'oppose à la contestation de la légalité des interceptions de télécommunications. Il fait valoir que les cas de nullité de procédure sont déjà trop fréquents dans le cadre de la procédure pénale. Le juge risquerait d'être contraint de fournir une preuve quasi impossible à apporter ; des délinquants chevronnés, bien conseillés par leurs avocats, s'ils contestaient la légalité de l'interception, pourraient parfois obtenir gain de cause. Un contrôle des nécessités de l'information, constituerait en fait une remise en cause des instruments de travail du juge d'instruction et sèmerait le doute sur la pertinence de ses appréciations.

A la fin de la première décennie du 21ème siècle, les juges ont systématiquement recours aux interceptions quand le quantum de la peine le permet. Il nous reste à connaître la réforme des juges d'instruction en 2009.

b) Les enquêtes préliminaires : les interceptions sont possibles, dans quinze cas, demandées par le procureur de la République et accordées par le juge des libertés et de

---

[465] Aucune intervention du Procureur de la République n'est admise à ce stade

[466] A l'Assemblée nationale, des amendements sont discutés lors de la deuxième séance du 3 juin 1991 :

- Amendement n° 34, présenté par Jacques Toubon et François Massot. L'article 100 du code de procédure pénale sera ainsi rédigé : « Les dispositions de l'alinéa précédent ne peuvent être mises en œuvre que si : l'interception de la communication présente un intérêt pour la manifestation de la vérité ; les autres moyens d'investigation sont inopérants ou insuffisant ; elles ne constituent pas un artifice déloyal », JOAN, 2ème séance du 13 juin 1991, p 3145, 1ère colonne

- Amendement n° 56, présenté par françois d'Aubert et Paul-Louis Tenaillon. Insérer les alinéas suivants « L'interception ne peut être mise en place que si : l'interception de communication à distance présente un intérêt pour la manifestation de la vérité ; les autres moyens d'investigation sont inopérants ou insuffisants ; elle ne constitue pas un artifice déloyal ni une violation des droits de la défense », JOAN, 2ème séance du 13 juin 1991, p 3145, 1ère colonne

[467] Amendement n° 23 présenté par M.Thyraud : « La décision d'interception est écrite. Elle est notifiée au procureur général qui a seul qualité pour saisir à tout moment, s'il le juge utile, la chambre d'accusation. Celle-ci statue sur l'intérêt de maintenir ou non l'interception. L'inculpé n'est pas appelé aux débats », JO Sénat, séance du 23 juin 1991, p 2075, 1ère colonne

Amendement n°36, présenté par M.Dreyfus-Schmidt et les membres du groupe socialiste et apparentés : « La décision d'interception est écrite. Elle est transmise au procureur de la République par le juge d'instruction dans un délai de 24 heures, qui dispose de 48 heures pour en contester le bien-fondé, au regard des dispositions des alinéas précédents devant le président de la chambre d'accusation, JO Sénat, séance du 23 juin 1991, p 2075, 1ère colonne

la détention. Ces mandats sont accordés libéralement par le juge des libertés et de la détention.

6.2) Les interceptions de sécurité : la France se met en conformité avec la jurisprudence de la CEDH. Elle ne veut pas encourir le risque d'une condamnation et organise un système qui s'inspire de la pratique antérieure, celle du GIC, celle de Michel Debré, tout en prenant en compte les propositions du rapport Schmelck et les commentaires subséquents aux arrêts Klass et Malone. Les dispositions en matière d'interceptions administratives ont fait l'objet d'un examen attentif par la commission des lois. Les interceptions de sécurité sont, encore plus que les interceptions judiciaires, une exception au principe d'inviolabilité des correspondances. Devant l'Assemblée nationale, le débat est philosophique. Le concept même d'interception de sécurité est accueilli avec réserve. Le gouvernement légifère parce qu'il ne peut faire autrement. Il ne doit pas faire preuve d'une excessive timidité, sous prétexte d'ordre public[468]

7) Autres pays :

7.1) Les Pays-Bas : les interceptions sont judiciaires et de sécurité.

En matière d'interceptions de sécurité, l'initiative revient au chef du service de renseignement intérieur[469] qui propose une demande dûment motivée aux quatre ministres compétents. La décision est arrêtée conjointement par le Premier ministre, le ministre de la Justice, le ministre de l'Intérieur, le ministre des transports et des travaux publics.

Le contrôle est parlementaire : le ministre de l'intérieur, qui est responsable du « Binnenlandse VeiligsDienst »est tenu d'expliquer au parlement sa politique en la matière. Il répond aux questions parlementaires sauf si les informations sont confidentielles. Lorsque les informations sont confidentielles, elles sont débattues avec la commission parlementaire pour les services de renseignement et de sécurité, constituée des quatre principaux groupes politique de la seconde chambre[470]. Ses membres ont une obligation de secret.

7.2) Le Grand Duché du Luxembourg : permet le recours aux interceptions judiciaires et aux interceptions de sécurité.

La loi du 26 novembre 1982, portant introduction au code d'instruction criminelle des articles 88.1 à 88.4, modifiée par la loi du 7 juillet 1989, prévoit la possibilité pour le juge d'instruction ou le président de la Chambre d'accusation d'ordonner des mesures d'interceptions de télécommunications. L'article 88.3 stipule que les pouvoirs publics peuvent recourir aux interceptions de sécurité. L'autorité habilitée à ordonner la mesure est le président du gouvernement, avec l'assentiment d'une commission, composée du président de la Cour supérieure de justice[471], du président du comité du contentieux du Conseil d'Etat et du Président de la Chambre des comptes. En cas d'urgence, le président

---

[468] Jacques Toubon : « Si nous voulons véritablement, dans ce domaine des écoutes, sauvegarder un élément essentiel de notre liberté, nous devons adopter une loi qui soit crédible aux yeux de l'opinion publique et efficace aux yeux de ceux qui les ordonnent et qui les exécutent. Elle doit également être crédible et efficace aux yeux de la communauté internationale qui nous a déjà jugés dans ce domaine et qui nous jugera peut-être encore à l'avenir », JOAN, 1ère séance du 13 juin 1991, 2ème colonne.

[469] Le BVD, « Binnenlandse Veiligheidsdienst »

[470] Les Etats généraux sont constitués de la première chambre, ou chambre haute, c'est-à-dire le Sénat, élu au suffrage indirect, et la deuxième chambre, ou chambre des députés, élus au suffrage universel direct. La deuxième chambre a un pouvoir beaucoup plus étendu que la chambre haute

[471] La Cour supérieure de justice comprend un président, deux conseillers à la Cour de cassation, neuf Présidents de Chambre à la Cour d'appel, dix premiers conseillers, dix conseillers à la Cour d'appel ; elle est compétente pour les affaires dont la Cour d'appel ou la Cour supérieure de justice ont à s'occuper en assemblée générale, les accusations admises contre les membres du gouvernement, les règlements de conflits d'attribution, les actions disciplinaires contre les magistrats, les accusations portées par la Chambre des députés contre les membres de la Commission des Communautés européennes

du gouvernement peut faire procéder immédiatement à la surveillance ; il saisit sans délai la commission qui décide si la surveillance doit ou non être maintenue.
La question s'est posée de savoir si l'article treize de la Convention européenne de sauvegarde des droits de l'homme, afférent au droit à l'octroi d'un recours effectif devant une instance nationale était compatible avec le droit luxembourgeois. Le système de recours luxembourgeois a été examiné par la Commission de la CEDH dans l'affaire Mersch et autres[472]. Selon le système allemand analysé dans l'Arrêt Klass et autres, l'obligation d'une notification a posteriori s'impose si la notification est susceptible de s'effectuer sans compromettre la finalité de la surveillance. L'affaire Mersch et autres se caractérise par l'absence totale de notification. Cependant, la Commission a estimé que le droit de s'adresser au Conseil d'Etat luxembourgeois, tenu d'effectuer une enquête, et les autres garanties, le droit d'intenter une action en responsabilité civile et le contrôle a priori de l'opportunité de la surveillance, étaient de nature à satisfaire aux exigences de l'article 13.

7.3) L'Australie :

Le « Telecommunication (Interception) Act australien établit une distinction entre les interceptions judiciaires, qui sont effectuées par les autorités de police et les interceptions administratives, qui sont réalisées sous la houlette du directeur général des services secrets australiens[473].
Les interceptions judiciaires sont susceptibles d'être demandées au niveau fédéral par la police fédérale australienne, qui a à sa disposition une structure spécialisée pour mettre à exécution une demande d'interception[474]. Ces interceptions peuvent également être demandées par les services de police des différents Etats ou dans l'Etat des Nouvelles-Galles du Sud par la « Commission contre le crime » ou la « Commission indépendante de lutte contre la corruption »
Les demandes d'interception de sécurité émanent du directeur des services secrets qui transmet les demandes sus-mentionnées au ministre de la justice. En 1979, les demandes étaient écrites et devaient comporter tous les éléments nécessaires à l'appréciation du ministre de la justice ou de son délégué : nom, adresse, motifs de la demande, faits à l'appui de ce motif. L'autorisation donnée pouvait être restrictive et ne valoir que pour certains moments de la journée ou de la nuit. Sa durée ne pouvait dépasser six mois, mais pouvait être révoquée à n'importe quel moment par le décisionnaire, le ministre de la justice.
Le contrôle est assuré par l'Omdusman, porte sur les conditions d'enregistrement, de transcription, de conservation et de destruction des interceptions. L'Ombdusman vérifie s'il y a eu autorisation en bonne et due forme prévue dans le « Telecommunication (Interception) Act de 1979, revu en 1991. Par ailleurs, l'Ombdusman établit un rapport destiné à l'exécutif de l'Etat dont dépend la structure concernée. Il a accès à tous les documents indispensables à son contrôle. De plus, les différents services qui demandent une interception de télécommunications, ont également l'obligation de fournir un rapport après chaque mesure d'interception..
Des lois ont été votées contre le terrorisme, qui apportent des modifications à la « Telecommunication (Interception) Act »..
Certains articles de la loi sur les télécommunications et des lois anti-terroristes, votées sous le gouvernement du conservateur John Howard menacent la confidentialité des sources journalistiques.

[472] Décision du 10 mai 1985 sur les requêtes n° 10439/83, n° 10440/83, n° 10441/83, n° 10452/83, n° 10512/83 ? DR 43
[473] Australian Secret Intelligence Organization
[474] The Telecommunication Interception Division

B) Les pays pratiquant les interceptions judiciaires :

1) La Suisse : en principe, les interceptions sont exclusivement judiciaires. En réalité, comme en Belgique, on peut établir une distinction entre deux formes d'interceptions. D'une façon générale, la décision de mise sous surveillance est secrète. Elle est décidée par le Procureur général de la Confédération. Ce secret perdure à la fin de la mesure. Cette dernière est soumise dans les 24 heures qui suivent son adoption à l'autorité de contrôle compétente et l'autorité de contrôle varie. S'il s'agit d'une interception judiciaire, l'autorité de contrôle compétente est la chambre d'accusation fédérale pour le procureur général de la Confédération. S'il s'agit d'une interception qui a un rapport avec l'armée ou la police, l'autorité de contrôle compétente est soit le président du tribunal militaire de Cassation pour l'auditeur en chef de l'armée, soit l'autorité judiciaire unique désignée par le droit cantonal pour le directeur cantonal de la police. L'autorité de contrôle doit se prononcer dans un délai de cinq jours. Elle peut annuler la décision si elle constate qu'il y a eu violation du droit fédéral, y compris excès ou abus de pouvoir d'appréciation.

Sur le sujet, la jurisprudence de la CEDH[475] a renforcé la position de la confédération helvétique, déclarant irrecevable la requête de M.Spillmann. sur la base de l'article treize de la Convention européenne de sauvegarde des droits de l'homme[476] : en matière d'écoutes téléphoniques, l'ensemble de moyens juridiques dont dispose le justiciable sur le plan fédéral, et en particulier la pratique appliquée dans ce domaine à la dénonciation au Département fédéral de justice et police, satisfont à l'exigence d'un recours effectif.

Le requérant a fait valoir qu'il n'existe, en Suisse, aucun recours effectif susceptible de remédier à la situation litigieuse. En particulier, la procédure de dénonciation[477] préconisée par le Gouvernement ne répondrait pas aux exigences de l'article 13 de la convention.

Dans ses observations, le Gouvernement relève de manière générale qu'en Suisse le particulier dispose, en matière de contrôle des interceptions téléphoniques, d'un ensemble de recours qui, examinés globalement, répondent aux exigences de l'article 13. Il s'agit du contrôle qui émane de l'instance judiciaire, à savoir le président de la chambre d'accusation du tribunal fédéral, de l'intervention de l'autorité administrative, à savoir le Ministère public fédéral, doublé des recours administratifs devant le Département fédéral de justice et police et devant le Conseil fédéral[478], instances administratives qui exercent des compétences juridictionnelles dans ce cadre.

Le Gouvernement s'est référé à la fameuse procédure de dénonciation et procède à une analyse : les dénonciations fondées sur l'article 71 PA sont traitées comme des recours formels au sens des articles 44 et suivants de ladite loi. En conséquence, selon le gouvernement suisse, l'intéressé jouit de tous les droits reconnus aux parties et bénéficie d'un droit à une décision formelle du Département fédéral de justice et police, qui est elle-même sujette à un recours auprès du Conseil fédéral.

M.Spillmann a fait valoir que les autorités auraient dû l'informer sur le point de savoir s'il avait été ou non l'objet d'interceptions téléphoniques. Par ailleurs, il considère que le Département fédéral de justice et police ne saurait en aucun cas être reconnu comme un organisme de recours indépendant dans la mesure où le Département fédéral de justice et police est le supérieur hiérarchique du Procureur général fédéral.

La Commission rappelle que, conformément à sa jurisprudence constante, l'article treize de la Convention européenne de sauvegarde des droits de l'homme vise l'octroi d'un recours contre une allégation de violation d'un des droits et libertés proclamés dans les

[475] CEDH, 8 mars 1988, Spillmann c/Suisse
[476] Droit à l'octroi d'un recours effectif devant une instance nationale
[477] Aufsichtsbeschwerde
[478] C'est-à-dire devant l'autorité gouvernementale helvétique

autres articles de la convention. Elle fait remarquer que dans l'affaire Klass[479], elle a estimé que si la notification devait aller à l'encontre de l'objectif des ingérences nécessaires à la sécurité nationale et justifiées par la convention[480] européenne de sauvegarde des droits de l'homme, une interprétation de l'article treize ayant pour effet de créer un droit d'être informé ne serait pas en harmonie avec le système de la convention[481]. Cette argumentation a été reprise par la Cour dans l'affaire Spillmann. La Commission fait valoir que le système de recours en matière d'interceptions téléphoniques pose des problèmes particuliers par rapport à l'article 13 de la Convention européenne de sauvegarde des droits de l'homme si une notification, même a posteriori, de la mesure prise serait susceptible d'aller à l'encontre de l'objectif même de cette mesure. En conséquence, ainsi que la CEDH l'a déclaré dans l'affaire Klass[482], un recours effectif selon l'article treize, dans la situation particulière de la surveillance secrète, doit s'entendre d'un recours aussi effectif qu'il peut l'être eu égard à sa portée limitée, inhérente à tout système de surveillance.

Dans l'arrêt Silver et autres[483] qui a permis un examen conjoint des articles 13 et 8, la CEDH a rappelé un certain nombre de principes, en particulier celui-ci : « le jeu de l'article treize dans un cas donné dépend de la manière dont l'Etat contractant intéressé a choisi de s'acquitter de l'obligation assumée par lui en vertu de l'article un : reconnaître directement à quiconque relève de sa juridiction les droits et libertés du titre premier »

La Commission examine les différentes voies de recours dont le requérant, M.Spillmann dispose en droit suisse afin de déterminer si elles sont effectives dans ce sens étroit. Il existe un contrôle a priori et, à un moindre degré, a posteriori.

Il existe un contrôle a priori de l'opportunité de l'interception, de la surveillance, puisque l'autorité qui ordonne la mesure d'interceptions est tenue de demander, dans un délai de vingt-quatre heures, l'approbation de la personne habilitée.

La Commission remarque aussi qu'un contrôle a posteriori paraît dans une certaine mesure possible.

Il est exact que M.Spillmann n'a pas été informé par les autorités sur le point de savoir s'il a fait l'objet ou non d'une mesure d'interceptions. En fait, c'est dans le cadre d'un échange de lettres entre l'intéressé et le Ministère public fédéral et à la lumière de la réponse écrite donnée par ce dernier que s'est posée, en l'occurrence, la question de la mise en œuvre d'un contrôle a posteriori.

Dans une lettre du 4 juin 1984, cette autorité, répondant à la demande de renseignements formulée par le requérant au sujet d'interceptions qui auraient pu être ordonnées à son encontre, a indiqué : « soit aucune mesure de surveillance n'avait eu lieu, soit la mesure de surveillance se prolongeait encore, soit la mesure de surveillance avait pris fin et n'avait pas ou pas encore été communiquée en raison du danger qu'une telle communication faisait courir au regard du but de la mesure ». Après la mainlevée de la mesure, dans l'hypothèse où celle-ci a été ordonnée, le requérant est informé sauf si une telle information risque de compromettre le but et l'objet de la mesure en question.

Quand l'ordre public, l'intérêt public justifient le maintien du secret, en particulier lorsque la sûreté intérieure et extérieure de la Confédération est en jeu, le Ministère public fédéral doit obtenir l'approbation du président de la chambre d'accusation du Tribunal fédéral pour être dispensé de l'obligation d'informer d'office l'intéressé de la mesure d'interceptions de télécommunications.

---

[479] Ante : première partie

[480] Article huit alinéa deux

[481] Cf : rapport de la Commission du 9 mars 1977, Série B 26,§71

[482] Arrêt du 6 septembre 1978, Série A 28, § 68

[483] Arrêt du 25 mars 1983, Série A 61, p 42,§ 111-113

Enfin, lorsque la procédure de dénonciation est mise en œuvre devant le Département fédéral de justice et police pour mettre en cause le refus du Ministère public fédéral de donner des informations sur les motifs, les modalités et la durée d'une mesure d'interceptions, cette instance traite, selon une pratique récente, les dénonciations qui lui sont adressées en application de l'article 71 PA en tant que recours au sens des articles 44 et suivants de ladite loi.

L'intéressé jouit par conséquent de tous les droits reconnus aux parties et bénéficie notamment d'un droit à une décision formelle. La dénonciation donne donc lieu à des vérifications auprès du président de la chambre d'accusation du Tribunal fédéral. Sur la base des informations obtenues, le Département fédéral de justice et police procède à une appréciation de la justification de la mesure d'interceptions et celle de l'éventuelle renonciation à une notification a posteriori à l'intéressé. De plus, cette autorité prend une décision formelle contre laquelle il est possible d'introduire un recours devant le Conseil fédéral, dernière instance nationale.

La Commission de la CEDH a considéré que dans le cas d'espèce la procédure décrite a trouvé une bonne application, dans la mesure où M.Spillmann a pu faire usage des voies de droit qui étaient à sa disposition à l'exception toutefois du recours au Conseil fédéral. La Commission de la CEDH a estimé que l'ensemble des recours prévus par le droit suisse répond, compte tenu du domaine particulier de la surveillance par interceptions et des circonstances spécifiques de l'affaire, aux exigences de l'article 13 de la CEDH.

Depuis lors, la Suisse est considérée comme présentant suffisamment de possibilités de recours et de garanties en matière d'interceptions de télécommunications.

2) La Suède : à l'origine, la législation suédoise prévoyait, outre les dispositions préventives en matière pénale[484], des dispositions particulières comme, notamment, la loi 1974/203 sur le traitement pénitentiaire en établissement, permettant d'intercepter les communications d'un détenu, si la sécurité l'exige. La loi 1989/529, sur le contrôle des étrangers, permettait au tribunal d'accorder une autorisation d'interception, pour déterminer si un étranger, ou l'organisation à laquelle il appartient, projetait une action illégale.

Le 18 juin 2008, le Parlement suédois a adopté à une courte majorité[485]une loi qui autorise un organisme civil, chapeauté par le ministère de la défense, à mettre en place des interceptions de communications électroniques. La finalité est bien entendu la sécurité du pays. La loi entre en application le premier janvier 2009. Elle dote l'Agence d'écoutes miliaires suédoise, un organisme civil qui se cantonnait jusqu'alors aux écoutes radio, du pouvoir d'intercepter les méls et les communications téléphoniques entrant et sortant du pays. Techniquement, pour être mis en place, ce système doit s'appliquer à l'ensemble des communications entrant et sortant du pays. C'est dans un second temps que l'Agence d'écoutes militaires distingue les communications extérieures. Cette agence n'est pas soumise à une autorisation judiciaire ou de police pour débuter sa surveillance. Aucun contrôle n'est exercé sur la façon dont les interceptions sont réalisées.

L'opposition à l'adoption de cette loi n'est pas insignifiante. La classe politique est partagée sur ce sujet. Une manifestation a été organisée devant le Parlement pour faire retirer le projet de loin, en vain. Un site de protestations a été installé, sans rien obtenir. Pour le gouvernement, le besoin était pressant dans la mesure où la plupart des communications électroniques sont de plus en plus fréquemment transmises par des câbles de fibre optique.

[484] Chapitre 27, section 16 du code de procédure pénale

[485] 143 voix pour, 138 contre,une abstention

La justification juridique repose sur les mécanismes de contrôle, deux commissions qui sont chargées de procéder à la surveillance des interceptions[486]. Il convient d'attendre le fonctionnement de ces organismes pour mesurer l'efficacité du contrôle. Selon Anders Eriksson[487] « Les gens ont le sentiment que c'est une intrusion dans leurs droits et leur liberté. Ils sont favorables à l'utilisation d'un tel procédé pour protéger la sécurité nationale mais cette loi va trop loin. » Tout va dépendre du fonctionnement des organismes de contrôle dont le contour n'est pas entièrement précisé.

C) Des interceptions administratives : le Royaume-Uni est le seul Etat où l'utilisation des interceptions est arrêtée par l'autorité administrative. Le juge n'est pas habilité à ordonner des interceptions et ceci quel que soit le motif invoqué. Les interceptions de sécurité se font sous la responsabilité du Ministre de l'Intérieur[488] qui délivre les autorisations d'après les directives du « Joint intelligence Commitee »[489]. Une dérogation est cependant possible en cas d'urgence, sans remettre en question le principe de la compétence exclusive de l'autorité administrative : sous réserve de l'accord téléphonique exprès du ministre, un autre ministre ou un haut fonctionnaire peuvent ordonner une interception de sécurité. L'autorisation est signée par le ministre de l'Intérieur dans les 48 heures.

Un double contrôle est mis en place. Le premier est constitué par le Commissioner. Ce dernier, commissaire indépendant, magistrat de haut rang nommé par le Premier ministre pour un mandat de trois ans renouvelable assure un contrôle interne du système en vérifiant sur place et auprès des services concernés[490] les conditions d'application des dispositions légales. Tous les acteurs qui participent à l'exécution des interceptions sont tenus de faciliter son action en lui transmettant les documents et informations nécessaires aux investigations. Le Commissioner est amené à réaliser des rapports. Il convient d'établir une distinction entre deux types de rapports. Dans le premier cas, si le Commissioner constate des manquements à la loi, il rédige un rapport dans toutes les circonstances où cela lui semble indispensable et fait parvenir le document au Premier ministre[491]. L'autre type de rapport est le rapport général annuel constitué à partir des conclusions qu'il a tirées de la confrontation entre la théorie et la pratique, entre la loi et son application. Ce rapport est communiqué à la Chambre des communes et à la Chambre des Lords mais le Premier ministre peut refuser la publication de certains passages du rapport destiné au Parlement s'il considère que les paragraphes incriminés sont susceptibles de porter atteinte à la sécurité nationale, à la prévention de la criminalité ou à la sauvegarde du potentiel économique du Royaume-Uni.

Le second niveau de contrôle correspond à un tribunal indépendant[492] composé de cinq membres, dotés d'un mandat de cinq ans renouvelable, nommés par la Reine et tous issus de la majorité parlementaire. Les membres de ce tribunal ont une expérience juridique d'au moins dix ans. Quant aux pouvoirs du tribunal, ils ne sont pas exhaustifs. Le tribunal est saisi par les personnes qui pensent être l'objet de mesures d'interceptions. Dans l'enquête qu'il mène à bien, il est assisté par le Commissioner, qui, dans le cadre de ses missions, a pu rassembler des informations qui s'avèrent

[486] Amendements de dernière minute avant l'adoption
[487] Ancien responsable des services secrets suédois et actuel responsable de l'autorité de régulation en matière de protection des données personnelles
[488] Secretary of state
[489] JIC
[490] En particulier, les services de renseignement
[491] Le rapport comporte deux parties, l'une publique et l'autre secrète
[492] Interception of Communication tribunal

utiles au tribunal. A l'issue de l'enquête, le tribunal dispose de larges compétences. S'il conclut qu'il y a eu violation de la loi, il fait connaître cette conclusion au requérant[493] et rend compte au Premier ministre des résultats de son enquête. De plus, il peut décider par voie d'ordonnance de l'annulation de l'autorisation ministérielle, de la destruction des procès-verbaux et des bandes contenant les informations illégalement interceptées. Le tribunal est également susceptible de fixer une indemnité constituant les dommages et intérêts dus en réparation du préjudice subi ou bien il engage le ministre compétent à verser au demandeur le montant de l'indemnité évaluée par le tribunal.

Le commissioner a fait remarquer dans l'un de ses rapports qu'en plus de l'intégrité des services participant à l'interception des correspondances, la mesure de protection primordiale contre les éventuels abus de l'institution serait le concours joint des services de police, des douanes et des services de renseignements en qualité de demandeurs et du ministre en qualité de service administratif accordant l'autorisation, et enfin des services exécutifs.

Une publicité importante a été consentie en faveur de ces recours, à l'instigation de la CEDH qui souhaitait[494]que des garanties soient consenties par le Royaume-Uni en matière d'interceptions. Néanmoins, si les rapports communiqués au Parlement ont permis de se forger une appréciation sur la politique d'interceptions en Grande-Bretagne, les recours individuels n'ont pratiquement jamais abouti. Le bilan est donc contrasté pour cette institution de contrôle à deux têtes et le Rip Act, d'une façon générale, les dispositions législatives de lutte contre le terrorisme n'ont pas facilité l'action du « Commissioner » et du tribunal indépendant. On ne peut parler de véritable progrès dans ce secteur et les requérants individuels n'ont pas obtenu satisfaction depuis la mise en place, en 1985, de la loi sur les interceptions de télécommunications. Ainsi, le bilan est-il contrasté pour ce qui concerne le Royaume-Uni.

DEUXIEME SOUS-PARTIE : LES MOTIFS DES INTERCEPTIONS DE TELECOMMUNICATIONS ET LES INTERCEPTIONS TECHNIQUES

Il est important d'examiner les motifs d'interceptions de télécommunications. Cela a des

conséquences sur le système juridique envisagé puisque l'interception repose sur le motif ou sur le quantum de la peine. Surtout, les organismes de contrôle ont vocation à vérifier la conformité des motifs

I) Les motifs :

A) Les motifs qui intéressent les interceptions judiciaires et les interceptions de sécurité

1) L'Allemagne :

La loi votée le 13 août 1968 prévoit que les interceptions sont possibles si la personne ciblée a commis des crimes graves comme l'assassinat, l'homicide volontaire, des délits au regard de la sécurité de l'Etat, la haute trahison, l'atteinte à la sûreté extérieure de l'Etat, l'espionnage, les activités d'agents secrets, l'association de malfaiteurs. La prise en compte des formes récentes de l'insécurité en Europe a conduit à l'élargissement des motifs justifiant le recours au « contrôle stratégique », c'est-à-dire à la surveillance exercée sur certaines liaisons entre l'Allemagne et l'étranger, destinée à réunir des informations non individualisées pour prévenir des menaces. La nature de ces menaces est prévue par le paragraphe 3 de l'article un de la loi du 13 août 1968 : agression armée,

[493] Ce qui est, surtout au 21ème siècle, rarissime

[494] Cf : Arrêt Malone, voir antérieurement

attentats terroristes sur le territoire allemand, trafic international de matériel de guerre ou de moyen de destruction massive bactériologique, chimique ou nucléaire, trafic de stupéfiants, blanchiment d'argent, faux monnayage. La surveillance ne doit pas permettre de retenir des éléments contre des personnes identifiées. Afin qu'une mesure d'interception stratégique soit autorisée, il faut que le ministre compétent délimite géographiquement au préalable une zone de risque dans un acte, qui, pour être valide, requiert l'approbation de contrôle parlementaire[495] composée de neuf députés du Bundestag.

Le Conseil constitutionnel fédéral dans un arrêt du 14 juillet 1999 a déclaré que des dispositions portant sur les diverses formes de contrôle stratégiques insérées dans la loi G10 en 1994 étaient en grande partie incompatibles avec la Constitution, sans pour autant déclarer d'une façon générale que ce type de surveillance était illicite.

En 2008, le gouvernement allemand a fait voter une loi renforçant nettement les pouvoirs de la police fédérale dans la lutte anti-terroriste, en l'autorisant notamment à installer des caméras au domicile de suspects ou à surveiller leurs ordinateurs. La loi élargit nettement les prérogatives de la police fédérale, en lui permettant d'intervenir, sans autorisation de la police des Länder, dans la vie privée en cas de menace. En matière d'interceptions, les personnalités religieuses sont susceptibles d'être écoutées, captées, alors qu'elles étaient auparavant protégées.

2) L'Italie : le code de procédure pénal est fort exhaustif : il autorise les interceptions pour le trafic d'armes, la contrebande, mais aussi pour les injures, les menaces, molestations ou troubles à la personne par le biais du téléphone. C'était vrai du moins jusqu'en 2008. Cela explique pourquoi l'Italie est le pays européen qui pratique le plus largement les interceptions et pourquoi tant d'affaires relatives aux interceptions de communications téléphoniques ont été médiatisées. Il faut attendre la mise en place de la nouvelle loi pour déterminer si la liste des motifs a diminué de façon importante. En principe, les motifs d'interceptions sont réduits au crime organisé et au terrorisme.
3) L'Espagne :

   Les motifs invoqués à l'appui d'interceptions de communications électroniques peuvent avoir deux fondements.

   Le premier correspond aux alinéas un et deux de l'article 55 de la Constitution selon lesquels le secret des communications peut être suspendu lorsque l'état d'exception ou de siège est proclamé en vertu d'une loi organique réprimant l'activité des bandes armées ou de mouvements terroristes. Par ailleurs, la loi anti-terroriste espagnole du premier décembre 1980 réserve la surveillance des communications à la prévention ou à la répression des activités délictueuses de bandes armées ou d'éléments terroristes. Ces activités comprennent les délits contre la vie et l'intégrité physique, les détentions illégales de personnes physiques sous menace de rançon, la possession ou la détention d'armes, munitions et explosifs, l'atteinte à la sûreté extérieure de l'Etat et d'une façon générale les délits qualifiés de terroristes par le code pénal espagnol.
4) Les USA :

   4.1) Le « Title III Act » (correspondant aux interceptions judiciaires) autorise les interceptions de télécommunications effectuées lors des enquêtes criminelles, quand il s'agit d'infractions graves, c'est-à-dire des crimes, meurtres, kidnappings, affaires de drogues ainsi que toutes les actions « qui attentent à la vie, à l'intégrité physique ou à la propriété, et qui sont punissables d'une peine d'emprisonnement d'au moins un an ». Au niveau des Etats, les motifs peuvent varier. Ainsi, au New-Jersey, les motifs pouvant justifier une demande d'interception sont les suivants : les kidnappings, les meurtres, les

[495] PKG

trafics d'argent, la corruption, les paris illégaux d'argent, les coups et blessures volontaires, les menaces terroristes, les incendies volontaires, le vol organisé, les trafics de stupéfiants, les trafics d'armes, les évasions, la fabrique de faux, le crime organisé.

4.2) Les interceptions effectuées en vertu du FISA Act :

Le FISA Act concerne la surveillance des télécommunications effectuées dans le secteur des activités de renseignements d'une puissance étrangère, celles qui sont nécessaires à la protection de la sécurité de l'Etat pour les motifs suivants : attaques contre le pays, effectives ou avérées, actes de sabotage, terrorisme international, activités subversives au profit des services de renseignements d'une puissance étrangère . Ces formulations peuvent paraître floues. Par « terrorisme international », on peut entendre tous les actes de violence et les agissements qui mettent en péril la vie humaine, et constituent une violation des lois pénales américaines ou étrangères ; le lieu de l'attentat peut se situer sur le territoire des USA ou à l'étranger.

Sont également comprises dans le concept de « terrorisme international » toutes les activités menées avec l'intention d'intimider ou de contraindre un gouvernement ou la population civile ou d'influencer l'action d'un gouvernement, par l'homicide volontaire, l'enlèvement ou le détournement. Ces dispositions s'appliquent, même quand ces actions ont lieu hors du territoire des USA, mais ont un caractère international.

Les interceptions de télécommunications restent aux USA un sujet sensible. Le 18 juillet 1996, le Congrès adopte une loi anti-terroriste, qui, à l'époque, est perçue comme particulièrement rigoureuse. Au lendemain de l'attentat commis pendant les Jeux Olympiques d'Atlanta, le 27 juillet 1996, le président des USA, alors Bill Clinton demande des mesures supplémentaires relatives à la lutte contre le terrorisme ; parmi les mesures envisagées, il demande le renforcement des interceptions de télécommunications, ce qui était sollicité par le FBI depuis longtemps et que les associations de droits de l'homme considéraient comme attentatoire aux libertés individuelles

Avec le Patriot Act, le champ d'application devient encore plus large, et les garanties sont minimes.

5) Belgique : Les interceptions judiciaires sont limitées à un petit nombre de motifs : grande criminalité, terrorisme, grand banditisme, crime organisé.

   Les interceptions de sécurité sont afférentes à la sécurité nationale et des forces armées, dans le cadre du Service général du renseignement.

6) La France :

   6.1) Les interceptions judiciaires : au stade de l'instruction, la notion de motif n'est pas retenue. C'est le quantum de la peine[496] qui est retenu.

   En matière d'enquêtes préliminaires, introduites par la loi Perben 2[497], les motifs sont les suivants : meurtre commis en bande organisée, tortures et actes de barbarie commis en bande organisée, trafic de stupéfiants, enlèvement et séquestration commis en bande organisée, traite des êtres humains, proxénétisme, vol commis en bande organisée, extorsion[498], destruction, dégradation et détérioration d'un bien commis en bande organisée, faux monnayage, crimes et délits constituant des actes de terrorisme, délits en matière d'armes commis en bande organisée, aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée, délits de blanchiment ou de recel, association de malfaiteurs.

   6.2) Interceptions de sécurité : les motifs sont prévus dans la loi du 10 juillet 1991 :

[496] Deux ans
[497] Loi du 9 mars 2004
[498] Cf : articles 312-6 et 312-7

a) Sécurité nationale : la sécurité nationale est un concept traditionnel mais le terme n'apparaissait pas en tant que tel dans le droit français. La notion est empruntée à l'article huit de la Convention européenne de sauvegarde des droits de l'homme. Elle recouvre la Défense nationale, les autres atteintes à la sûreté et à l'autorité de l'Etat. Sur ce thème, si à l'Assemblée nationale, la question, en 1991 n'est abordée que par Jacques Toubon[499], les discussions au Sénat sont âpres.

Le droit de l'Union européenne définit presque tous les concepts, mais le droit français ne l'imite pas toujours, même s'il obéit aux règlements et s'il transpose les directives. Jacques Thyraud constate qu'il est déjà difficile de définir les notions de sûreté de l'Etat et de sécurité publique. Il ne souhaite pas que le concept de sécurité nationale soit introduit dans le corpus juridique français[500]. Le rapporteur, Marcel Rudloff, fait remarquer que le raisonnement de Jacques Thyraud est juste mais que la sécurité nationale trouve sa place dans un secteur qui n'est pas judiciaire[501]. Jacques Thyraud retire son amendement : il est sceptique. L'Etat ne peut rester désarmé devant des menaces ou des crimes. Les termes « sécurité nationale » sont peut-être flous : ce sera à la commission de contrôle de préciser le concept[502].M.Rudloff a indiqué que le concept ne devait rien au droit pénal ; néanmoins, dans l'ancien Code pénal, les articles 70 à 85 visent la trahison et l'espionnage ; les articles 86 à 92 les attentats, complots et autres infractions contre l'autorité de l'Etat et l'intégrité du territoire national ; les articles 93 à 96, les crimes tendant à troubler l'Etat par le massacre et la dévastation ; les articles 97 à 99, les crimes commis par la participation à un mouvement insurrectionnel ; les articles 100 à 103 regroupent des notions diverses[503]. Ces articles sont abrogés mais les incriminations se trouvent dans le livre IV de l'actuel Code pénal qui constituent les « atteintes aux intérêts fondamentaux de la nation ». Les atteintes aux intérêts fondamentaux de la nation succèdent à la sûreté de l'Etat, qui avait lui-même remplacé dans l'ordonnance du 4 juin 1960 la « sécurité intérieure et extérieure ».

Selon le douzième rapport de la CNCIS[504], la doctrine est d'avis qu'il y a bien « maintien de la fusion de la sûreté extérieure et de la sûreté intérieure en une notion unique, la sûreté de l'Etat, effectuée par l'ordonnance du 4 juin 1960, mais camouflée dans le nouveau code sous le couvert de la notion polymorphe des intérêts fondamentaux de la nation »[505]. Assez rapidement[506], la CNCIS a fait savoir que « la notion de sécurité nationale devait être comprise au vu des nouvelles dispositions du Code pénal qui fait figurer la sécurité parmi les intérêts fondamentaux de la nation, au même titre que l'intégrité du territoire, la forme républicaine des institutions ou les moyens de la défense. » Il ne suffit pas de se référer à la crainte générale d'un trouble à l'ordre public pour répondre aux exigences de motivation résultant de la loi. La CNCIS indique dans le

[499] Amendement repoussé lors de la 2ème séance du 13 juin 199&, JOAN, pp 3152 et 3153

[500] Amendement n° 27 présenté par Jacques Thyraud. Les mots « sécurité nationale » sont remplacés par les mots « sûreté de l'Etat », JO Sénat, séance du 25 juin 1991, 2080, 2ème colonne

[501] Marcel Rudloff : « S'agissant d'un concept nouveau qui sera mis en vigueur par une commission non-judiciaire, il n'est pas mauvais d'employer une autre expression que pour les poursuites pénales », JO Sénat, séance du 25 juin 1991, p 2081, 1ère colonne.

[502] Charles Lederman : « Il (l'Etat) ne doit pas être désarmé non plus devant des mises en cause de la sécurité nationale. Il paraît qu'il faut maintenant employer cette expression alors que, jusqu'à présent, même si elle figure dans certains textes européens, nous n'en avons pas encore la définition. Toutefois, puisqu'on laisse à la commission qui va être créée, si elle l'est effectivement, le soin de définir tous les concepts, en effet, il ne peut être question d'incrimination, nous verrons bien », JO Sénat, séance du 23 juin 1991, p 2081, &ère colonne

[503] Exemption de peine, non-dénonciation de crime

[504] La Documentation française, Rapport 2003, pp 53 à 58

[505] André Vitu, Jurisclasseur pénal, rubrique article 410.1 « atteintes aux intérêtss fondamentaux de la nation », paragraphe 57

[506] Rapport d'activité 1994, pp 17 et s

rapport d'activité 1994 que la crainte d'un trouble à l'ordre public n'autorise le recours à une interception qu'en cas de menace particulièrement grave à la sécurité. En outre, les interceptions de sécurité ne sauraient être utilisées comme moyen de pénétrer un milieu syndical ou politique et de pratiquer la surveillance d'opposants étrangers, si la sécurité de l'Etat français n'est pas en cause.

b)La prévention du terrorisme :

La prévention du terrorisme fait l'objet d'un consensus. Certains parlementaires souhaitent qu'elle entre dans la zone des incriminations et non pas dans celui de la prévention. Mais la France ayant été l'objet de multiples attentats, la nécessité d'empêcher les assassinats organisés pour des raisons politiques paraît impérative.

Tout au plus, certains défenseurs des droits de l'homme, étrangers au Parlement, font-ils remarquer que l'Etat, sous couvert de prévention du terrorisme, peut être amené à pratiquer des interceptions de sécurité concernant des intellectuels, partisans de causes pour lesquelles militent des adeptes de la violence et les journalistes dialoguant avec lesdits intellectuels. Le nouveau code pénal a introduit une incrimination spécifique du terrorisme[507] alors que celui-ci n'était prévu jusqu'ici qu'en matière procédurale.

c)La prévention de la criminalité et de la délinquance organisée, de la reconstitution ou du maintien de groupements dissous :

La prévention de la criminalité et de la délinquance organisée fait aussi partie des motifs légaux d'interceptions de sécurité. La prévention de la criminalité et de la délinquance englobe le trafic illicite de stupéfiants[508], le grand banditisme, le trafic d'armes, de munitions, de produits explosifs et de matières nucléaires, le faux monnayage, la grande délinquance financière, la traite des êtres humains et les vols d'objets d'art.

L'Assemblée nationale est divisée. Certains parlementaires font remarquer que tous les aspects mentionnés correspondent à des délits ou des crimes poursuivis par le code pénal. Pourquoi faire entrer dans l'ordre administratif ce qui relève de l'ordre judiciaire ?

Certes, l'article huit de la Convention européenne de sauvegarde des droits de l'homme reconnaît, dans la délimitation des motifs visés par les interceptions de sécurité, le trafic de stupéfiants et la lutte contre le proxénétisme. Or, la traite des êtres humains n'est pas synonyme de proxénétisme, même si la traite des êtres humains réduit des personnes à l'état d'esclaves, contraints d'effectuer des travaux de force, sans bénéficier d'aucun droit ou protection qui augmenterait, même légèrement, le coût de la main d'œuvre.

Quant au grand banditisme, au trafic d'armes, de munitions, de produits explosifs et de matières nucléaires, au faux monnayage, à la grande délinquance financière, aux vols d'œuvres et objets d'art, ils ne sont pas envisagés par l'article huit de la Convention européenne de sauvegarde des droits de l'homme. C'est ce qui justifie, pour les auteurs de la loi, le recours à la prévention. Cependant, dans la mesure où des incriminations existent, deux types d'interceptions peuvent se cumuler : les interceptions administratives (prévention) et les interceptions judiciaires lorsque l'infraction semble avoir été commise (nécessité de l'information).

La reconstitution ou le maintien de groupements dissous apparaît dans le projet. Le motif semble un peu obsolète. Il a un caractère politique, puisqu'il vise des mouvements d'extrême gauche ou d'extrême droite, ou des partisans de causes autonomistes, indépendantistes. Les ennemis de la liberté ont certes les droits qu'ils ne concéderaient pas aux autres, mais la société estime qu'elle doit défendre les institutions républicaines. La défense des libertés publiques au détriment de groupuscules menaçants paraît justifier ce

[507] Code pénal, articles L 421.1 à L.421.5

[508] Le trafic illicite de stupéfiants est présent dans d'autres législations, par exemple la législation norvégienne.

motif. C'est en tout cas l'avis de Charles Lederman, qui a en mémoire la Cagoule et autres milices de l'avant deuxième guerre mondiale[509].

d) La protection des éléments essentiels du potentiel scientifique et économique de la France : initialement dénommée « protection des intérêts économiques et scientifiques fondamentaux de la France ».

Ce motif appelle des remarques d'ordre général. Il semble induire une multiplication d'interceptions de sécurité utilisant plusieurs techniques de communications électroniques et concernant divers profils de personnes.

Le concept est novateur. L'intérêt public s'attachant au potentiel scientifique et économique de la France traduit-il un relent de dirigisme ? Certes pas. Cet intérêt existe dans tous les pays[510]. Ces derniers ont le devoir de lutter contre les nébuleuses qui ne correspondent à aucune des entités juridiques connues. Le concept peut paraître un peu flou[511]. La notion englobe des délits divers (incriminations pénales) et des pratiques légales.

Deux amendements sont proposés, l'un à l'Assemblée nationale, par Jean-Jacques Hyest[512], l'autre par le gouvernement[513]. L'un et l'autre s'inspirent du projet de réforme du code pénal qui introduit la notion « d'éléments essentiels de son potentiel scientifique et économique ». En fait, les travaux concernant le projet de loi sur les interceptions légales et sur le nouveau code pénal sont quasi concomitants. C'est ce qui explique les interférences et la communauté de formulation. Des discussions ont eu lieu sur l'opportunité de faire coïncider les textes de 1991 et le nouveau Code pénal.

Le livre IV du projet de réforme du code pénal a été déposé à l'Assemblée nationale. L'article 410.1 définit les intérêts fondamentaux de la nation qui englobent, entre autres, des « éléments essentiels du potentiel scientifique et économique ». L'ancien code pénal punissait déjà les intelligences avec des agents étrangers de nature à nuire aux intérêts économiques essentiels de la France[514].

Les deux amendements sont quasi identiques : seul, le mot « sauvegarde » présent dans l'amendement n°76 est absent de l'amendement 86. L'amendement 76 reprend tous les termes dans le nouveau code pénal. Il est adopté. La protection du potentiel scientifique et économique de la France concerne diverses techniques de communications électroniques : dans les domaines économiques et scientifiques ; le téléphone, s'il est encore utilisé, est complété par d'autres systèmes, par exemple, la télécopie, et, vecteur privilégié des échanges commerciaux, le mél. Au fur et à mesure de l'évolution des technologies de communications électroniques, d'autres catégories de transmission sont intéressées.

---

[509] Charles Lederman : « La notion de reconstitution ou de maintien de groupements dissous, en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées nous paraît compréhensible », JO Sénat, séance du 25 juin 1991, p 2080, &ère colonne

[510] Y compris les Etats les plus libéraux : USA, Royaume-Uni qui cherchent à préserver le patrimoine économique, scientifique de leurs entreprises et de leur administration

[511] François d'Aubert : « C'est une formule fourre-tout, presque un alibi et je ne sais pas très bien à quoi elle peut correspondre très précisément. Ainsi, hier, au cours de la visite du GIC, j'ai demandé en plaisantant à l'un de nos interlocuteurs si ce texte permettait une surveillance accrue des entreprises japonaises. Ne comprenant pas l'ironie, il m'a répondu … « Tout à fait », JOAN, 1ère séance du 13 juin 1991, p 3131, &ère colonne.

[512] Un amendement n° 76 est présenté par Jean-Jacques Hyest et les membres du groupe de l'Union du centre, ainsi rédigé : « Dans l'article 3, substituer aux mots « la protection des intérêts économiques et scientifiques fondamentaux de la France » les mots « la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », JOAN, 2ème séance du 13 juin 1991, p 3131, 1ère colonne

[513] Un amendement n° 86 est présenté par le gouvernement ainsi rédigé : « Dans l'article 3, substituer aux mots « des intérêts économiques et scientifiques fondamentaux de la France » les mots « des éléments essentiels du potentiel économique et scientifique de la France », JOAN, 2ème séance du 13 juin 1991, 2ème colonne

[514] Cf : article 80.3 du code pénal

Plusieurs profils de personnes sont visés : les hommes d'affaires, les possesseurs de comptes bancaires.

Les interceptions fiscales sont évoquées[515] lors.du débat devant l'Assemblée nationale. Le garde des Sceaux se veut rassurant : les interceptions de sécurité ne pourront pas intervenir à l'occasion d'enquêtes entreprises dans le domaine du contrôle fiscal, et, en matière douanière, elles seront limitées à la lutte contre le trafic de la drogue et le blanchiment de l'argent tiré de ce trafic.

Le secret bancaire[516] risque-t-il d'être mis à mal ? La quasi-totalité des virements inter-bancaires transite par un réseau qu'alimentent les ordinateurs des banques, et les ordres de bourse sont compensés à Paris par un système analogue. Ce phénomène relève de l'informatique plus que des communications électroniques, mais les liens entre informatique et communications électroniques sont si difficilement dissociables que la question se pose.

Certains dirigeants économiques et syndicaux peuvent être soupçonnés[517]. Le gouvernement considère que ces soupçons relèvent de la paranoïa. Un exécutif démocratique qui reconnaît la liberté d'entreprise, la liberté syndicale, ne se laisserait pas aller à des dérives qui feraient de personnalités économiques ou syndicales autant d'ennemis potentiels. D'ailleurs, l'organisme de contrôle veille à ce que les motifs ne soient pas détournés de l'esprit de la loi, qui respecte les principes généraux du droit et les libertés individuelles. Qu'entend-on par « sauvegarde des éléments essentiels du potentiel scientifique et économique de la nation » au sens du Code pénal ? Celle-ci fait partie des intérêts fondamentaux de la nation tels que définis par l'article 410.1 du Code pénal. Cet article permet d'aborder le titre premier du livre IV « Des crimes et délits contre la nation, l'Etat, et la paix publique ». Il ne définit d'ailleurs pas exactement la notion d'intérêts fondamentaux de la nation, se contentant d'en donner une énumération. Dans les intérêts fondamentaux de la nation, est retenue la sauvegarde des éléments essentiels de son potentiel scientifique et économique et aussi de « son patrimoine culturel ». Ce point a été ajouté par le Parlement contre l'avis du Gouvernement Selon André Vitu (cf : Jurisclasseur pénal), cette formulation « permet d'étendre la protection du Code pénal non seulement aux différents secteurs de l'économie au sens étroit du terme mais également à la recherche scientifique et aux innovations techniques ou technologiques sur lesquelles reposent précisément la force ou la compétitivité du pays ». A l'article 410 succèdent les articles 411 qui incriminent les différentes atteintes à ces intérêts. Parmi celles-ci sont plus spécifiquement intéressantes les infractions des articles 411-5 à 411-8 afférentes aux intelligences avec une puissance étrangères et à la livraison d'informations à celle-ci.

« Article 411.5 Le fait d'entretenir des intelligences avec une puissance étrangère, avec une entreprise ou organisation étrangère ou sous contrôle étranger ou avec leurs agents, lorsqu'il est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de dix ans d'emprisonnement et de 150000 euros d'amende.

Article 411.6 Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts

[515] Cf : François d'Aubert, Assemblée nationale, &ère séance du 13 juin 1991

[516] Sur le secret bancaire, « Le secret bancaire préserve les informations qui ont un caractère confidentiel, le contenu du bilan ou le mouvement du compte » (Paris, 17 octobre 1931, JCP, 1932, 119)

[517] Charles Lederman : « Une telle disposition peut conduire à mettre sous écoute téléphonique tous les ingénieurs de notre pays. J'ai même l'impression que tous les dirigeants d'entreprises porraient être suspectés d'intelligence avec l'ennemi et mis sous écoute. Ne verra-t-on pas, par exemple les dirigeants syndicaux de telle ou telle usine française être placés sur écoute téléphonique, au motif qu'il y aurait lieu de sauvegarde le potentiel économique de la France », JO Sénat, séance du 25 juin 1991, p 2081, 2ème colonne

fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225000 euros d'amende.

Article 411.7 Le fait de recueillir ou de rassembler, en vue de les livrer à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents, des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150000 euros d'amende

Article 411.8 Le fait d'exercer pour le compte d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger ou de leurs agents, une activité ayant pour but l'obtention ou la livraison de dispositifs, renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de dix ans d'emprisonnement et de 150000 euros d'amende.

Le procédé vise l'espionnage, y compris économique, comme le transfert illicite de technologie. Cette fourniture est le fait d'ingénieurs, d'agents de renseignement de pays tiers, d'officines spécialisées et est utilisée par des services de renseignement de pays tiers, à des entreprises, à des organisations étrangères.

Ainsi, selon le rapport d'activité de la CNCIS 2003, le transfert illicite d'un secret de fabrication à une personne étrangère établit la réunion de plusieurs éléments constitutifs des délits de l'article 411.7.

La sauvegarde des éléments essentiels du potentiel scientifique et économique de la nation suppose une suspicion d'atteinte à ce potentiel, une menace et que la cible dont on se propose d'intercepter les communications est impliquée dans la menace.

La CNCIS a pour finalité de contrôler la conformité des motifs a priori. Pour ce faire, la CNCIS a élaboré sa doctrine sur les critères d'appréciation en se fondant sur le respect des principes fondamentaux du droit et sur les principes appliqués par la CEDH :

- le principe de légalité : la demande d'interception doit ressortir, dans une interprétation stricte au profit des éventuels « interceptés », à l'un des motifs définis par la loi ;
- le principe de proportionnalité : l'atteinte à la vie privée est envisagée par comparaison avec le résultat escompté. Si ce dernier ne peut être certain, il ne sera pas fait recours aux interceptions de sécurité ;
- le principe de subsidiarité : le recours aux interceptions de sécurité ne s'effectue qu'en l'absence d'autres moyens d'investigation qui ne porteraient pas atteinte à la vie privée.

La loi de 1991 n'avait pas prévu[518] de dispositions relatives en cas d'urgence ; pourtant, les services des ministères concernés ont eu souvent l'impression, voire la certitude, d'être cernés par l'urgence. Dans la pratique, les demandes étaient accompagnées, quand une extrême diligence semble indispensable, d'une mention « en urgence » ou « en extrême urgence », en « urgence absolue ».

Le traitement en urgence ne semblait pas présenter de problème particulier : les agents d'exécution sont seulement invités à travailler avec rapidité. Jusqu'en 2003, le cas était différent en cas d'extrême urgence. L'examen de la justification des motifs n'était effectué par l'organisme de contrôle qu'a posteriori. Cette mesure s'expliquait par l'impératif d'immédiateté sans lequel l'objectif ne serait pas atteint. La CNCIS considérait que l'extrême urgence ne pouvait être invoquée que dans des situations exceptionnelles[519].

[518] Contrairement à la législation allemande

[519] La recommandation de la CNCIS de février 1995 stipulait que « la demande d'extrême urgence doit être accompagnée d'une justification spéciale mentionnant l'événement dont l'immédiateté rend indispensable le

Or, dès 1994, la CNCIS a constaté que l'extrême urgence était quelquefois invoquée sans justification suffisante : la régularisation n'intervenait qu'après plusieurs jours. S'ils se perpétuaient, ils risquaient de rendre inopérant le contrôle de la CNCIS. La CNCIS refuse, en 1994, le bénéfice de l'extrême urgence à des demandes qui ne correspondaient pas aux urgences invoquées précédemment et elle a précisé qu'elle avait l'intention de montrer encore davantage de vigilance.
Une recommandation de février 1995 a été suivie d'effets. Les mentions « extrême urgence » ont été utilisées avec davantage de précautions. A partir de 1996, les demandes en urgence absolue n'ont au contraire cessé de croître : +8, 91% en 1996, + 10,96% en 1997, + 14,59 % en 1998. Ce phénomène semblait lié à l'effort de prévention du terrorisme.
Les demandes d'interception étaient appuyées par une fiche dont le modèle a été révisé, avec l'accord de la CNCIS. Cette fiche retenait des données sur le nom, la profession de l'abonné, ceux de l'utilisateur, le lien entre l'utilisateur et l'abonné. Le contrôle de la « production de province »[520]était réalisable grâce à des appareils nouveaux de transmission.
Quant à la demande de renouvellement, elle doit, selon la CNCIS, être initialisée avec prudence. Le renouvellement ne doit pas être la règle, mais l'exception. Or, lors de premières années d'application, le nombre de renouvellements a été élevé. Voilà pourquoi la commission a recommandé en 1994 que la pratique des renouvellements fût circonscrite[521].
Cette recommandation a produit des effets mais insuffisants au gré de la commission qui a renouvelé ses critiques : la CNCIS a redouté que l'extrême urgence, comme le renouvellement, ne soient pas des recours exceptionnels[522], qu'ils n'impliquent pas de réflexion particulière et portent atteinte aux libertés individuelles, sans que cela fût justifié par un intérêt général.
Sur ces deux points qui conditionnaient largement l'application sur les interceptions de sécurité, la commission a réagi dès sa mise en place, grâce à une rationnelle utilisation du pouvoir de recommandation et a procédé à un suivi régulier.
En 2003, sans révision de la loi de 1991, le régime d'avis préalable a été étendu aux cas d'urgence, d'extrême urgence. Cela a été permis par une réactivité amélioré. Le temps de latence se compte en heures. Le contrôle des motifs a donc été généralisé.
La répartition par motifs est instructive et est révélée par la CNCIS dès 1995. La référence la plus fréquente est soit le terrorisme, soit la criminalité organisée. La sécurité nationale vient en troisième position. Une augmentation conséquente apparaît en 1996. Le motif « potentiel économique » connaît une croissance exponentielle avec cependant une baisse en 1998 et en 1999. Depuis l'entrée en vigueur du nouveau code pénal, ce motif est entré dans les mœurs juridiques ; il correspond à des préjudices importants pour les personnes morales, de grande et de moyenne dimension. En 2007, le rapport de la CNCIS enregistre un chiffre de 6000 interceptions de sécurité : 4214 interceptions initiales, 1850 renouvellements[523]. 964 des 4215 demandes ont été présentées selon la procédure d'urgence absolue, soit 23% de ces demandes[524].

---

recours à une telle procédure ». La régularisation écrite intervient « sans délai », III Rapport d'activité de la CNCIS, 1994, La Documentation française, 1995, p 21

[520] CNCIS : VIIème Rapport d'activité, 1998, La Documentation française, 199, p 15

[521] « Toute demande de renouvellement… accompagnée d'une évaluation des résultats de la demande initiale et d'un exposé actualisé des motifs pouvant justifier une telle prolongation » Recommandation de 1994, citée dans le IIIème rapport d'activité de la CNCIS, 1994, La Documentation française, 1995, p 21

[522] « La Commission constate que cette recommandation a commencé à produire effet mais estime devoir renforcer encore le contrôle des justifications afin de ne pas permettre des « renouvellements de routine », III ème rapport d'activité de la CNCIS 1994, La Documentation française, 1995, p 21

[523] Entre 2005 et 2007, le chiffre est quasiment inchangé ; le contingent est le même

[524] 17% en 2006

Le motif « groupement dissous » est peu utilisé[525]. Sa pointe d'écrêtement apparaît en 1996, l'année où le motif « sécurité nationale » est le plus utilisé. Une corrélation existe entre ces deux chiffres, liée au contexte politique et juridique. En revanche, le chiffre baisse considérablement en 1997, pour devenir insignifiant, puis pour disparaître.
En 2008, la DST et les RG sont rattachés à la DCRI, direction centrale du renseignement intérieur. Il convient d'étudier les éventuelles répercussions de ce changement organisationnel sur les demandes émanant des services de renseignement.

7) Autres pays :

7.1) Les Pays-Bas : l'interception est possible en cas de flagrant délit ou en cas de délit pour lequel la détention préventive est autorisée[526].

7.2) Le Grand Duché du Luxembourg :

La surveillance ou le contrôle à l'aide de moyens techniques appropriés, de toutes les formes de communication est autorisée aux fins de rechercher des infractions contre la sûreté extérieure de l'Etat.

Les interceptions judiciaires sont permises pour les infractions les plus graves[527]

7.3) L'Australie :

Pour ce qui concerne les interceptions de sécurité, les demandes ont pour motifs la prévention des activités préjudiciables à la sécurité du pays ou l'obtention d'informations essentielles à la sécurité du pays.

B) Les interceptions qui sont judiciaires :

1) La Suisse : les interceptions sont possibles pour l'instruction de crimes graves[528] et aussi pour les actes punissables commis au moyen de télécommunications.
2) La Suède : les interceptions sont possibles pour l'instruction des crimes graves[529]. De nouveaux motifs sont retenus avec la loi de 2008.

C) Les interceptions sont de sécurité

Le Royaume-Uni : la loi stipule que les interceptions sont possibles pour l'intérêt de la sécurité nationale (motif qui est utilisé fréquemment), pour la prévention ou la découverte d'un crime grave[530], pour la sauvegarde de la prospérité économique du Royaume-Uni.[531]. En 1985, ces motifs ne sauraient être invoqués que dans l'hypothèse où les informations recherchées ne peuvent pas être acquises par des moyens plus respectueux des libertés individuelles. Depuis le Rip Act, l'interprétation de la loi est plus laxiste. Si la sauvegarde des libertés individuelles est officiellement prise en compte, le souci de l'ordre public est une priorité.
Ainsi, il apparait que la motivation, en matière d'interceptions judiciaires correspond la plupart du temps à des crimes et aussi à des délits dont la gravité varie avec la culture juridique du pays.
En matière d'interceptions de sécurité, les motifs sont le plus souvent relatifs à la sécurité extérieure ou intérieure des Etats.

---

[525] Groupements dissous : 1995 : 17 demandes initiales, 23 renouvellements ; 1996 : 20 demandes initiales, 23 renouvellements ; 1997 : 7 demandes initiales, 7 renouvellements ; 1998 : 0 demande initiale, 9 renouvellements ; 1999 : 0 demande initiale, 3 renouvellements. Ensuite, le motif « groupement dissous disparaît des statistiques.
Sources : VI ème rapport d'activité de la CNCIS 1997, La Documentation française 1998, p 15 ; VIIIème rapport d'activité de la CNCIS, La Documentation française, 1998, p16

[526] Article 125f du Code de procédure pénale

[527] Articles 88.1 et 88.2 du Code pénal

[528] Article 66.1 de la loi fédérale sur la procédure pénale

[529] Chapitre 27, section 6 du code procédure judiciaire

[530] Article deux,(2)b de l'Interception of Communications Act de 1985

[531] Qui concerne surtout l'espionnage économique

II) Les interceptions de données techniques : apparaissent avec le développement d'Internet.

Au niveau de l'Union européenne, la directive dénommée « Data Retention » permet en 2006 de conserver les paramètres techniques pendant une durée qui va de six à vingt-quatre mois. Cette directive est intervenue après l'adoption du projet de décision-cadre par le Conseil européen les 29 et 30 avril 2004, sur l'initiative de quatre pays, la France, l'Irlande, le Royaume-Uni, la Suède. Ce texte envisage une durée de conservation minimale fixée à un an, susceptible d'être portée à trois ans. Ces données concernent les appels, les SMS, les méls effectués par les abonnés. La directive s'appuie sur le projet de directive-cadre. Les associations de défense des libertés civiles, dont IRIS[532], EDRI[533]et Privacy International ont manifesté leur inquiétude dans une lettre ouverte. Ils redoutent une surveillance massive et collective, à titre préventif, de l'ensemble des citoyens et des résidents.

Au niveau national, des durées ont été fixées pour les données techniques. En la matière, le Royaume-Uni a joué un rôle d'avant-garde ; la Cour constitutionnelle de Karlsruhe a pris en compte les libertés individuelles ; en France, le législateur a progressivement mis l'accent sur davantage de sécurité.

A)Les données de connexion : la convention sur la cybercriminalité avait permis de stocker les données de connexion pendant une durée de trois mois. Cette décision avait induit des débats. Les défenseurs des libertés individuelles avaient dénoncé cette mesure et, en particulier, la durée jugée trop longue de la conservation. Ainsi s'étaient prononcés IRIS, Imaginons un réseau Internet solidaire, et la Ligue des droits de l'homme. La question de la conversation des données de connexion est prise en compte par la Commission et le Parlement européen. Dans la directive du 12 juillet 2002, il est indiqué que les données de connexion peuvent être stockées pendant un an. Une nouvelle discussion est engagée sur l'opportunité de la durée-un an ou plus d'un an.

B)Les données techniques en général : sont de plus en plus fréquemment prises en considération.

1) Le Royaume-Uni

1.1) RIPA : est une loi du Royaume-Uni qui régule les compétences des autorités qui effectuent de la surveillance et des interceptions. Elle prend en compte l'importance d'Internet et les méthodes de chiffrage qualifiées de solides.

La RIPA peut être invoquée pour des motifs tenant à la sécurité nationale, à la prévention des crimes et des troubles à l'ordre public, à la protection de la santé publique et de la santé économique du pays.

La RIPA est entrée en vigueur le 28 juillet 2000. En septembre 2003, le ministre de l'Intérieur de l'époque, David Blunkett a fait savoir que le champ d'application de RIPA était élargi. En 2008, la liste englobe les Jobcentres[534], les conseils municipaux. Au moment du vote de la loi, seuls neuf organismes pouvaient se référer à RIPA, dont les services de police et de renseignement. En 2008, 792 organismes peuvent s'en prévaloir.

Le RIPA permet :

- d'exiger, dans le secret, qu'un FAI lui donne accès aux communications d'une personne

[532] Imaginons un réseau Internet solidaire

[533] European Digital Rights

[534] Subventionnée par le gouvernement britannique, un Jobcentre est à la fois une agence de recherche d'emplois et un centre d'études pour traiter les dossiers afférents à la sécurité sociale

- la surveillance de l'ensemble des communications électroniques transitant par le territoire britannique
- de demander à un fournisseur d'accès de mettre à niveau ses équipements de télécommunications afin de faciliter la surveillance
- pour le gouvernement d'exiger qu'une personne lui remette les clés ayant servi à chiffrer ses informations[535]

RIPA concerne donc à la fois les interceptions de communications électroniques et de données techniques. Cette loi, dit-on, aurait recueilli l'assentiment des parlementaires mais aurait fait l'objet de réserves de la part d'associations de défense des droits de l'homme. En fait, RIPA a été critiqué par l'ensemble des personnes morales et physiques attachées aux droits de l'homme. Des parlementaires, inquiets du rôle nouveau tenu par les conseils municipaux en la matière, ont émis des observations. Keith Vaz, président du Home Affairs Committee à la Chambre des communes considère que RIPA induit des abus, puisque certains dossiers sont « petty and vindictive ». Brian Binley, également membre du Parlement souhaite que les conseils municipaux ne soient plus habilités à se prévaloir de RIPA

1.2) Anti- Terrorism Crime and Security Act 2001 : le Royaume-Uni permet aux fournisseurs de services de communications électroniques de rassembler et de stocker les données de transmission. Les renseignements sur l'abonné : nom, date de naissance, numéro de téléphone, adresse de facturation, adresse électronique, adresse IP, méthodes de paiement, identifiants de la carte de crédit peuvent être conservés pendant douze mois. Les renseignements téléphoniques : numéros de téléphone fixe ou mobile, l'identificateur unique, la date de la communication, l'heure et la durée de l'appel, l'emplacement de l'interlocuteur peuvent être stockés pendant douze mois. Les renseignements sur les méls envoyés et reçus : les adresses IP et électroniques, la date, l'heure peuvent être conservés pendant six mois. Les renseignements sur les activités Internet : la date et l'heure, les adresses IP, les adresses URL visitées peuvent être stockées.

Par ailleurs, les articles 21 à 25 de RIPA créent un système qui autorise les organisations référencées à accéder aux données de transmission. La demande est initiée par une personne désignée et n'implique pas l'autorisation d'un juge. Elle est prévue surtout à des fins d'enquête criminelle, de sécurité nationale ou de protection du public. Des protections sont mises en vigueur : un commissaire[536] surveille l'exercice des pouvoirs conférés aux personnes désignées[537]. De plus, un tribunal est diligenté pour recevoir les plaintes du public. Les renseignements recollés dans le cadre des données de transmission sont nombreux. Les plaintes déposées par le public sont rares.

Le « Anti-Terrorism, Crime and Security Act » a porté au Royaume-Uni la durée de conservation des données de connexion des internautes par les fournisseurs d'accès à un an au moins. Le ministère de l'Intérieur a indiqué qu'il entendait « avoir un droit de regard sur les transactions financières en ligne, ou contrôler les méls privés ». Le contrôle s'amenuise : la police est dispensée en de multiples occasions de l'autorisation préalable d'un juge. Il suffit d'obtenir l'accord du ministre de l'Intérieur ou l'un de ses proches collaborateurs pour agir.

[535] Communications, fichiers, agenda
[536] Interception of Communications Commissioner
[537] Article 57 de RIPA

Elizabeth France, commissaire à l'Information en Grande-Bretagne a estimé[538] que RIPA révisé et « Anti-Terrorism, Crime and Security Act » entrent parfois en conflit. Par exemple, la loi antiterroriste précise que les données de connexion peuvent être retenues « pendant une période plus longue que ne le réclament les besoins des opérateurs, mais seulement si ces données sont nécessaires à des enquêtes impliquant la sécurité nationale ». RIPA, de son côté, autorise un grand nombre d'instances, sans mandat judiciaire, à accéder à ces données alors que la majorité de ces instances n'ont pas pour objectif de protéger la sécurité nationale.
Les données techniques sont donc aisément accessibles au Royaume-Uni.

1.3) Les attentats de Londres, très médiatisés, ont été exploités par les autorités gouvernementales. Ces dernières ont fait savoir que la conversation de longue durée des données était souhaitable « Les enregistrements des télécommunications, que ce soit par téléphone ou par le biais d'e-mails, qui permettent de savoir quels appels ont été passés d'un numéro à l'autre et à quelle heure, sont d'une très grande importance pour les services de renseignements » a déclaré Charles Clarke, le ministre britannique de l'intérieur de l'époque dans une interview à la BBC. Il est essentiel, selon lui, de retrouver l'heure d'un appel ou d'envoi d'un message, son émetteur et son destinataire « Nous croyons qu'il est important d'obtenir sur une longue durée la rétention de ces données ».

Le Royaume-Uni fait valoir que le rejet par le parlement européen (qui considérait le projet soutenu par le Royaume-Uni comme « inapproprié et déraisonnablement sévère ») de la décision-cadre n'a pas de véritable valeur juridique. Il est favorable à la conservation des données de localisation lorsqu'une communication est passée par un téléphone mobile, et à la conservation de l'historique des sites web consultés, des adresses IP des personnes contactées par messagerie instantanée, ou adresses e-mail des correspondants d'un abonné. Il considère que la durée de conservation doit être de 12 à 36 mois. C'est ainsi que la directive sur la conservation des données a rapidement avancé.

2) L'Allemagne : dans ce pays, la problématique des données techniques a donné lieu à un débat législatif et juridictionnel

2.1) Les lois :

Le 24 mai 2007, le Bundestag adopte la loi « anti hacker » en débattant notamment sur les paragraphes 202 et 303. Le texte est adopté sans amendements. Le paragraphe 202 a prohibe l'accès non autorisé à des données informatiques de l'Etat et des entreprises, en particulier le contournement de mesures techniques de protection des données.
En juin 2007, la Commission pour la protection des données de l'Etat de Saxe critique dans son huitième rapport « une tendance vers un Etat Big Brother » Elle mentionne entre autres le fichier anti-terroriste.
Le 4 juillet 2007, le Bundestag adopte la loi sur la propriété intellectuelle. Un amendement fait de l'échange de fichiers par les réseaux P2P une infraction passible d'une contravention. Les taxes pour copies privées peuvent être modulées à la demande de l'industrie. Le 10 novembre 2007, le Bundestag adopte par 366 voix contre 156 la loi qui transpose la directive « Data Retention ». Le 1er janvier 2008, la loi impose aux opérateurs de téléphonie fixe et mobile de stocker les numéros de téléphone, date et heure des échanges ou lieu de l'appel. A partir de

[538] Déclaration d'août 2002

2009, les fournisseurs d'accès à Internet sont astreints à la même obligation pour ce qui concerne la conservation des adresses IP et des logs de connexion. La conservation des données de connexion est limitée à six mois. Selon Brigitte Zypries, alors ministre de la justice : « Les seules données qui seront conservées sont celles qui sont générées de toute manière »

En décembre 2007, à l'initiative de différents groupes, allant de la droite à la gauche, plus de 20000 Allemands déposent une plainte devant la Cour constitutionnelle allemande à Karlsruhe.

2.2) La Cour constitutionnelle de Karlsruhe a rendu une décision préliminaire le 19 mars 2008. Cette décision n'exclut pas le principe de conservation des données de connexion, mais limite néanmoins l'utilisation de ces données de connexion à des délits et crimes graves, homicides, abus sexuels, affaires de terrorisme, affaires de fraude fiscale ou de corruption et à condition que la demande d'accès aux données intervienne dans le cadre d'une procédure judiciaire. Les sociétés d'auteurs ou de producteurs de cinéma ou de musique ne pourront pas utiliser ces données pour lutter contre le piratage sur Internet.

Ainsi, la Cour de Karlsruhe montre une fois de plus sa vigilance à l'égard de la protection de la vie privée.

3) La France : tous les opérateurs attendaient de connaître l'étendue de leurs obligations de conservation en termes de données de connexion depuis l'adoption de la loi sur la sécurité quotidienne[539], de la loi pour la confiance dans l'économie numérique[540] et de la loi anti-terrorisme[541].

Le décret du 24 mars 2006 n'englobe pas toutes les situations légales où la conservation est prévue. Ainsi, le décret laisse de côté les hypothèses où la conservation est liée à l'application de la LCEN. Ces cas sont ceux où les fournisseurs d'accès ou d'hébergement se voient imposer 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 elles sont prestataires ». La loi stipule qu'un « décret en Conseil d'Etat, pris après avis de la CNIL, définit les données…et détermine la durée et les modalités de leur conservation ». En l'absence de visa de la LCEN dans le décret n° 2006-358, il faut en conclure que les « données relatives au trafic ne sont pas les données de nature à permettre l'identification des créateurs de contenus ».

La loi du 23 janvier 2006 n'est pas expressément visée par le décret mais l'article L.34-1-1 de cette loi renvoie à l'article L34-1 pour ce qui est des personnes soumises à la conservation et pour les catégories de données qui doivent être communiquées aux agents habilités. Ainsi, l'article L.34-1-1 du Code des Postes et des communications électroniques[542] est afférent aux données conservées par les « opérateurs et personnes mentionnées au I » de l'article L 34-1 du CPCE.

L'article R 10612 du CPCE, créé par le décret, définit les « données relatives au trafic » mais uniquement pour l'application des II et III de l'article L 34-1 du CPCE et non pour l'ensemble des cas où cette conservation peut être requise. La définition précise que les données relatives au trafic sont des « informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques

[539] Loi n° 2001-1062 du 15 novembre 2001
[540] Loi n 2004-524 du 21 juin 2004
[541] Loi n° 2006-64 du 23 janvier 2006
[542] CPCE

dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi »

La définition repose donc sur un élément technique : les informations sont extraites de celles que produisent les procédés de communication électronique. Le choix de ces informations se fait au regard de leur pertinence en fonction des finalités poursuivies par la loi mais il demeure une incertitude puisque la définition évoque les informations qui sont susceptibles d'être enregistrées par les opérateurs.

La définition de l'article R 10-12 présente un cadre commun pour l'ensemble des données relatives au trafic mais renvoie en fonction des finalités de la loi à des mesures plus précises. Les données « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications »

Pour l'application du II de l'article L 34-1 du CPCE, les données qui doivent être conservées sont :

- Les informations permettant d'identifier l'utilisateur
- Les données relatives aux équipements terminaux de communication 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 susceptibles d'identifier le ou les destinataires de la communication
- Les données susceptibles d'identifier l'origine et la localisation de la communication

Ces informations constituent, semble-t-il, le minimum nécessaire à la recherche, la constatation, la poursuite des infractions. Les objectifs, selon le Forum des droits de l'Internet, d'identification tout au long de la chaîne sont clairs.

Pour l'application du III de l'article 34-1 du CPCE, les données pour lesquelles les opérateurs sont habilités à conserver sont les suivants :

- Les données techniques permettant d'identifier l'utilisateur (dont les adresses IP)
- Les données afférentes aux équipements terminaux de communication utilisés
- Les caractéristiques techniques, la date, l'heure, la durée de chaque communication
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs
- Les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.

La finalité de cette possibilité de conserver des données techniques est clairement limitée à la nécessité de facturer le service ou à en obtenir le paiement, ce qui correspond à la période de recouvrement des créances et, éventuellement, de contestation des dettes par les utilisateurs. Si le

service n'implique pas de facturation, les données ne peuvent donc pas être conservées.
Pour la sécurité des réseaux et installations, les opérateurs peuvent conserver :

- Les données permettant d'identifier l'origine de la communication
- Les caractéristiques techniques, la date, l'horaire, la durée de chaque communication
- Les données à caractère technique permettant d'identifier le ou les destinataires de la communication
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs

Une durée fixe d'un an est assignée à la conservation des données afférentes au trafic lorsqu'il s'agit de la recherche, de la constatation , de la poursuite des infractions. Cette durée ne peut être réduite et commence à courir à compter de l'enregistrement des données.
Une durée fixe d'un an est assignée à la conservation des données afférentes lorsqu'il s'agit de la facturation, du paiement des créances.
Une durée maximale de trois mois est assignée à la conservation des données afférentes à la sécurité des réseaux et des installations.
Les opérateurs de télécommunication et les fournisseurs d'accès ne sont pas les seules personnes concernées par ce décret sur la conservation des données de connexion. Les personnes qui, au titre d'une activité professionnelle accessoire, fournissent 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 champ d'application du décret de mars 2006. Tel est notamment le cas des cybercafés. Des compensations financières sont envisagées afin de couvrir les surcoûts identifiables et spécifiques auxquels seront obligées de faire face les différentes personnes morales.
Un autre décret d'application est relatif à la LCEN et à son article six. Le chapitre premier du décret détermine, en application du II de l'article six, la nature des données à conserver par les intermédiaires techniques et la durée de cette conservation, qui est fixée à un an, à partir d'un point de départ qui peut être la modification par l'abonné d'un contenu hébergé, y compris sa suppression. La nature des données n'est pas facile à définir. Officiellement, les données ne servent qu'à « permettre l'identification de quiconque a contribué à la création du contenu du service », mais en fait, le décret prévoit la conservation de nombreuses données, y compris le mot de passe fourni lors de la souscription d'un contrat d'abonnement ou lors de la création d'un compte auprès du prestataire Internet. Le chapitre deux du décret détermine à quelles conditions les services de police et de gendarmerie peuvent demander et traiter les données conservées par les fournisseurs d'accès et d'hébergement. Ce chapitre indique que les données, une fois obtenues pourront être conservées pendant une durée de trois ans.
La France possède, avec l'Unité de Coordination de la Lutte Antiterroriste, à Levallois-Perret, une plate-forme d'interception des données de connexion. Le dispositif ne permet pas de faire des interceptions plus fiables en ce qui concerne le contenu, mais il parvient à réunir des informations sur les différents moyens de communication du

suspect[543]. Si la demande est acceptée, les enquêteurs connaissent les adresses téléphoniques, les points de connexion Internet, les fournisseurs d'accès, les abonnements liés aux numéros repérés, les sites consultés, les correspondants par téléphone, SMS ou courriel, la géolocalisation du portable. En bref, cela permet de réunir des informations qui se trouvent dans les mémoires d'ordinateur, de cerner les réseaux personnels d'un individu. Ensuite, il est possible de procéder à une interception de sécurité ou judiciaire.

Ces mesures ont été critiquées en France par les organismes de défense des droits de l'homme. Les décrets, qui ont pris la suite de la loi sur la sécurité quotidienne[544], la loi sur la sécurité intérieure, trouve sa place dans une logique de contrôle social. La conservation des données de communication identifie les activités des personnes physiques et situe les réseaux relationnels. Elle constituerait une immixtion dans la vie privée. « Avec l'utilisation de la biométrie, de la vidéosurveillance et du fichage généralisé, elle devient partie intégrante des politiques de sécurité en France et en Europe »[545]

Les données techniques jouent aussi un rôle important dans le droit de la propriété intellectuelle. Pour la CNIL, comme pour la Commission de Bruxelles, les adresses IP sont des données personnelles La décision du Conseil d'Etat annulant la décision de la CNIL du 18 octobre 2005 autorise la collecte d'adresses IP dans le cadre de la lutte contre les téléchargements illégaux ; ainsi des constats de contrefaçon sont-ils effectués et les adresses IP associées sont conservées.

La loi « Création et Internet » prévoit que le rapprochement entre les adresses IP et l'identité des titulaires de ligne peut être effectué par les fournisseurs d'accès Internet à la demande de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet, et non plus seulement du juge judiciaire comme c'est le cas dans les procès engagés sur le fondement du délit de contrefaçon.

Le 24 septembre 2008, l'amendement 138 de la réforme européenne du Paquet Télécoms a été adopté à une large majorité par les eurodéputés[546] : « en appliquant le principe selon lequel aucune restriction ne peut être imposée aux droits et libertés fondamentaux des utilisateurs finaux (d'Internet) sans décision préalable des autorités judiciaires, notamment conformément à l'article onze de la charte des droits fondamentaux de l'Union européenne, concernant la liberté d'expression et d'information, sauf lorsque la sécurité publique est menacée, auquel cas la décision peut intervenir ultérieurement ».

D'une façon générale, la conservation des données techniques pendant une certaine durée est entrée dans le corpus législatif des différents pays de l'Union européenne et la durée de conservation donne encore lieu à des débats même si l'Union européenne a pour l'instant instauré un butoir de deux ans. Le contrôle est quasiment inexistant, sauf dans le cas de l'Allemagne, avec la Cour constitutionnelle de Karlsruhe.

[543] Fixe, mobile, SMS, ordinateur éventuellement sur Wifi
[544] LSQ
[545] « Décret LSQ, peine maximale pour la vie privée », communiqué de presse d'IRIS, 26 mars 2006
[546] 573 voix pour, 74 voix contre

4) L'Italie : a renforcé sa surveillance sur les communications électroniques. Son Assemblée nationale a validé le 28 janvier 2008 un décret gouvernemental publié en Urgence la veille de Noël en décembre 2007. Les opérateurs internet et téléphoniques sont tenus de conserver les données de connexion de leurs abonnés pendant soixante mois, soit cinq ans : c'est actuellement la durée de conservation la plus longue au sein de l'Union européenne. Jusqu'en 2008[547],

la loi stipulait que ces données de connexion devaient être stockées pendant trente mois. La norme présente change la donne. A partir de la troisième année, les données de connexion sont stockées sur des serveurs différents ; elles sont séparées des informations les plus récentes ; leur consultation est limitée : seuls les services de police ou organismes d'Etat enquêtant sur le kidnapping, le crime organisé, le terrorisme, les délits informatiques peuvent y accéder. Le décret a été critiqué par l'organisme de régulation nationale en matière de protection des données personnelles : « La nouvelle discipline imposée sur les données concernant les communications électroniques et l'utilisation de l'internet pourraient aller à l'encontre des normes constitutionnelles, relatives à la liberté et au secret des communications, et à la liberté d'expression » a-t-elle indiqué avant l'examen du texte par les députés.

Les organisations non-gouvernementales ont protesté contre ce qu'elles considèrent comme une atteinte aux libertés individuelles. C'est notamment le cas d'Alcei[548]. Cette dernière proteste d'abord contre le recours au décret, nullement justifié selon elle sur les plans juridique et politique. Alcei n'insiste pas trop sur la prolongation de la durée de conservation [549]; elle met en cause le principe de rétention des données.

5) La Belgique : a été l'un des premiers Etats à légiférer pour instituer la conservation des données de connexion. En 2001, avant les attentats du 11 septembre, qui ont été utilisés par les autorités gouvernementales de la plupart des Etats occidentaux pour valider des mesures de surveillance, la conservation des données de connexion a été fixée à un an. Néanmoins, l'arrêté royal qui devait apporter des précisions sur l'application de ce texte n'a pas vu le jour.
6) L'Espagne : La ley de Servicios de la Societad de la Informacion y de Comercio electronico[550] a été adoptée par le Parlement espagnol le 27 juin 2002 et est entrée en vigueur le 8 septembre 2002. La durée de conservation des données de connexion a été fixée à un an. De nombreuses critiques se sont élevées, mettant en cause la constitutionnalité de la mesure.
7) Les autres Etats européens : au sein de l'Union européenne, la durée de conservation des données de connexion est très variable : trois ans pour la Lettonie[551], un an pour la Lituanie[552], un an pour la Pologne…. Il faut prendre en compte l'historicité juridique, la culture nationale, le rôle joué par le pays sur le plan géo-politique.
8) Les USA : les USA protègent mal les données personnelles. Seul, le Privaçy Act s'est-il soucié du stockage des données publiques. Encore les dérogations sont-elles nombreuses. C'est pourquoi les données de connexion sont-elles

[547] Source précédente : décret législatif n° 196 de 2003
[548] Association pour la liberté dans les communications électroniques interactives
[549] Le texte « a été créé dans la hâte pour amender le présent texte, qui introduisait une limite de trente mois au stockage des données, alors que désormais, ce sera cinq ans », communiqué de janvier 2008
[550] LSSICA
[551] Article 19 de la loi sur les communications électroniques du 1er mai 2004
[552] Article 64 de la loi sur les communications électroniques du 1er mai 2004

conservées de manière générale. Les moteurs de recherche enregistrent l'ensemble des données saisies par les utilisateurs et qui peuvent être rendues publiques sur injonction de justice. Une enquête[553]de 2006 démontre que les dangers courus dans le domaine des libertés individuelles et collectives sont réels. L'enquête[554] indique que les moteurs de recherche de Google, Yahoo, Microsoft conservent et archivent pour une durée non déterminée mais vraisemblablement longue les mots saisis dans le champ « recherche » de ces moteurs. Seul AOL a décidé d'effacer ces données au bout de trente jours. Sont également enregistrés les liens de la page de résultats qui sont sélectionnés et visités par les utilisateurs. Par ailleurs, les données de connexion que sont l'adresse IP ciblée selon les centres d'intérêt des internautes, les applications pratiques afférentes à ces données sont prises en compte. Il est possible, sur simple injonction de la justice auprès du fournisseur d'accès Internet, d'obtenir l'identité d'une personne à partir de son adresse IP et des horaires de connexion. Certains parlementaires ont fait connaître leurs réticences, ont souhaité l'adoption d'une loi qui imposerait aux moteurs de recherche l'obligation d'effacer les données de connexion qui sont aussi des données personnelles dans un délai qui serait fixé par la loi.[555]. En 2008 aucune loi n'a été débattue. Le Department of Justice peut accèder à ces informations sur injonction et est susceptible de lister les personnes qui ont saisi certains mots-clés à des fins de répression. De plus, les personnes physiques peuvent obtenir ces informations en sollicitant auprès du juge une injonction relative au moteur de recherche, dans le cadre d'affaires civiles, en dehors de toute incrimination pénale.
La justice va dans le même sens, pour des affaires en relation avec le droit de la propriété intellectuelle. Le 29 mai 2006, TorrentSpy, site connu des amateurs de téléchargement a été condamné par un juge californien de Los Angeles à enregistrer les données de connexion relatives aux internautes qui le visitent, pour faciliter le travail de la MPAA[556] dans sa lutte contre le piratage des œuvres cinématographiques. Producteurs et autres distributeurs de contenus se félicitent de cette décision. D'autres juristes considèrent que ce jugement porte atteinte au droit à la vie privée. Du côté de TorrentSpy, le communiqué est clair : « Les serveurs TorrentSpy n'ont jamais enregistré votre adresse IP, les recherches que vous avez effectuées ou la façon dont vous utilisez le site… Nous sommes dévoués au respect de votre vie privée et nous nous battons pour vos droits ». La MPAA menait une bataille juridique depuis février 2006 contre des sites spécialisés dans l'hébergement et le référencement de liens torrent, tels TorrentSpy. Elle reprochait à ces sites de faciliter le piratage des œuvres cinématographiques. Les sites mis en cause ont fait valoir qu'ils usaient simplement de la liberté d'expression telle qu'elle est décrite dans le premier amendement de la Constitution américaine.

J'ai essayé de prendre contact avec deux autorités de contrôle, notamment la belge. Comme je le prévoyais, ces contacts ont été infructueux. Ils n'étaient pas prêts à collaborer et j'ai constaté qu'il était plus facile d'accéder à des informations via Internet que par le mél. Je n'ai pas été étonnée. J'escomptais

[553] CNet News a diligenté une enquête qui est parue fin janvier 2006 dans ZDNet US sous forme de FAQ
[554] Cf : e-juristes.org du site du Master 2 Droit des nouvelles technologies, Université Paris X
[555] Telle est la position du sénateur du Massachussets, Ed Markey
[556] Motion Picture Association of America

ce genre de comportements. J'ai donc travaillé avec la documentation rassemblée et je m'en suis contentée.

Claudine Guerrier, professeur de droit à
Institut Télécom/TELECOM§Management ParisSud/ Cemantic
9 janvier 2009